ГОСУДАРСТВЕННОЕ НАУЧНОЕ УЧРЕЖДЕНИЕ
«ИНСТИТУТ МАТЕМАТИКИ НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК БЕЛАРУСИ»

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Международная научная конференция

Дискретная математика, алгебра и их приложения

14–18 сентября 2015 г.,
г. Минск, Республика Беларусь

Посвящается столетию со дня рождения академика Д. А. Супруненко

Тезисы докладов

МИНСК 2015

УДК 519.1, 512
ББК 22.174 + 22.14
Д 44

Редакторы:
И. Д. Супруненко, В. В. Лепин, О. И. Дугинов

Дискретная математика, алгебра и их приложения: Тез. докл. Междунар.
Д 44 науч. конф. Минск, 14 – 18 сентября 2015 г. — Мн.: Институт математики НАН Беларуси, 2015. — 172 с.

ISBN 978-986-6499-86-2

Сборник содержит тезисы докладов, представленных на международной научной конференции «Дискретная математика, алгебра и их приложения».

ISBN 978-986-6499-86-2

АЛГЕБРА И АЛГЕБРАИЧЕСКАЯ ГЕОМЕТРИЯ

О КОНЕЧНЫХ НЕРАЗРЕШИМЫХ ГРУППАХ, ГРАФЫ ГРЮНБЕРГА—КЕГЕЛЯ КОТОРЫХ НЕ СОДЕРЖАТ ТРЕУГОЛЬНИКОВ

О.А. Алексеева[1], А.С. Кондратьев[2]

[1]Русско-Британский институт управления, Ворошилова 12, 454014 Челябинск, Россия
Alekseeva.O.A@rbiu.ru
[2]Институт математики и механики им. Н.Н. Красовского УрО РАН, Ковалевской 16, 620990 Екатеринбург, Россия
a.s.kondratiev@imm.uran.ru

Пусть G — конечная группа и $\pi(G)$ — множество всех простых делителей ее порядка. Графом простых чисел (или графом Грюнберга—Кегеля) $\Gamma(G)$ группы G называется граф с множеством вершин $\pi(G)$, в котором две различные вершины p и q смежны тогда и только тогда, когда G содержит элемент порядка pq.

Лючидо [1] исследовала конечные группы, графы Грюнберга—Кегеля которых являются деревьями, т. е. связными графами, не содержащими циклы. Мы рассматриваем более общую задачу описания строения конечных групп, графы Грюнберга—Кегеля которых не содержат треугольников, т. е. 3-циклов. Легко доказывается, что если G — группа с таким свойством, то либо G разрешима, либо фактор-группа $G/S(G)$ группы G по ее разрешимому радикалу $S(G)$ почти проста, т. е. имеет неабелев простой цоколь. В [2] и [3] мы описали конечные почти простые и разрешимые группы с таким свойством соответственно.

В данной работе мы продолжаем эти исследования, рассматривая строение конечных неразрешимых групп с таким свойством. Доказана

Теорема. *Если G – конечная неразрешимая группа и граф $\Gamma(G)$ не содержит треугольников, то $|\pi(G)| \leq 8$ и $|\pi(S(G))| \leq 3$.*

Кроме того, получено детальное описание групп G, удовлетворяющих условию теоремы, в случае, когда $\pi(S(G))$ содержит число, не делящее порядок группы $G/S(G)$.

Работа выполнена при финансовой поддержке гранта РНФ (проект 15-11-10025).

Литература

1. Lucido M. C. *Groups in which the prime graph is a tree* // Boll. Unione Mat. Ital. (8). 2002. V. 5-B. №1. P. 131–148.

2. Алексеева О. А., Кондратьев А. С. *Конечные почти простые группы, графы Грюнберга—Кегеля которых не содержат треугольников* // Межд. конф. "Мальцевские чтения". Тез. докл. Новосибирск: ИМ и НГУ, 2014. С. 50.

3. Алексеева О. А., Кондратьев А. С. *О конечных разрешимых группах, графы Грюнберга—Кегеля которых не содержат треугольников* // Межд. конф. "Мальцевские чтения". Тез. докл. Новосибирск: ИМ и НГУ, 2015. С. 83.

О ПЕРЕСЕЧЕНИЯХ МАКСИМАЛЬНЫХ θ-ПОДГРУПП КОНЕЧНЫХ ГРУПП

Л.М. Белоконь

Белорусско-Российский университет, проспект Мира 43, 212000 Могилёв, Беларусь
bellu2006@yandex.ru

Рассматриваются только конечные группы. Используются определения и обозначения, принятые в монографиях [1] и [2]. Обозначаем через π некоторое множество простых чисел; $\pi' = \mathrm{P}\backslash\pi$, P — множество всех простых чисел. Пусть $\mathfrak{F}$ – непустая формация, θ — подгрупповой m-функтор [2]. Если для любой группы G множество $\theta(G)$ включает все $\mathfrak{F}$-абнормальные максимальные подгруппы группы G, то θ будем называть $\mathfrak{F}$-абнормально полным m-функтором; в случае $\mathfrak{F} = \mathfrak{N}$ m-функтор θ называется абнормально полным [3]. Через θ_π будем обозначать подгрупповой m-функтор, сопоставляющий каждой группе G саму группу G и множество всех тех её максимальных θ-подгрупп, индекс каждой из которых не делится на числа из π. Через $\Phi_\theta(G)$ обозначают пересечение всех θ-подгрупп группы G. Если для любой группы G множество $\theta(\mathrm{G})\backslash\{\mathrm{G}\}$ совпадает с множеством всех максимальных (всех максимальных $\mathfrak{F}$-абнормальных) подгрупп в G, то $\Phi_{\theta_\pi}(G) = \Phi_\pi(G)$, ($\Phi_{\theta_\pi}(G) = \Delta^{\mathfrak{F}}_\pi(G)$, соответственно; $\Delta^{\mathfrak{F}}_\pi(G) = \Delta_\pi(G)$, если $\mathfrak{F} = \mathfrak{N}$). Через $\Phi_{\theta,\overline{N}}(G)$ ($\Phi_{\theta_\pi,\overline{N}}(G)$) обозначаем пересечение всех максимальных θ-подгрупп (θ_π-подгрупп, соответственно) группы G, не содержащих нормальной в G подгруппы N. Пересечение всех максимальных (всех максимальных $\mathfrak{F}$-абнормальных) подгрупп группы G, каждая из которых имеет взаимно простой с числами из π индекс и не содержит N, обозначаем через $\Phi_{\pi,\overline{N}}(G)$ ($\Delta^{\mathfrak{F}}_{\pi,\overline{N}}(G)$ соответственно). Если в группе G не существует максимальных подгрупп, отвечающих указанным требованиям, соответствующие пересечения считаем совпадающими с G. Подгруппа $\tilde{\mathrm{F}}_N(G)$ группы G, N — нормальная в G подгруппа, определяется следующим образом: $\tilde{\mathrm{F}}_N(G) \supseteq N$, $Soc(G/N) = \tilde{F}_N(G)/N$ [4]; используем обозначения $\tilde{\mathrm{F}}_{\Phi_\theta}(G)$, $\tilde{\mathrm{F}}_{\Phi_{\theta_\pi}}(G)$, $\tilde{\mathrm{F}}_{\Phi_\pi}(G)$, $\tilde{\mathrm{F}}_{\Delta^{\mathfrak{F}}_\pi}(G)$ в соответствующих случаях для $N \in \left\{ \Phi_\theta(G), \quad \Phi_{\theta_\pi}(G), \quad \Phi_\pi(G), \quad \Delta^{\mathfrak{F}}_\pi(G) \right\}$.

Теорема 1. *Имеют место следующие утверждения.*

(1) *Для всякой группы G и подгруппового m-функтора θ справедливо равенство*

$$\Phi_{\theta_\pi,\overline{\tilde{\mathrm{F}}_{\Phi_{\theta_\pi}}(G)}}(G) = \Phi_{\theta_\pi}(G).$$

(2) *Пусть $\mathfrak{F} = \mathfrak{G}_\pi\mathfrak{F}$ — локальная S_n-замкнутая формация, содержащая формацию всех нильпотентных π'-групп $\mathfrak{N}_{\pi'}$. И пусть группа $G \notin \mathfrak{F}$, подгруппа $\Phi_\pi(G)$ обладает свойством C_π. Если m-функтор θ является $\mathfrak{F}$-абнормально полным, то $\Phi_{\theta_\pi,\overline{\tilde{\mathrm{F}}_{\Phi_{\theta_\pi}}(G)}}(G) \neq G$.*

Следствие 1.1 [4]. *Имеют место следующие утверждения.*

(1) *Для всякой группы G и непустой формации $\mathfrak{F}$ выполняется равенство $\Delta^{\mathfrak{F}}_\pi(G) = \Delta^{\mathfrak{F}}_{\pi,\overline{\tilde{\mathrm{F}}_{\Delta^{\mathfrak{F}}_\pi}(G)}}(G)$.*

(2) *Пусть $\mathfrak{F} = \mathfrak{G}_\pi\mathfrak{F}$ — локальная S_n-замкнутая формация, содержащая формацию всех нильпотентных π'-групп $\mathfrak{N}_{\pi'}$. Если группа $G \notin \mathfrak{F}$, подгруппа $\Phi_\pi(G)$ обладает свойством C_π, то $\Delta^{\mathfrak{F}}_{\pi,\overline{\tilde{\mathrm{F}}_{\Delta^{\mathfrak{F}}_\pi}(G)}}(G) \neq G$.*

Так как $\Phi_\pi(G) \neq G$, если G — π'd-группа и подгруппа $\Phi_\pi(G)$ обладает свойством C_π, то из утверждения (1) теоремы 1 получаем

Следствие 1.2 [4]. *Пусть G — π'd-группа, подгруппа $\Phi_\pi(G)$ обладает свойством C_π. Тогда в G существует хотя бы одна максимальная, π'-индекса подгруппа, не содержащая $\tilde{\mathrm{F}}_{\Phi_\pi}(G)$; пересечение всех таких подгрупп совпадает с $\Phi_\pi(G)$.*

Теорема 2. *Пусть* θ – $\mathfrak{G}_\pi\mathfrak{N}_{\pi'}$*-абнормально полный* m*-функтор. И пусть подгруппа* $\Phi_\pi(G)$ *группы* G *обладает свойством* C_π*. Тогда:*

(1) $\Phi_{\theta_\pi,\overline{\tilde{\mathrm{F}}_{\Phi_\pi}(G)}}(G) = \Phi_{\theta_\pi}(G)$;

(2) *если* $G \neq \mathrm{F}_{\pi'}(G)$, *то* $\Phi_{\theta_\pi,\overline{\tilde{\mathrm{F}}_{\Phi_\pi}(G)}}(G) \neq G$.

Следующий результат, вытекающий из теоремы 2 при $\pi = \varnothing$, доказан в [5] для случая θ — эпиморфный абнормально полный m-функтор.

Следствие 2.1. *Пусть* θ — *абнормально полный* m*-функтор,* G *группа. Тогда:*

(1) $\Phi_{\theta,\overline{\tilde{\mathrm{F}}(\mathrm{G})}}(G) = \Phi_\theta(G)$;

(2) *если* $G \neq \mathrm{F}(G)$, *то* $\Phi_{\theta,\overline{\tilde{\mathrm{F}}(\mathrm{G})}}(G) \neq G$.

Из утверждения (1) следствия 2.1, как и из следствия 1.2, вытекает утверждение [5] о совпадении подгруппы Фраттини неединичной группы G с пересечением всех её максимальных подгрупп, не содержащих $\tilde{\mathrm{F}}(G)$.

Теорема 3. *Пусть подгруппа* $\Phi_\pi(G)$ *группы* G *обладает свойством* C_π*. Тогда:*

(1) $\Delta_{\pi,\overline{\tilde{\mathrm{F}}_{\Phi_\pi}(G)}}(G) = \Delta_\pi(G)$;

(2) *если* $G \neq \mathrm{F}_{\pi'}(G)$, *то в* G *существуют максимальные абнормальные подгруппы, имеющие взаимно простые с числами из* π *индексы и не содержащие* $\tilde{\mathrm{F}}_{\Phi_\pi}(G)$.

Теорема 3, выводимая из теоремы 2, а также теорема 2 и следствие 2.1 включают результат работы [5] о том, что в каждой ненильпотентной группе G существует ненормальная максимальная подгруппа M такая, что $M\tilde{F}(G) = G$; пересечение всех таких максимальных ненормальных подгрупп M совпадает с подгруппой Гашюца $\Delta(G)$.

Литература

1. Шеметков Л. А. *Формации конечных групп.* М: Наука, 1978.

2. Каморников С. Ф., Селькин М. В. *Подгрупповые функторы и классы конечных групп.* Мн.: Бел. навука, 2003.

3. Бородич Е. Н., Бородич Р. В. *О пересечениях* $\mathfrak{F}$*-абнормальных максимальных* θ*-подгрупп* // Весці Нацыянальнай Акадэміі Навук Беларусі. 2007. № 3. С. 47–52.

4. Белоконь Л. М. *О пересечениях максимальных подгрупп конечных групп* // Проблемы физики, математики и техники. 2014. № 4(21). С. 46–59.

5. Васильев А. Ф., Васильева Т. И., Сыроквашин А. В. *Заметка о пересечениях некоторых максимальных подгрупп конечных групп* // Проблемы физики, математики и техники. 2012. № 2(11). С. 62–64.

О БИРАЦИОНАЛЬНОЙ КОМПОЗИЦИИ КВАДРАТИЧНЫХ ФОРМ НАД ПОЛЕМ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ

А.А. Бондаренко

Белорусский государственный университет, механико-математический факультет
Независимости 4, 220050 Минск, Беларусь bondarenko@bsu.by

Пусть $f(X)$ и $g(Y)$ — невырожденные квадратичные формы размерности m и n над полем K, $char\ K \neq 2$.

Определение. Если произведение $f(X) \cdot g(Y)$ бирационально эквивалентно над K квадратичной форме $h(Z)$ над K размерности $m+n$, то будем говорить, что квадратичные формы $f(X)$ и $g(Y)$ образуют бирациональную композицию $h(Z)$ над полем K.

Первые результаты по проблеме композиции восходят к Гурвицу, который изучал задачу о “сумме квадратов”. Классические результаты Гурвица и Радона по этой задаче хорошо известны (см. [1]). В [2] получены первые общие теоремы о бирациональной композиции квадратичных форм над полем K, полное решение проблемы бирациональной композиции

квадратичных форм над локальным полем дано в [3], над глобальным полем положительной характеристики в [4].

Основная цель настоящего сообщения — решение проблемы бирациональной композиции над полем алгебраических чисел.

Решение проблемы бирациональной композиции квадратичных форм $f(X)$ и $g(Y)$ над полем алгебраических чисел L в случае, если $f(X)$ либо $g(Y)$ изотропна над L, следует из теоремы 1 статьи [2]. Полное решение проблемы, когда обе квадратичные формы $f(X)$ и $g(Y)$ анизотропные над полем L, при $1 \leq m \leq n \leq 4$, дает

Теорема. *Пусть $f(X)$ и $g(Y)$ — анизотропные квадратичные формы размерности m и n над полем алгебраических чисел L, $1 \leq m \leq n \leq 4$. Тогда бирациональная композиция $h(Z)$ над L определена однозначно с точностью до L-эквивалентности следующим образом:*

1) при $1 = m \leq n \leq 4$ бирациональная композиция существует всегда и

$$h(z_1, \ldots, z_{n+1}) = ag(z_1, \ldots, z_n),$$

где $a \in D_L(f)$;

2) при $m = n = 2$ и $m = n = 3$ бирациональная композиция существует тогда и только тогда, когда $f(X)$ и $g(Y)$ эквивалентны с точностью до множителя над L, и если $m = n = 2$, то $h(z_1, z_2, z_3, z_4) = ag(z_1, z_2)$, где $a \in D_L(f)$, если $m = n = 3$, то $h(z_1, z_2, z_3, z_4, z_5, z_6) = \lambda(z_1^2 + \alpha z_2^2 + \beta z_3^2 + \alpha\beta z_4^2)$, где $g(Y) \sim \lambda f(X)$, $f(X) \sim a(x_1^2 + \alpha x_2^2 + \beta x_3^2)$;

3) при $m = n = 4$ бирациональная композиция существует тогда и только тогда, когда $f(X)$ и $g(Y)$ эквивалентны с точностью до множителя над L одной и той же пфистеровой форме, и если $f(X) \sim a(x_1^2 + \alpha x_2^2 + \beta x_3^2 + \alpha\beta x_4^2)$, $g(Y) \sim b(y_1^2 + \alpha y_2^2 + \beta y_3^2 + \alpha\beta y_4^2)$, то $h(z_1, z_2, z_3, z_4, z_5, z_6, z_7, z_8) = ab(z_1^2 + \alpha z_2^2 + \beta z_3^2 + \alpha\beta z_4^2)$;

4) при $m = 2$ и $n = 3$ бирациональная композиция существует тогда и только тогда, когда $f(X)$ является с точностью до множителя над L подформой $g(Y)$, и если $f(X) \sim a(x_1^2 + \alpha x_2^2)$, $g(Y) \sim b(y_1^2 + \alpha y_2^2 + \alpha\beta y_3^2)$, то $h(z_1, z_2, z_3, z_4, z_5) = ab(z_1^2 + \alpha z_2^2 + \beta z_3^2 + \alpha\beta z_4^2)$;

5) при $m = 2, 3$ и $n = 4$ бирациональная композиция существует тогда и только тогда, когда $g(Y)$ эквивалентна с точностью до множителя над L пфистеровой форме, и $f(X)$ с точностью до множителя над L является подформой $g(Y)$, и если $f(X) \sim a(x_1^2 + \alpha x_2^2)$ при $m = 2$, $f(X) \sim a(x_1^2 + \alpha x_2^2 + \beta x_3^2)$ при $m = 3$, и $g(Y) \sim b(y_1^2 + \alpha y_2^2 + \beta y_3^2 + \alpha\beta y_4^2)$, то $h(z_1, \ldots, z_{m+n}) = ab(z_1^2 + \alpha z_2^2 + \beta z_3^2 + \alpha\beta z_4^2)$.

Если среди архимедовых нормирований поля L нет вещественных, то теорема полностью решает вопрос о бирациональной композиции анизотропных форм над L, ибо любая анизотропная форма над этим полем размерности ≤ 4.

Над полями алгебраических чисел, у которых есть вещественные нормирования, вопрос о бирациональной композиции анизотропных форм далек от завершения.

Литература

1. Lam K. Y. *Topological methods for studing the composition of quadratic forms* // Quadratic and hermitian forms. Conf. Proc. Providence. Rhod Island. 1984. Vol. 4. P. 173–192.

2. Бондаренко А. А. *О бирациональной композиции квадратичных форм* // Весці НАН Беларусі, сер. фіз.-мат. навук. 2007. № 4. С. 56–61.

3. Бондаренко А. А. *Бирациональная композиция квадратичных форм над локальным полем* // Матем. зам. 2009. Т. 85. № 3. С. 661–670.

4. Бондаренко А. А. *Бирациональная композиция квадратичных форм над полем функций* // Весці НАН Беларусі, сер. фіз.-мат. навук. 2014. № 3. С. 28–32.

СИММЕТРИИ АЛГОРИТМОВ МАТРИЧНОГО УМНОЖЕНИЯ

В.П. Бурименко

Лаборатория теории конечных групп Института математики НАН Беларуси,
Кирова 32а, 246000 Гомель, Беларусь
vpburich@gmail.com

Данная работа связана с проблемой быстрого умножения матриц. Рассматриваются некоммутативные (в смысле [1]) алгоритмы умножения матриц. Пусть K — поле, R — ассоциативная K-алгебра, X и Y — $m \times n$ и $n \times p$ матрицы над R. Вычисление произведения XY обычным способом ("строка на столбец") требует mnp умножений в R. Однако, существуют более быстрые алгоритмы. При $m = n = p = 2$ достаточно 7 умножений (алгоритм Штрассена, [2]), при $(m, n, p) = (2, 3, 3)$ — 15 умножений (алгоритм Хопкрофта, [3]), $m = n = p = 3$ — 23 умножения (алгоритм Ладермана, [4]), при $m = n = p = 2l$ — $(n^3 - 4n)/3 + 6n^2$ умножений (алгоритм трилинейного агрегирования Пана, [5]). Обозначим минимальное необходимое число умножений через $r(m, n, p)$ (вообще говоря, $r(m, n, p)$ зависит от K).

Если есть (нетривиальный) алгоритм умножения $m \times n$ матрицы на $n \times p$ матрицу, требующий r умножений, его можно применить рекурсивно и показать, что умножение двух квадратных $N \times N$ матриц над K требует $O(N^\tau)$ арифметических операций, где $\tau = 3 \log_{mnp} r$ (см. [1]). Поэтому нахождение верхней оценки для $r(m, n, p)$ при конкретных m, n, p — практически (и теоретически) важная задача.

Алгоритмы матричного умножения тесно связаны с разложениями тензоров. Пусть $\widetilde{U} = U_1 \otimes \ldots \otimes U_l$ — тензорное произведение нескольких пространств над K. Тензор $u \in \widetilde{U}$ называется *разложимым*, если $u = u_1 \otimes \ldots \otimes u_l$, $u_i \in U_i$. Далее, если $t \in \widetilde{U}$ — произвольный тензор, и $\mathcal{A} = \{t_1, \ldots, t_s\}$ — множество разложимых тензоров такое, что $t_1 + \ldots + t_s = t$, тогда $\mathcal{A}$ называется *алгоритмом* (длины s) *для вычисления тензора* t. Минимальная длина $s = |\mathcal{A}|$ называется *рангом* тензора t, и обозначается через $\mathrm{rk}(t)$.

Через $M_{ab} = M_{a,b}(K)$ обозначим пространство $a \times b$ матриц над K. Для данных m, n, p положим $L_1 = M_{mn}$, $L_2 = M_{np}$, $L_3 = M_{pm}$, $L = L_1 \otimes L_2 \otimes L_3$, и рассмотрим тензор

$$\langle m, n, p \rangle = \sum_{1 \le i \le m,\ 1 \le j \le n,\ 1 \le k \le p} e_{ij} \otimes e_{jk} \otimes e_{ki} \in L.$$

Хорошо известно, что алгоритмы, вычисляющие произведение $m \times n$ и $n \times p$ матриц, находятся в биекции с алгоритмами, вычисляющими тензор $\langle m, n, p \rangle$, и что

$$r(m, n, p) = \mathrm{rk}(\langle m, n, p \rangle).$$

Таким образом, изучение алгоритмов матричного умножения — это в точности изучение разложений тензоров $\langle m, n, p \rangle$.

Автор считает, что одним из плодотворных путей для построения экономичных алгоритмов (т.е., коротких разложений тензоров) является исследование алгоритмов, обладающих нетривиальной группой симметрии. Дадим необходимые определения.

Пусть $\widetilde{U} = U_1 \otimes \ldots \otimes U_l$ — тензорное произведение, как выше. Автоморфизм $g \in GL(\widetilde{U})$ *разложим*, если он согласован, в очевидном смысле, со структурой тензорного произведения на $\widetilde{U}$ (при этом g может переставлять факторы $U_1, \ldots, U_l$ нетривиальным образом). Группу всех разложимых автоморфизмов обозначим $S(\widetilde{U}) = S(U_1, \ldots, U_l)$. Для данного тензора $t \in \widetilde{U}$ определим его *группу изотропии* $\Gamma(t)$ как

$$\Gamma(t) = \{g \in S(\widetilde{U}) \mid g(t) = t\}.$$

Далее, для данного алгоритма $\mathcal{A} = \{t_1, \ldots, t_s\}$, вычисляющего t, определим его *группу автоморфизмов*

$$\mathrm{Aut}(\mathcal{A}) = \{g \in S(\widetilde{U}) \mid g(\mathcal{A}) = \mathcal{A}\}.$$

Ясно, что всегда $\mathrm{Aut}(\mathcal{A}) \leq \Gamma(t)$.

Очевидно, первый шаг при исследовании алгоритмов с точки зрения их симметрии — определить группы автоморфизмов для известных хороших алгоритмов. Это является основным результатом настоящей работы.

Пусть $\mathcal{S}$, $\mathcal{H}$, $\mathcal{L}$, $\mathcal{P}_{2l}$ означают алгоритмы Штрассена, Хопкрофта, Ладермана и Пана, соответственно (точнее, соответствующие алгоритмы, вычисляющие тензоры $\langle 2,2,2\rangle$, $\langle 2,3,3\rangle$, $\langle 3,3,3\rangle$, $\langle 2l,2l,2l\rangle$). Доказана следующая теорема.

Теорема 1. *Имеют место изоморфизмы*

$$\mathrm{Aut}(\mathcal{S}) \cong S_3 \times S_3\,, \quad \mathrm{Aut}(\mathcal{H}) \cong S_3 \times Z_2\,,$$

$$\mathrm{Aut}(\mathcal{L}) \cong S_4\,, \quad \mathrm{Aut}(\mathcal{P}_{2l}) \cong S_l \times Z_2 \times S_3\,.$$

(Конечно, указанные группы автоморфизмов найдены в явном виде, а не только с точностью до изоморфизма.)

В ходе исследования найдена группа изотропии $\Gamma(t)$, где $t = \langle m,n,p\rangle$, для любых m, n, p.

Теорема 2. *Пусть $\Gamma(t)$ — группа изотропии тензора $t = \langle m,n,p\rangle$, и $\Gamma^0(t)$ — подгруппа элементов $g \in \Gamma(t)$, сохраняющих факторы произведения $L_1 \otimes L_2 \otimes L_3$ (т.е. вида $g = g_1 \otimes g_2 \otimes g_3$, $g_i \in GL(L_i)$). Тогда $\Gamma^0(t)$ совпадает с группой всех преобразований вида*

$$T(a,b,c) : x_1 \otimes x_2 \otimes x_3 \mapsto ax_1b^{-1} \otimes bx_2c^{-1} \otimes cx_3a^{-1}\,,$$

где $x_i \in L_i$, $a \in GL_m(K)$, $b \in GL_n(K)$, $c \in GL_p(K)$. Факторгруппа $\Gamma(t)/\Gamma^0(t)$ изоморфна одной из групп 1, Z_2 или S_3.

Конечно, гораздо более важной, чем теорема 1, является следующая

Обратная задача. Для данной подгруппы $G \leq \Gamma(t)$ и $r \geq 1$ описать все G-инвариантные алгоритмы длины r, вычисляющие t.

(Именно в ходе решения задач такого вида и возможно было бы найти новые алгоритмы).

Литература

1. Bürgisser P., Clausen M., Shokrollahi M. A. *Algebraic Complexity Theory.* Springer, 1997.

2. Strassen V. *Gaussian elimination is not optimal* // Numer. Math. 1969. V. 13. № 4. P. 354–356.

3. Hopcroft J. E., Kerr L. R. *On minimizing the number of multiplications necessary for matrix multiplication* // SIAM J. Appl. Math. 1971. V. 20. P. 30–36.

4. Laderman J. *A noncommutative algorithm for multiplying* 3×3 *matrices using 23 multiplications* // Bull. Amer. Math. Soc. 1976. V. 82. P. 180–182.

5. Pan V. Ya. *Strassen algorithm is not optimal. Trilinear technique of aggregating, uniting and cancelling for constructing fast algorithms for matrix multiplication* // Proc. 19th Annual conference on Foundations of Computer Science, Ann Arbor, 1979. P. 166–176.

ДИАГОНАЛИЗУЕМЫЕ КОРНИ МАТРИЧНЫХ ПОЛИНОМОВ НАД КОНЕЧНЫМИ ПОЛЯМИ

Ф.Б. Буртыка

Южный федеральный университет
Большая Садовая 105/42, 344006 Ростов-на-Дону, Россия
bbfilipp@ya.ru

Рассмотрим матричные полиномы следующего вида:

$$\mathcal{F}(X) = \mathbf{F}_d \cdot X^d + \mathbf{F}_{d-1} \cdot X^{d-1} + \cdots + \mathbf{F}_2 \cdot X^2 + \mathbf{F}_1 \cdot X + \mathbf{F}_0 \in \mathbb{Z}_p^{N\times N}[X], \quad (1)$$

где $\mathbf{F}_i \in \mathbb{Z}_p^{N\times N}$ – коэффициенты и $X \in \mathbb{Z}_p^{N\times N}$ – переменная, являющиеся матрицами, состоящими из элементов кольца вычетов $\mathbb{Z}_p$ по модулю простого числа p, $p > 2$. Корнем (1) называется матрица $\mathbf{S} \in \mathbb{Z}_p^{N\times N}$ такая, что $\mathcal{F}(\mathbf{S}) = \mathbf{0}$, где $\mathbf{0} \in \mathbb{Z}_p^{N\times N}$ – нулевая матрица. Нахождение корней матричных полиномов $\in \mathbb{Z}_p^{N\times N}[X]$ имеет приложения в криптографии, например, анализ криптостойкости ПГШ на матричных полиномах [1-3] или отыскание периодов полилинейных рекуррентных регистров сдвига [4].

Для поиска корней (1) можно, к примеру, *свести его к системе скалярных алгебраических уравнений* над $\mathbb{Z}_p$. Данный метод был рассмотрен в [5] на примере матричных полиномов над $\mathbb{Z}_2$, однако он является неэффективным, так как система скалярных уравнений имеет большие размеры и является труднорешаемой.

Другой метод поиска корней (1) основан на работе с *полиномиальными матрицами*. С его помощью можно найти все корни, являющиеся диагонализируемыми матрицами. Данный метод был рассмотрен в [6,7] для матричных полиномов над полем комплексных чисел $\mathbb{C}$. В данной работе рассматривается вопрос о его переносимости на случай $\mathbb{Z}_p$. Напомним некоторые необходимые определения из [6].

Определение 1. Диагонализируемыми корнями (1) называются корни $\mathbf{S} \in \mathbb{Z}_p^{N\times N}$, представимые в виде $\mathbf{S} = \mathbf{V} \cdot \mathbf{D} \cdot \mathbf{V}^{-1}$, где $\mathbf{V} \in \mathbb{Z}_p^{N\times N}$ – обратимая матрица, $\mathbf{D} \in \mathbb{Z}_p^{N\times N}$ – диагональная матрица.

Определение 2. Полиномиальной матрицей, соответствующей матричному полиному (1), называется $\mathcal{F}(x) = \mathbf{F}_d \cdot x^d + \mathbf{F}_{d-1} \cdot x^{d-1} + \cdots + \mathbf{F}_2 \cdot x^2 + \mathbf{F}_1 \cdot x + \mathbf{F}_0 \in \mathbb{Z}_p^{N\times N}[x]$, где $\mathbf{F}_i \in \mathbb{Z}_p^{N\times N}$ – коэффициенты, $x \in \mathbb{Z}_p$ – скалярная переменная (т.е. в полиномиальной матрице элемент с индексами i, j – это полином, коэффициенты которого взяты из i, j-х элементов матриц-коэффициентов матричного полинома при соответствующих степенях).

Определение 3. Латентным корнем $\mathcal{F}(x) \in \mathbb{Z}_p^{N\times N}[x]$ называется такое $\lambda \in \mathbb{Z}_p$, что $det(\mathcal{F}(\lambda)) = 0$, где $d(x) = det(\mathcal{F}(x)) \in \mathbb{Z}_p[x]$ – скалярный полином степени $d \cdot N$.

Определение 4. Латентным вектором, соответствующим латентному корню $\lambda \in \mathbb{Z}_p$ полиномиальной матрицы $\mathcal{F}(x)$, называется вектор $\vec{v} \in Ker(\mathcal{F}(\lambda))$.

Теорема 1. *Пусть $\mathcal{F}(x) \in \mathbb{Z}_p^{N\times N}[x]$ имеет латентные корни $\lambda_1, ..., \lambda_N \in \mathbb{Z}_p$, такие что для $\forall \lambda_i, i \in \overline{1, N}$ существуют латентные векторы $\vec{v_i} \in \mathbb{Z}_p^N$, образующие линейно независимую систему векторов $\{\vec{v}_1, ..., \vec{v}_N\}$. Тогда*

$$\mathbf{S} = \mathbf{V} \cdot diag(\lambda_1, ..., \lambda_N) \cdot \mathbf{V}^{-1} \in \mathbb{Z}_p^{N\times N} \quad (2)$$

является корнем матричного полинома $\mathcal{F}(X) \in \mathbb{Z}_p^{N\times N}[X]$, где $\mathbf{V} \in \mathbb{Z}_p^{N\times N}$ — матрица, i -й столбец которой равен $\vec{v}_i$, $diag(\lambda_1, ..., \lambda_N)$ – диагональная матрица со значениями λ_i на диагонали.

Теорема 1 была доказана в [6] для поля комплексных чисел $\mathbb{C}$. Однако легко проверить, что она выполняется и для $\mathbb{Z}_p$. Действительно, она просто следует из того, что все собственные числа и векторы любого корня $\mathbf{S} \in \mathbb{Z}_p^{N\times N}$ полинома $\mathcal{F}(X) \in \mathbb{Z}_p^{N\times N}[X]$ являются латентными корнями и векторами соответственно для $\mathcal{F}(x)$.

Данная теорема дает алгоритм поиска всех диагонализируемых корней $\mathcal{F}(X)$. Сначала необходимо найти все корни $\lambda_1, ..., \lambda_t$ скалярного полинома $det(\mathcal{F}(x)) \in \mathbb{Z}_p[x]$, затем для $\forall i \in \overline{1,t}$ вычисляется $Ker(\mathcal{F}(\lambda_i))$. Из векторов $\in Ker(\mathcal{F}(\lambda_i))$ и λ_i строятся различные комбинации в соответствии с формулой (2) и получаются, соответственно, различные корни (1).

Рассмотрим вопрос о количестве диагонализируемых корней.

Теорема 2. *Пусть $\mathcal{F}(x) \in \mathbb{Z}_p^{N\times N}[x]$ с $deg(\mathcal{F}) = d$ имеет t латентных корней $\lambda_1, ..., \lambda_t$ таких, что $\lambda_i \neq \lambda_j$ для $i \neq j$, $N \leq t \leq N \cdot d$. И пусть $\forall\lambda_i$ соответствует одномерное подпространство латентных векторов $V_i = Lin\{\vec{v}_i\}$. Тогда количество диагонализируемых корней $\mathcal{F}(X) \in \mathbb{Z}_p^{N\times N}[X]$ не превосходит $C_{d\cdot N}^N$.*

Теорема 3. *Пусть $\mathcal{F}(x) \in \mathbb{Z}_p^{N\times N}[x]$ с $deg(\mathcal{F}) = d$ имеет латентные корни $\lambda_1, ..., \lambda_{d\cdot N}$ такие, что $\lambda_i \neq \lambda_j$ для $i \neq j$. И пусть $\forall\lambda_i$ соответствует одномерное подпространство латентных векторов $V_i = Lin\{\vec{v}_i\}$ таких, что любой набор векторов $\{\vec{v}_{i_1}, ..., \vec{v}_{i_N}\}$ является линейно независимым. Тогда все корни $\mathcal{F}(X) \in \mathbb{Z}_p^{N\times N}[X]$ являются диагонализируемыми, и их количество $= C_{d\cdot N}^N$. Других корней (1) не имеет.*

Матричные полиномы $\mathcal{F}(X) \in \mathbb{Z}_p^{N\times N}[X]$, для которых выполнено условие из теоремы 3, – это, так называемые, *полиномы общего положения* [7]. Они имеют *только* диагонализируемые решения. Матричные полиномы же, не находящиеся в случае общего положения, могут иметь недиагонализируемые решения, которые необходимо искать отдельно.

Отметим, что в [6-7] утверждения теорем 2 и 3 обосновывались для случая поля $\mathbb{C}$. В данной работе установлено, что они также справедливы и для $\mathbb{Z}_p$.

Установлена также следующая теорема.

Теорема 4. *Пусть $\mathcal{F}(x) \in \mathbb{Z}_p^{N\times N}[x]$ имеет латентные корни $\lambda_1, ..., \lambda_N$, где $\lambda_i \neq \lambda_j$. И пусть $\exists\lambda_j$ с k-мерным подпространством латентных векторов $\mathtt{V}_j = Lin\{\vec{v}_{j,1}, ..., \vec{v}_{j,k}\}$. А остальным $\lambda_i, i \neq j$ пусть соответствуют одномерные подпространства латентных векторов $\mathtt{V}_i = Lin\{\vec{v}_i\}$. И пусть выполняется $\mathtt{V}_j \cap Lin\{\vec{v}_1, ..., \vec{v}_{j-1}, \vec{v}_{j+1}..., \vec{v}_N\} = \emptyset$. Тогда количество диагонализируемых корней (1) $< p^k - k \cdot (p-1)$.*

Заметим, что в случае поля $\mathbb{C}$ матричный полином, удовлетворяющий условиям теоремы 4, будет иметь бесконечное число корней.

Работа выполнена при финансовой поддержке гранта РФФИ №15-07-00597 А.

Литература

1. Буртыка Ф. Б. *Симметричное полностью гомоморфное шифрование с использованием неприводимых матричных полиномов.* // Известия Южного федерального университета. Технические науки, 2014. Т. 157. № 8. С. 107–122.

2. Burtyka Ph. B., Makarevich O. B. *Symmetric fully homomorphic encryption using decidable matrix equations.* // Proceedings of the 7th International Conference on Security of Information and Networks, ACM, 2014. P. 186–197.

3. Буртыка Ф. Б. *Пакетное симметричное полностью гомоморфное шифрование на основе матричных полиномов.* // Труды Института системного программирования РАН. 2014. Т. 26. № 5. С. 99-115.

4. Гольтваница М. А., Зайцев С. Н., Нечаев А. А. *Скрученные линейные рекурренты максимального периода над кольцами Галуа* //Фундаментальная и прикладная математика. 2012. Т. 17. № 3. С. 5–23.

5. Буртыка Ф. Б. *О сложности нахождения корней булевых матричных полиномов* // Математическое моделирование. 2015. Т. 27.

6. Dennis, Jr J. E., Traub J. F., Weber R. P. *The algebraic theory of matrix polynomials* //SIAM Journal on Numerical Analysis. 1976. Т. 13. № 6. С. 831–845.

7. Гельфанд С. И. *О числе решений квадратного уравнения* // Общематематический семинар Глобус. Выпуск 1. НМУ. МЦНМО. 2004. С. 124–133.

НАСЫЩЕННЫЕ ФОРМАЦИИ И ВЗАИМНО ПЕРЕСТАНОВОЧНЫЕ ПРОИЗВЕДЕНИЯ КОНЕЧНЫХ ГРУПП

А.Ф. Васильев[1], **Т.И. Васильева**[2], **Д.Н. Симоненко**[2]

[1]Гомельский государственный университет им. Ф. Скорины, Советская 104, 246019 Гомель, Беларусь
formation56@mail.ru
[2]Белорусский государственный университет транспорта, Кирова 34, 246653 Гомель, Беларусь
tivasilyeva@mail.ru, dsimonenkon@mail.ru

Рассматриваются только конечные группы. Класс групп, замкнутый относительно взятия гомоморфизмов и подпрямых произведений, называется формацией.

Пусть $\mathfrak{F}$ — некоторая формация. Нахождение условий, при которых $\mathfrak{F}$ содержит всякую группу $G = AB$, где $A \in \mathfrak{F}$ и $B \in \mathfrak{F}$, является классической задачей. Еще в 1938 году Фиттинг [1] доказал нильпотентность группы, являющейся произведением своих нормальных нильпотентных подгрупп. Этот результат послужил основой последующих многочисленных исследований по изучению формаций, замкнутых относительно произведений заданных $\mathfrak{F}$-подгрупп. В 1972 году Брайс и Косси [2] получили конструктивное описание всех разрешимых наследственных формаций $\mathfrak{F}$, содержащих всякую группу G, представимую в произведение своих нормальных $\mathfrak{F}$-подгрупп. В работе [4] Амберг, Л. С. Казарин, Хёфлинг нашли наследственные формации $\mathfrak{F}$, замкнутые относительно произведений произвольных $\mathfrak{F}$-подгрупп. В работах [5], [6] в классе всех разрешимых групп было получено описание нормально наследственных насыщенных формаций $\mathfrak{F}$, содержащих всякую группу $G = AB$, где A и B — абнормальные (контрнормальные, т.е. $A^G = G = B^G$) $\mathfrak{F}$-подгруппы в G.

В последние годы активно изучаются произведения групп, у которых факторы связаны определенными условиями перестановочности для подгрупп.

Согласно [7, с. 151] группа $G = AB$ называется произведением взаимно перестановочных подгрупп A и B, если A перестановочна с каждой подгруппой из B и B перестановочна с каждой подгруппой из A. Более того, если каждая подгруппа из A перестановочна с каждой подгруппой из B, то группа $G = AB$ называется произведением тотально перестановочных подгрупп A и B. В работе [8] Асаад и Шаалан показали, что группа $G = AB$, где A и B — тотально перестановочные сверхразрешимые подгруппы G, сама является сверхразрешимой. Этот результат послужил основой исследований в [9], [10] (см. также [7]) по нахождению формаций $\mathfrak{F}$, замкнутых относительно произведений тотально перестановочных подгрупп. Отметим следующий результат из [10].

Пусть $\mathfrak{F}$ — формация, содержащая класс всех сверхразрешимых групп. Тогда $\mathfrak{F}$ содержит всякую группу $G = AB$, где A и B — тотально перестановочные сверхразрешимые подгруппы группы G.

Для краткости формулировок введем

Определение. Пусть $\mathfrak{F}$ и $\mathfrak{X}$ — классы групп, причем $\mathfrak{F} \subseteq \mathfrak{X}$. Класс $\mathfrak{F}$ назовем MP-замкнутым в $\mathfrak{X}$, если $\mathfrak{F}$ содержит всякую $\mathfrak{X}$-группу $G = AB$, где A и B — взаимно перестановочные $\mathfrak{F}$-подгруппы группы G.

Пустой класс будем считать MP-замкнутым в любом классе $\mathfrak{X}$.

В случае, когда $\mathfrak{X} = \mathfrak{G}$ — класс всех групп, класс $\mathfrak{F}$ будем называть MP-замкнутым. Если $\mathfrak{X} = \mathfrak{S}$ — класс всех разрешимых групп, то $\mathfrak{F}$ будем называть разрешимым MP-замкнутым классом.

Известно немного примеров формаций, замкнутых относительно взятия взаимно перестановочных произведений подгрупп (см. [7]). В частности, MP-замкнутыми являются формации всех π-групп, формации всех разрешимых π-групп, формации всех дисперсивных по Оре групп и некоторые др.

Возникает следующая

Проблема. *Пусть $\mathfrak{F}$ — формация (класс Фиттинга, класс Шунка) и $\mathfrak{X}$ — класс групп, причем $\mathfrak{F} \subseteq \mathfrak{X}$. Для данного класса $\mathfrak{X}$ описать все формации (классы Фиттинга, классы Шунка) $\mathfrak{F}$, MP-замкнутые в $\mathfrak{X}$.*

В настоящем сообщении данная проблема исследуется в случае, когда $\mathfrak{F}$ — насыщенная формация, а $\mathfrak{X}$ — класс всех групп.

Напомним, что формация $\mathfrak{F}$ называется насыщенной, если из $G/\Phi(G) \in \mathfrak{F}$ всегда следует, что $G \in \mathfrak{F}$.

Многие классические формации являются насыщенными, например, формации всех нильпотентных, всех сверхразрешимых, всех разрешимых групп и др. Гашюц [11] ввел понятие локальной формации, которое позволяет конструировать насыщенные формации. Согласно известной теореме Любезедер-Шмида семейства всех насыщенных и всех локальных формаций совпадают (см. [12, гл. IV]).

Теорема. *Пусть $\mathfrak{F}$ — насыщенная формация, содержащая все сверхразрешимые π-группы для $\pi = \pi(\mathfrak{F})$, и F — максимальный внутренний локальный экран $\mathfrak{F}$. Формация $\mathfrak{F}$ является MP-замкнутой тогда и только тогда, когда формация $F(p)$ MP-замкнута для любого простого p.*

Из теоремы получается следующий известный результат (см. [7, с. 162]).

Следствие 1. *Пусть группа $G = AB$ — произведение взаимно перестановочных подгрупп A и B. Если A и B дисперсивны по Оре, то G дисперсивна по Оре.*

В работе [13] В. С. Монахов исследовал класс всех групп, у которых любая подгруппа Шмидта является сверхразрешимой. Им было показано, что такой класс является насыщенной наследственной формацией Фиттинга, содержащей все сверхразрешимые группы.

Следствие 2. *Пусть группа $G = AB$ — произведение взаимно перестановочных подгрупп A и B. Если в A и B любая подгруппа Шмидта является сверхразрешимой, то любая подгруппа Шмидта группы G сверхразрешима.*

Отсюда вытекает следующий хорошо известный результат.

Следствие 3. *Если группа $G = AB$ — произведение взаимно перестановочных нильпотентных подгрупп A и B, то G сверхразрешима.*

Литература

1. Fitting H. *Beiträge zur Theorie der endlichen Gruppen* // Jahresber. Deutsch. Math.-Verein. 1938. Bd. 48. S. 77–141.

2. Bryce R. A., Cossey J. *Fitting formations of finite soluble groups* // Math. Z. 1972. Bd. 127. № 3. S. 217–233.

3. Hawkes T. O. *On Fitting formations* // Math. Z. 1970. V. 117. № 1–4. P. 177–182.

4. Амберг Б., Казарин Л. С., Хефлинг Б. *Конечные группы с кратными факторизациями* // Фундамент. и прикл. матем. 1998. Т. 4. Вып. 4. С. 1251–1263.

5. Васильев, А. Ф. *Об абнормально факторизуемых конечных разрешимых группах* // Украинский матем. журн. 2002. Т. 54. № 9. С. 1163–1171.

6. Vasil'ev A. F. *On Products of Nonnormal Subgroups of Finite Groups* // Acta Applicandae Mathematicae. 2005. V. 85. № 1. P. 305–311.

7. Ballester-Bolinches A., Esteban-Romero R., Asaad M. *Products of Finite Groups.* Berlin-New; York: Walter de Gruyter, 2010.

8. Asaad M., Shaalan A. *On the supersolubility of finite groups* // Arch. Math. 1989. V. 53. № 4. P. 318–326.

9. Maier R. *A completeness property of certain formations*// Bull. London Math. Soc. 1992. V. 24. P. 540–544.

10. Ballester-Bolinches A., Pérez-Ramos M. D. *A question of R. Maier concerning formations* // J. Algebra. 1996. V. 182. P. 738–747.

11. Gaschütz W. *Zur Theorie der endlichen auflösbaren Gruppen* // Math. Z. 1963. Bd. 80. № 4. S. 300–305.

12. Doerk K., Hawkes T. *Finite soluble groups.* Berlin-New; York: Walter de Gruyter, 1992.

13. Монахов В. С. *О конечных группах с заданным набором подгрупп Шмидта* // Матем. заметки. 1995. Т. 58. Вып. 5. С. 717–722.

ПОПАРНО ПЕРЕСТАНОВОЧНЫЕ ПРОИЗВЕДЕНИЯ И K-$\mathbb{P}$-СУБНОРМАЛЬНЫЕ ПОДГРУППЫ КОНЕЧНЫХ ГРУПП

А.С. Вегера

Гомельский государственный университет имени Ф. Скорины, Советская 104, 246019 Гомель, Беларусь
artem.vegera@gmail.com

Рассматриваются только конечные группы. О. Кегелем в работе [1] было предложено определение $\mathfrak{F}$-достижимой (согласно современной терминологии [2] K-$\mathfrak{F}$-субнормальной) подгруппы.

Пусть $\mathfrak{F}$ — непустая формация. Подгруппа H группы G называется K-$\mathfrak{F}$-субнормальной в G, если существует цепь подгрупп $H = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_{n-1} \subseteq H_n = G$ такая, что либо H_{i-1} нормальна в H_i, либо $H_i^{\mathfrak{F}} \subseteq H_{i-1}$ для любого $i = 1, \ldots, n$.

Следуя идее О. Кегеля, в работе [3] было введено следующее

Определение 1. Подгруппа H группы G называется K-$\mathbb{P}$-субнормальной в G (обозначается H K-$\mathbb{P}$-*sn* G), если существует цепь подгрупп $H = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_{n-1} \subseteq H_n = G$ такая, что либо H_{i-1} нормальна в H_i, либо $|H_i : H_{i-1}|$ есть простое число для любого $i = 1, \ldots, n$.

Если $H = G$ или в указанной выше цепи индекс $|H_i : H_{i-1}|$ — простое число для любого $i = 1, \ldots, n$, то H называется $\mathbb{P}$-субнормальной в G [4].

Очевидно, что всякая субнормальная подгруппа является K-$\mathbb{P}$-субнормальной. Обратное утверждение в общем случае неверно [3].

Свойства $\mathbb{P}$-субнормальных и K-$\mathbb{P}$-субнормальных подгрупп и их приложения к изучению произведений $G = AB$ были рассмотрены в работах [3-5].

В настоящем сообщении изучается влияние K-$\mathbb{P}$-субнормальности на строение групп $G = G_1G_2 \cdots G_n$, представимых в произведение своих попарно перестановочных подгрупп G_1, G_2, $\ldots$, G_n.

Определение 2 [3]. Группа G называется $\overline{\mathfrak{w}}$-сверхразрешимой, если любая ее силовская подгруппа является K-$\mathbb{P}$-субнормальной в G.

В [3] было установлено, что класс всех $\overline{\mathfrak{w}}$-сверхразрешимых групп образует наследственную насыщенную формацию и состоит из дисперсивных по Оре групп.

Теорема 1. *Пусть $G = G_1G_2 \cdots G_n$ — произведение разрешимых попарно перестановочных подгрупп G_1, G_2, $\ldots$, G_n. Если подгруппы G_i K-$\mathbb{P}$-*sn* G_iG_j и G_j K-$\mathbb{P}$-*sn* G_iG_j для любых $i, j \in \{1, 2, \ldots n\}$, то G разрешима.*

Следствие 1 [3]. *Пусть $G = AB$ — произведение разрешимых подгрупп A и B. Если A K-$\mathbb{P}$-*sn* G и B K-$\mathbb{P}$-*sn* G, то G разрешима.*

Теорема 2. *Пусть $G = G_1G_2 \cdots G_n$ — произведение попарно перестановочных сверхразрешимых подгрупп G_1, G_2, $\ldots$, G_n. Если для любой пары $i, j \in \{1, 2, \ldots n\}$, где $i \neq j$, подгруппа G_i K-$\mathbb{P}$-*sn* G_iG_j, подгруппа G_j K-$\mathbb{P}$-*sn* G_iG_j и коммутант группы G нильпотентет, то G сверхразрешима.*

Согласно [6] и [7] группа $G = AB$ называется произведением взаимно перестановочных (взаимно *sn*-перестановочных) подгрупп A и B, если A перестановочна с любой (соответственно, субнормальной) подгруппой из B, а B перестановочна с любой (соответственно, субнормальной) подгруппой из A.

Следствие 2 [8, с. 166]. *Пусть $G = G_1G_2 \cdots G_n$ — произведение попарно взаимно sn-перестановочных (взаимно перестановочных) сверхразрешимых подгрупп G_1, G_2, $\ldots$, G_n. Если коммутант группы G нильпотентет, то G сверхразрешима.*

Теорема 3. *Пусть $G = G_1G_2\cdots G_n$ — произведение попарно перестановочных $\overline{\mathrm{w}}$-сверхразрешимых подгрупп G_1, G_2, ..., G_n. Если для любой пары $i, j \in \{1, 2, \dots n\}$, где $i \neq j$, подгруппа G_i K-$\mathbb{P}$-sn G_iG_j, подгруппа G_j K-$\mathbb{P}$-sn G_iG_j и индексы $|G_iG_j : G_i|$ и $|G_iG_j : G_j|$ взаимно просты, то G $\overline{\mathrm{w}}$-сверхразрешима.*

Следствие 3 [9]. *Пусть $G = G_1G_2\cdots G_n$ — произведение попарно взаимно sn-перестановочных (взаимно перестановочных) $\overline{\mathrm{w}}$-сверхразрешимых подгрупп G_1, G_2, ..., G_n. Если для любой пары $i, j \in \{1, 2, \dots n\}$, где $i \neq j$, индексы $|G_iG_j : G_i|$ и $|G_iG_j : G_j|$ взаимно просты, то G $\overline{\mathrm{w}}$-сверхразрешима.*

Литература

1. Kegel O. H. *Untergruppenverbände endlicher Gruppen, die den Subnormalteilerverband echt enthalten* // Arch. Math. 1978. Bd. 30. № 3. S. 225–228.

2. Ballester-Bolinches A., Ezquerro L. M. *Classes of Finite Groups.* Dordrecht: Springer, 2006.

3. Васильев А. Ф., Васильева Т. И., Тютянов В. Н. *О* K-$\mathbb{P}$-*субнормальных подгруппах конечных групп* // Матем. заметки. 2014. Т. 95. № 4. С. 517–528.

4. Васильев А. Ф., Васильева Т. И., Тютянов В. Н. *О конечных группах сверхразрешимого типа* // Сиб. мат. журн. 2010. Т. 51. № 6. С. 1270–1281.

5. Васильев А. Ф., Васильева Т. И., Тютянов В. Н. *О произведениях $\mathbb{P}$-субнормальных подгрупп в конечных группах* // Сиб. мат. журн. 2012. Т. 53. № 1. С. 59–67.

6. Assad M., Shaalan A. *On the supersolubility of finite groups* // Arch. Math. 1989. V. 53. № 4. P. 318–326.

7. Alejandre M., Ballester-Bolinches A., Cossey J., Pedraza-Aguilera M. *On some permutable products of supersoluble groups* // Rev. Mat. Iberoamericana. 2004. V. 20. P. 413–425.

8. Ballester-Bolinches A., Esteban-Romero R., Asaad M. *Products of Finite Groups.* Berlin-New; York: Walter de Gruyter, 2010.

9. Ballester-Bolinches A., Ezquerro L. M., Heliel A. A., Al-Shomrani M. M. *Some Results on Products of Finite Groups* // Bull. Malays. Math. Sci. Soc. 2015. DOI 10.1007/s40840-015-0111-7.

О СВОЙСТВЕ РЕШЕТОЧНОГО ОБЪЕДИНЕНИЯ π-РАЗРЕШИМЫХ ФИТТИНГОВЫХ ФУНКТОРОВ

Е.А. Витько

Витебский государственный университет имени П.М. Машерова
Московский пр-т 33, 210038 Витебск, Беларусь alenkavit@tut.by

В определениях и обозначениях мы следуем [1].

Все рассматриваемые в работе группы конечны.

Пусть $\mathfrak{X}$ — некоторый непустой класс Фиттинга. Отображение f, которое каждой группе $G \in \mathfrak{X}$ ставит в соответствие некоторое непустое множество ее подгрупп $f(G)$, называется [2] фиттинговым $\mathfrak{X}$-функтором, если выполняются следующие условия:

(i) если $\alpha : G \to \alpha(G)$ — изоморфизм, то $f(\alpha(G)) = \{\alpha(X) : X \in f(G)\}$;

(ii) если $N \trianglelefteq G$, то $f(N) = \{X \cap N : X \in f(G)\}$.

Фиттингов $\mathfrak{X}$-функтор называется:

1) π-разрешимым, если $\mathfrak{X} = \mathfrak{S}^\pi$ — класс всех π-разрешимых групп;

2) сопряженным, если для каждой группы $G \in \mathfrak{X}$ множество $f(G)$ есть класс сопряженных подгрупп группы G;

3) π-связанным, если каждая подгруппа $X \in f(G)$ является π-связанной подгруппой группы $G \in \mathfrak{X}$;

4) пронормальным, если каждая подгруппа $X \in f(G)$ является пронормальной в группе $G \in \mathfrak{X}$.

Фиттинговы π-разрешимые функторы f и g называются перестановочными, если $XY = YX$ для любых подгрупп $X \in f(G)$ и $Y \in g(G)$ таких, что существует холловская система группы G, которая редуцируется в X и в Y.

Пусть f — фиттингов $\mathfrak{X}$-функтор. Тогда $\mathrm{Char} f$ — множество всех простых чисел p, для которых существует группа $G \in \mathfrak{X}$ и подгруппа $X \in f(G)$ такие, что число p является делителем $|X|$. Множество $\mathrm{Char} f$ называется характеристикой функтора f.

Определение. Пусть $\{f_i : i \in I\}$ — множество пронормальных сопряженных попарно перестановочных π-разрешимых π-связанных фиттинговых функторов и $\mathrm{Char} f_i \cap \mathrm{Char} f_j = \emptyset$ для всех $i, j \in I$, если $i \neq j$. Определим операцию $\vee$ следующим образом: $(\vee_{i\in I} f_i)(G) = \{\prod_{i\in I} X_i : X_i \in f_i(G)$, существует холловская система группы G, которая редуцируется в подгруппу X_i для всех $i \in I\}$.

Пусть f — сопряженный фиттингов $\mathfrak{X}$-функтор. Тогда f^* — отображение, которое каждой группе $G \in \mathfrak{X}$ сопоставляет множество $\{\pi_1(T) : T \in f(G \times G)\}$, где π_1 — проекция подгруппы T на первую компоненту.

Теорема. *Пусть $\{f_i : i \in I\}$ — множество пронормальных сопряженных попарно перестановочных π-разрешимых π-связанных фиттинговых функторов, $Char f_i \cap Char f_j = \emptyset$ для всех $i, j \in I$, если $i \neq j$. Тогда $(\vee_{i\in I} f_i)^* = \vee_{i\in I} f_i^*$.*

Литература

1. Doerk K. *Finite Soluble Groups.* Berlin New York : Walter de Gruyter, 1992.

2. Витько Е. А., Воробьев Н. Т. *Фиттинговы функторы и радикалы конечных групп* // Сиб. матем. журнал. 2011. Т. 52. № 6. С. 1253–1263.

ОБ АЛГЕБРАИЧЕСКИХ РЕШЕТКАХ ФОРМАЦИЙ КОНЕЧНЫХ ГРУПП

Н.Н. Воробьев[1], **А.Р. Кузнецова**[2]

Учреждение образования "Витебский государственный университет им. П.М. Машерова",
кафедра алгебры и методики преподавания математики,
Московский проспект 33, 210038 Витебск, Беларусь
[1]vornic2001@mail.ru, [2]anyakuznetsovar@gmail.com

Все рассматриваемые группы конечны. Мы будем использовать стандартную терминологию из [1, 2].

Напомним, что формацией называется класс групп, который замкнут относительно взятия гомоморфных образов и конечных подпрямых произведений. Совокупность классов групп Θ называется полной решеткой формаций [2], если пересечение любой совокупности формаций из Θ снова принадлежит Θ, и во множестве Θ имеется такой класс $\mathfrak{F}$, что $\mathfrak{H} \subseteq \mathfrak{F}$ для любого другого класса $\mathfrak{H} \in \Theta$. Полная решетка формаций Θ называется частичной алгеброй формаций [2] (см. также [3]), если для любого простого числа p и для любой формации $\mathfrak{F} \in \Theta$ имеет место $\mathfrak{N}_p\mathfrak{F} \in \Theta$. Здесь символом $\mathfrak{N}_p$ обозначают класс всех p-групп. Как показано в монографии А.Н. Скибы [2] такие полные решетки и частичные алгебры играют при изучении классов групп ту же роль, что и сами классы (формации, классы Фиттинга и др.) при изучении групп. Нетрудно показать, что класс всех тотально насыщенных формаций l_∞, а при фиксированном $n \geqslant 0$ класс всех n-кратно насыщенных формаций l_n являются частичными алгебрами (см. подробнее [2]).

Элемент a полной решетки L называется компактным, если из неравенства $a \leqslant \vee(x_i \mid i \in I)$ следует, что $a \leqslant x_{i_1} \vee x_{i_2} \vee \ldots \vee x_{i_n}$, где $i_1, i_2, \ldots, i_n \in I$, для некоторого натурального n. Полная решетка формаций называется алгебраической, если каждый ее элемент может

быть представлен в виде решеточного объединения подходящего семейства компактных элементов.

Основной результат представляет следующая

Теорема. *Всякая частичная алгебра формаций является алгебраической решеткой.*

Следствие 1 (А.Н. Скиба [2]). *Решетка всех τ-замкнутых n-кратно насыщенных формаций l_n^τ алгебраична.*

Следствие 2. *Решетка n-кратно насыщенных формаций l_n алгебраична.*

Следствие 3 (В.Г. Сафонов [4]). *Решетка всех τ-замкнутых тотально насыщенных формаций l_∞^τ алгебраична.*

Следствие 4. *Решетка тотально насыщенных формаций l_∞ алгебраична.*

Литература

1. Шеметков Л. А. *Формации конечных групп.* М.: Наука, 1978.

2. Скиба А. Н. *Алгебра формаций.* Мн.: Беларуская навука, 1997.

3. Воробьев Н. Н. *Алгебра классов конечных групп.* Витебск: ВГУ имени П.М. Машерова, 2012.

4. Сафонов В. Г. *Об алгебраичности решетки τ-замкнутых тотально насыщенных формаций* // Алгебра и логика. 2006. Т. 45. № 5. С. 620–626.

ИНЪЕКТОРЫ КОНЕЧНЫХ ГРУПП

Н.Т. Воробьев[1], **М.Г. Семёнов**[2]

Витебский государственный университет имени П.М. Машерова
Московский проспект 33, 210038 Витебск, Беларусь
[1]vorobyovnt@tut.by, [2]mg-semenow@mail.ru

Значительный прогресс в развитии неарифметической силовской теории конечных групп был достигнут в работе Гашюца, Фишера и Хартли [1], где установлено, что для любого класса Фиттинга $\mathfrak{F}$ в любой конечной разрешимой группе существуют $\mathfrak{F}$-инъекторы и любые два из них сопряжены. Напомним, что класс групп $\mathfrak{F}$ называют классом Фиттинга, если $\mathfrak{F}$ замкнут относительно взятия нормальных подгрупп и произведений нормальных $\mathfrak{F}$-подгрупп. При этом подгруппа V группы G называется $\mathfrak{F}$-инъектором G, если $V \bigcap N$ является $\mathfrak{F}$-максимальной подгруппой в N для любой субнормальной подгруппы N из G. Локализуя понятие класса Фиттинга, Л.А. Шеметков определил в [2] множество Фиттинга конечной группы, как непустое множество $\mathcal{F}$ её подгрупп, которое замкнуто относительно взятия нормальных подгрупп, нормальных произведений и сопряжений. Понятие $\mathcal{F}$-инъектора для множества Фиттинга $\mathcal{F}$ определяется аналогично понятию $\mathfrak{F}$-инъектора для класса Фиттинга $\mathfrak{F}$. Заметим, что каждому классу Фиттинга $\mathfrak{F}$ соответствует множество Фиттинга $\mathcal{F} = \{H \leqslant G : H \in \mathfrak{F}\}$, хотя обратное в общем случае неверно (см. [3, пример VIII.2.2(b)]). Более того, в этом случае множество всех $\mathfrak{F}$-инъекторов и $\mathcal{F}$-инъекторов группы G совпадают. Поэтому, указанная выше теорема Гашюца-Фишера-Хартли является следствием теоремы Шеметкова [2] о том, что для любого множества Фиттинга $\mathcal{F}$ в конечной π-разрешимой группе (π – множество всех простых делителей порядков всех групп из $\mathcal{F}$) существуют $\mathcal{F}$-инъекторы и любые два из них сопряжены.

Пусть $\mathcal{F}$ – множество Фиттинга конечной группы G и $G_{\mathcal{F}}$ – наибольшая нормальная $\mathcal{F}$-подгруппа G. Можно показать, что если $\mathfrak{X}$ – класс Фиттинга, то $\mathcal{F} \bullet \mathfrak{X} = \{H \leqslant G : H/H_{\mathcal{F}} \in \mathfrak{X}\}$ является множеством Фиттинга G. Пусть π – некоторое множество простых чисел, π' – дополнение π во множестве всех простых чисел и $\mathfrak{E}_{\pi'}$ – класс Фиттинга всех π'-групп. Множество Фиттинга $\mathcal{F}$ группы G назовем π-насыщенным, если $\mathcal{F} = \mathcal{F} \bullet \mathfrak{E}_{\pi'}$. Нами доказана

Теорема 1. *В любой конечной π-разрешимой группе G для любого π-насыщенного множества Фиттинга $\mathcal{F}$ группы G существуют $\mathcal{F}$-инъекторы и любые два из них сопряжены.*

Пусть в дальнейшем $\pi = \sigma(\mathcal{F})$ – множество всех простых делителей порядков всех $\mathcal{F}$-подгрупп из множества Фиттинга $\mathcal{F}$ группы G и $\mathfrak{S}^\pi$ – класс всех π-разрешимых групп. Теоремы Шеметкова [2] и Баллестера-Болинше [4] о существовании и сопряженности $\mathcal{F}$-инъекторов являются специальными случаями следующего, доказанного нами, результата.

Теорема 2. *Пусть $\mathcal{F}$ – множество Фиттинга конечной группы G. Тогда если $G \in \mathcal{F}\bullet\mathfrak{S}^\pi$, то в G существуют $\mathcal{F}$-инъекторы и любые два из них сопряжены.*

Литература

1. Fischer B., Gaschütz W., Hartley B. *Injektoren endlicher auflösbarer Gruppen* // Math. Z. 1967. Bd. 102. S. 337–339.

2. Шеметков Л. А. *О подгруппах π-разрешимых групп* // В кн.: Конечные группы. Минск: Наука и техника, 1975. С. 207–212.

3. Doerk K., Hawkes T. O. *Finite Soluble Groups*. Berlin–New York : Walter de Gruyter & Co., 1992.

4. Ballester-Bolinches A., Ezquerro L. M. *Classes of finite groups*. Dordrecht : Springer, 2006.

ОБ ОДНОЙ ГИПОТЕЗЕ ТОМПСОНА ДЛЯ ЗНАКОПЕРЕМЕННЫХ ГРУПП

И.Б. Горшков

Институт математики и механики им. Н. Н. Красовского УРО РАН
Екатеринбург, Россия ilygor8@gmail.com

Пусть G конечная группа, $N(G)$ множество размеров классов сопряженных элементов группы G. В восьмидесятых годах прошлого столетия Томпсоном была сформулирована следующая гипотеза.

Гипотеза Томпсона.*Пусть L конечная неабелева простая группа, G конечная группа с тривиальным центром и $N(G) = N(L)$. Тогда $G \simeq L$.*

Обозначим через $\pi(G)$ множество всех простых делителей порядка группы G. Пусть $GK(G)$ — граф простых чисел группы G с множество вершин $\pi(G)$, и два простых числа p и q из $\pi(G)$ соединены ребром, если в G найдется элемент порядка pq. В настоящий момент справедливость гипотезы Томпсона доказана почти для всех конечных простых групп с несвязным графом простых чисел. В частности, Алави и Данешкхах (смотри [1]) доказали ее для знакопеременных групп степени p, $p+1$ и $p+2$, где p простое число большее 11. В работах [2−4] была доказана справедливость гипотезы для знакопеременных групп степени 10, 16 и 22, имеющих связный граф простых чисел. Однако вопрос о справедливости гипотезы для знакопеременных групп остается открытым. Пусть G конечная группа с тривиальным центром такая, что $N(G) = N(V_n)$, где V_n знакопеременная или симметрическая группа степени $n \geq 5$. Было доказано, что в G существует композиционный фактор H изоморфный знакопеременной группе степени $m \leq n$, где m больше либо равно максимального простого числа не превосходящего n. Также, было доказано, что максимальный простой делитель числа $|G|/|H|$ не превосходит $n/2$.

Литература

1. Alavi S.H., Daneshkhah A. *A new characterization of alternating and symmetric groups* // Journal of Applied Mathematics and Computing. 2005. Vol. 17. No. 1–2. P. 245–258.

2. Vasil'ev A.V. *On Thompson's conjecture* // Sibirskie Elektronnye Matematicheskie Izvestiya. 2009. Vol. 6. P. 457–464.

3. Gorshkov I.B. *Thompson's conjecture for simple groups with a connected prime graph* // Algebra and Logic. 2012. Vol. 51. No. 2. P. 111–127.

4. Xu M. *Thompson's conjecture for alternating group of degree 22* // Frontiers of Mathematics in China. 2013. Vol. 8. No. 5. P. 1227–1236.

О ВЕРХНЕЙ ОЦЕНКЕ ПЕРМАНЕНТОВ

Д.Б. Ефимов

Отдел математики Коми НЦ РАН, Чернова 3а, 167000 Сыктывкар, Россия dmefim@mail.ru

Вычисление перманентов имеет большую алгоритмическую сложность. Поэтому актуальной является задача их оценки. В данной работе мы рассматриваем верхние оценки перманентов произвольных вещественных матриц третьего порядка, опираясь на подход, предложенный Юркатом и Райзером в [1].

Определение 1. Алгеброй Пименова с n образующими назовем ассоциативную алгебру $P_n(\iota)$, порожденную над полем вещественных чисел единицей и элементами $\iota_k,\ k=1,\dots,n$, связанными определяющими соотношениями: $\iota_k^2=0$, $\iota_k\iota_l=\iota_l\iota_k$, $k,l=1,\dots,n$.

Из определения следует, что алгебра $P_n(\iota)$ является конечномерной размерности 2^n, коммутативной, обладает единицей, и каждый ее элемент однозначно представляется в следующем стандартном виде:

$$a=a_0+\sum_{t=1}^{n}\sum_{k_1<\dots<k_t} a_{k_1\dots k_t}\iota_{k_1}\dots\iota_{k_t},\quad a_0,a_{k_1\dots k_t}\in R.$$

Зафиксируем в алгебре $P_1(\iota)$ основной базис $\{1,\iota\}$. Тогда регулярному модулю $P_1(\iota)$ соответствует следующее двумерное матричное регулярное представление:

$$T: a_0+\iota a_1\to\begin{pmatrix} a_0 & 0\\ a_1 & a_0\end{pmatrix}.$$

В общем случае справедливо следущее утверждение.

Утверждение 1. *Если в алгебре $P_n(\iota)$ зафиксировать основной упорядоченный базис $\{1,\iota_1,\iota_2,\dots,\iota_1\iota_2\dots\iota_n\}$, то регулярному модулю $P_n(\iota)$ соответствует матричное представление, сопоставляющее каждому элементу $a\in P_n(\iota)$ $2^n\times 2^n$-матрицу $T(a)$, являющуюся нижнетреугольной, симметричной относительно второстепенной диагонали и с элементами a_0 на главной диагонали. Коэффициент $a_{k_1k_2\dots k_t}$ при мономе $\iota_{k_1}\iota_{k_2}\dots\iota_{k_t}$ входит в данное представление в качестве элемента ровно 2^{n-t} раз. В частности, коэффициент $a_{12\dots n}$ встречается ровно один раз и находится в нижнем левом углу матрицы $T(a)$.*

Нетрудно видеть, что $\operatorname{Ker}T=\{0\}$, поэтому данное матричное представление является точным, и алгебру $P_n(\iota)$ можно рассматривать как алгебру $2^n\times 2^n$ нижнетреугольных вещественных матриц специального вида.

Утверждение 2. *Рассмотрим 8×8 матрицу $T(a)$, где $a=\sum_{k=1}^{3}a_k\iota_k$ — однородный элемент первой степени в алгебре $P_3(\iota)$. Обозначим $|a|=\sqrt{\sum_{k=1}^{3}a_k^2}$. Тогда справедливы следующие утверждения: 1) Если хотя бы один коэффициент a_k равен нулю, то максимальное сингулярное число матрицы $T(a)$ равно $|a|$; 2) Если все коэффициенты a_k не равны нулю, то максимальное сингулярное число матрицы $T(a)$ находится в промежутке $(|a|,2|a|/\sqrt{3})$.*

Хорошо известна связь между алгеброй Грассмана и функцией определителя (см., например, [2]). Аналогичная связь существует между алгеброй Пименова и функцией перманента ([3], стр. 110). Опишем ее более подробно. В алгебре $P_n(\iota)$ рассмотрим m $(m\le n)$ однородных элементов первой степени $a_i=\sum_{k=1}^{n}a_{ik}\iota_k$, $i=1,\dots,m$. Через $A=(a_{ij})$ обозначим прямоугольную $m\times n$ матрицу, образованную коэффициентами элементов a_i. Обозначим через $A_{k_1\dots k_m}$ матрицу, которую образуют столбцы с номерами $k_1<k_2<\dots<k_m$ матрицы A. Тогда нетрудно видеть, что

$$a_1a_2\dots a_m=\sum_{k_1<\dots<k_m}\operatorname{per}(A_{k_1\dots k_m})\iota_{k_1}\dots\iota_{k_m},$$

где $\mathrm{per}(A_{k_1\ldots k_m})$ означает перманент матрицы $A_{k_1\ldots k_m}$. В частности, если $m = n$, то

$$a_1 a_2 \ldots a_n = \mathrm{per}(A)\iota_1\iota_2\ldots\iota_n. \tag{1}$$

Далее рассмотрим схему, предложенную Юркатом и Райзером в [1]. Перейдем в формуле (1) от элементов алгебры Пименова к некоторому их матричному представлению. В отличии от [1] мы будем рассматривать матричное регулярное представление:

$$T(a_1)T(a_2)\ldots T(a_n) = T(\mathrm{per}(A)\iota_1\iota_2\ldots\iota_n). \tag{2}$$

Из утверждения 1 следует, что матрица в правой части равенства (2) представляет собой $2^n \times 2^n$ матрицу, у которой в левом нижнем углу стоит элемент $\mathrm{per}(A)$, а все остальные элементы равны 0:

$$T(a_1)T(a_2)\ldots T(a_n) = \mathrm{per}(A)E_{2^n,1}.$$

Тогда применяя к данному равенству любую матричную норму $||\cdot||$, для которой $||E_{2^n,1}|| \geq 1$, получаем неравенство

$$|\mathrm{per}(A)| \leq ||T(a_1)||||T(a_2)||\ldots||T(a_n)||, \tag{3}$$

позволяющее оценить перманент матрицы сверху.

Применим к неравенству (3) спектральную норму $||\cdot||_s$. Для произвольной вещественной матрицы A она равна ее максимальному сингулярному числу, т.е. корню из максимального собственного числа матрицы A^TA. Как следует из утверждения 2, в случае $n = 3$ $||T(a_i)||_s \leq \frac{2}{\sqrt{3}}|a_i|$. Отсюда получаем следующую оценку для перманента произвольной вещественной матрицы 3-го порядка:

$$|\mathrm{per}(A)| \leq \frac{8}{3\sqrt{3}}|a_1||a_2||a_3|. \tag{4}$$

Если одна из компонент элемента a_i равна 0, то как следует из утверждения 2, $||T(a_i)||_s = |a_i|$. Отсюда, с учетом того, что перманент матрицы не меняется при перестановке строк и столбцов получаем, что для перманента произвольной вещественной 3×3 матрицы, среди элементов которой есть хотя бы один нулевой, выполняется следующее неравенство

$$|\mathrm{per}(A)| \leq \frac{4}{3}|a_1||a_2||a_3|. \tag{5}$$

Во многих случаях оценки (4), (5) дают лучший результат, чем оценки, приведенные в [3], стр. 116-117, хотя и не сравнимы с ними. Учитывая специальный вид матриц $T(a)$, $a \in P_n(\iota)$, можно попытаться доказать утверждение, аналогичное утверждению 2, и в случае произвольного n, и, следовательно, получить оценки, аналогичные формулам (4), (5), для вещественных квадратных матриц произвольного порядка.

Литература

1. Jurkat W. B., Ryser H. J. *Matrix factorizations of determinants and permanents* // Journal of Algebra. 1966. V. 3. P. 1–27.

2. Browne J. *Grassmann Algebra.* Melbourne, Australia: Quantica Publishing, 2009.

3. Минк Х. *Перманенты.* М.: Мир, 1982.

НАИМЕНЬШАЯ ТРИПРЯМОУГОЛЬНАЯ КОНГРУЭНЦИЯ НА СВОБОДНОМ ТРИОИДЕ

Юл. В. Жучок

Луганский национальный университет имени Тараса Шевченко
площадь Гоголя, 1, Старобельск, 92703, Украина yulia.mih@mail.ru

Ж.-Л. Лодэ и М.О. Ронко [1] ввели понятие триоида. Непустое множество T, снабженное тремя бинарными ассоциативными операциями $\dashv$, $\vdash$ и $\perp$, удовлетворяющими следующие аксиомы: $(x \dashv y) \dashv z = x \dashv (y \vdash z)$, $(x \vdash y) \dashv z = x \vdash (y \dashv z)$, $(x \dashv y) \vdash z = x \vdash (y \vdash z)$, $(x \dashv y) \dashv z = x \dashv (y \perp z)$, $(x \perp y) \dashv z = x \perp (y \dashv z)$, $(x \dashv y) \perp z = x \perp (y \vdash z)$, $(x \vdash y) \perp z = x \vdash (y \perp z)$, $(x \perp y) \vdash z = x \vdash (y \vdash z)$ для всех $x, y, z \in T$, называется триоидом. Если операции $\vdash$ и $\perp$ совпадают, то триоид превращается в димоноид [2, 3]. Если же операции $\dashv$, $\vdash$ и $\perp$ совпадают, то триоид превращается в полугруппу. Таким образом, каждый димоноид и каждая полугруппа могут рассматриваться как триоиды. Примеры триоидов можно найти в [4, 5].

Триоид $(T, \dashv, \vdash, \perp)$ будем называть прямоугольным триоидом или прямоугольной трисвязкой, если полугруппы $(T, \dashv)$, $(T, \vdash)$ и $(T, \perp)$ являются прямоугольными связками. Класс всех прямоугольных триоидов является подмногообразием многообразия триоидов. Если ρ — конгруэнция на триоиде $(T, \dashv, \vdash, \perp)$ такая, что $(T, \dashv, \vdash, \perp)/\rho$ есть прямоугольный триоид, то будем говорить, что ρ — трипрямоугольная конгруэнция.

Рассмотрим конструкцию свободного триоида.

Пусть Y — произвольное непустое множество, $\overline{Y} = \{\overline{x} \,|\, x \in Y\}$, $X = Y \cup \overline{Y}$ и $F[X]$ — свободная полугруппа на X. Пусть далее $P \subset F[X]$ — подполугруппа, которая содержит слова w, в запись которых элемент $\overline{x}$ $(x \in Y)$ входит как минимум один раз. Для каждого $w \in P$ через $\widetilde{w}$ обозначим слово, полученное из w заменой всех букв $\overline{x}$ $(x \in Y)$ на x.

На множестве P определим операции $\dashv$, $\vdash$ и $\perp$ по правилам:

$$w \dashv u = w\widetilde{u}, \quad w \vdash u = \widetilde{w}u, \quad w \perp u = wu$$

для всех $w, u \in P$. Алгебру $(P, \dashv, \vdash, \perp)$ обозначим через $Frt(Y)$.

Предложение. *$Frt(Y)$ — свободный триоид.*

Доказательство этого предложения совпадает с доказательством предложения 1.9 из [1], полученным для свободного триоида ранга 1.

Пусть далее $\omega \in F[X]$ и $w \in Frt(Y)$. Через $\omega^{(0)}$ (соответственно, $\omega^{(1)}$) обозначим первую (соответственно, последнюю) букву слова ω. Положим u — начальное (соответственно, конечное) подслово слова w минимальной длины такое, что $u^{(1)} \in \overline{Y}$ (соответственно, $u^{(0)} \in \overline{Y}$). В этом случае $\widetilde{u^{(1)}}$ (соответственно, $\widetilde{u^{(0)}}$) будем обозначать через $w^{[0]}$ (соответственно, $w^{[1]}$).

Определим отношение γ на множестве $Frt(Y)$, полагая

$$w_1 \gamma w_2 \Leftrightarrow (\widetilde{w_1}^{(0)}, w_1^{[0]}, w_1^{[1]}, \widetilde{w_1}^{(1)}) = (\widetilde{w_2}^{(0)}, w_2^{[0]}, w_2^{[1]}, \widetilde{w_2}^{(1)})$$

для всех $w_1, w_2 \in Frt(Y)$.

Следующая теорема характеризует наименьшую трипрямоугольную конгруэнцию на свободном триоиде $Frt(Y)$.

Теорема. *Отношение γ является наименьшей трипрямоугольной конгруэнцией на свободном триоиде $Frt(Y)$.*

Кроме этого, в терминах трисвязок подтриоидов [5] описано строение свободных триоидов.

Литература

1. Loday J.-L., Ronco M. O. *Trialgebras and families of polytopes* // Contemp. Math. 2004. V. 346. P. 369–398.

2. Loday J.-L. *Dialgebras* // In: Dialgebras and related operads. Lect. Notes Math. Springer-Verlag, Berlin. 2001. V. 1763. P. 7–66.

3. Zhuchok A. V. *Dimonoids* // Algebra and Logic. 2011. V. 50, № 4. P. 323–340.

4. Zhuchok A. V. *Semiretractions of trioids* // Ukr. Math. J. 2014. V. 66, № 2. P. 218–231.

5. Zhuchok A. V. *Tribands of subtrioids* // Proc. Inst. Applied Math. and Mech. 2010. V. 21. P. 98–106.

О ПЕРЕСЕЧЕНИЯХ АБЕЛЕВОЙ И НИЛЬПОТЕНТНОЙ ПОДГРУПП В КОНЕЧНЫХ ГРУППАХ

В.И. Зенков

Институт математики и механики УрО РАН
С.Ковалевской 16, 620990 Екатеринбург, Россия
v1i9z52@mail.ru

Пусть G — конечная группа, A — абелева подгруппа и B — нильпотентная подгруппа из G. Ранее автором [1, теорема 1] было доказано, что для любых абелевых подгрупп A и B из G минимальные по включению пересечения вида $A \bigcap B^g$, где $g \in G$, лежат в $F(G)$, где $F(G)$ — подгруппа Фиттинга группы G. Но уже пример симметрической группы $G = S_4$, где A — абелева подгруппа порядка 4, не лежащая в $F(G)$, а $B \in \mathrm{Syl}_2(G)$, показывает, что минимальные по включению пересечения вида $A \bigcap B^g$ лежат в $F(G)$, а если рассмотреть минимальные по включению пересечения вида $B \bigcap A^g$, то не все они лежат в $F(G)$. Этот пример показывает, что для рассмотрения минимальных по включению пересечений абелевой и нильпотентной подгрупп важен порядок, в котором записаны подгруппы. Но существует более сложный пример (см. пример 5) группы G, в котором даже в случае записи минимальных по включению пересечений в виде $A \bigcap B^g$ не все они лежат в $F(G)$. Однако во всех указанных примерах существует некоторое минимальное по включению пересечение вида $A \bigcap B^g$, которое лежит в $F(G)$. Как показывает следующая теорема, это явление имеет место в любой разрешимой конечной группе.

Теорема. *Пусть G — разрешимая конечная группа, A — абелева и B — нильпотентная подгруппы из G. Тогда в группе G существует элемент g такой, что $A \bigcap B^g \leq F(G)$.*

Пример 1. $G = E_9 \leftthreetimes D_8$ с точным действием D_8 на E_9. Пример показывает, что ослабить условие абелевости группы A в теореме до нильпотентности невозможно с сохранением заключения, так как при $A = B \simeq D_8$ имеем $A \bigcap B^g \neq 1$ для любого элемента g из G.

Пример 2. $G = \mathrm{Aut}(L_3(2))$. В этой группе при $A = B \in \mathrm{Syl}_2(G)$ имеем $A \bigcap B^g \neq 1$ для любого элемента g из G. Таким образом, и в неразрешимых группах условие абелевости A нельзя ослабить до нильпотентности с сохранением заключения теоремы.

Покажем, что условие нильпотентности подгруппы B также невозможно ослабить до сверхразрешимости с сохранением заключения теоремы.

Пример 3. Группа $G = S_3$ сверхразрешима. Пусть $A \simeq S_2 \in \mathrm{Syl}_2(G),\ B = G$. Тогда $A \bigcap B^g = A \not\leq F(G)$ для любого элемента g из G.

Пример 4. $G = A_5,\ A \in \mathrm{Syl}_2(G),\ B \simeq Z_5 \leftthreetimes Z_2$. Тогда $A \bigcap B^g \neq 1$ для любого элемента g из G.

Эти примеры показывают, что условия, наложенные в теореме на подгруппы A и B невозможно существенно ослабить как в разрешимом, так и в неразрешимом случае с сохранением заключения теоремы.

Следующий пример показывает, что в некоторых случаях, рассматриваемых в условиях теоремы, для абелевой подгруппы A существует подгруппа B^g такая, что $A \bigcap B^g \neq 1$ — минимальное по включению пересечение и $A \bigcap B^g \not\leq F(G)$.

Пример 5. $G = Z_2 \times S_4$. В этой группе $Z(G) = Z_2$, $O_2(G) \simeq E_8$. Силовская 2-подгруппа T из G равна $Z(G) \times S$, где $S \simeq D_8$ и $Z(T) \simeq E_4$. Пусть x — элемент порядка 4 из S, а z — инволюция из $Z(G)$. Тогда xz — элемент порядка 4 такой, что $\langle (xz)^2 \rangle = \langle x^2 \rangle = Z(S)$ и для инволюции i, для которой $S = \langle x, i \rangle$, имеем $(xz)^i = x^i z^i = x^{-1}z^{-1} = (xz)^{-1}$. Поэтому $\langle xz, i \rangle \simeq \langle x, i \rangle \simeq D_8$ и $\langle xz, i \rangle \bigcap \langle x, i \rangle = \langle i, x^2 \rangle \simeq E_4$. Следовательно, если взять подгруппу $A = \langle i, x^2 z \rangle \simeq E_4$ и $S_1 = \langle xz, i \rangle$, то $A \bigcap S_1 = \langle i \rangle \not\leq O_2(G)$ и $A \bigcap O_2(G) = \langle x^2 z \rangle$. Если положить $B = S_1 = \langle xz, i \rangle \simeq D_8$, то $S_1 \bigcap O_2(G) = \langle x^2, xzi \rangle \simeq E_4$. Таким образом, инволюция x^2 из S_1 лежит в $G' \simeq A_4$, а инволюции xzi и x^3zi из S_1 лежат в $O_2(G) \backslash G'$. В $O_2(G)$ семь инволюций, причем на трех инволюциях из $O_2(G) \bigcap G'$, являющихся центрами подгрупп S_1, S_1^f и $S_1^{f^2}$, элемент f порядка три из G действует транзитивно, централизуя инволюцию z из $Z(G)$. Следовательно, элемент f действует транзитивно на трех инволюциях из $O_2(G)$, лежащих вне $Z(G)$ и вне G', а также на множестве неупорядоченных пар, составленных из таких инволюций, которых также три. Поэтому пара инволюций $\{xz_i, x^3z_i\}$ из $S_1 \backslash G'$ не содержит третью инволюцию x^2z из $O_2(G) \backslash G'$. Но при сопряжении элементом f, а затем f^2 инволюция x^2z будет содержаться в парах инволюций, соответствующих подгруппам S_1^f и $S_1^{f^2}$. Так как $S_1 \bigcap S_1^f = O_2(G')$, то $A \bigcap S_1^f = \langle x^2 z \rangle = A \bigcap S_1^{f^2}$. Таким образом, $m = \{\langle x^2 z \rangle, \langle i \rangle\} = M$, причем одно минимальное пересечение $\langle x^2 z \rangle$ лежит в $F(G)$, а второе $\langle i \rangle$ не лежит в $F(G)$.

Работа выполнена за счет гранта Российского научного фонда (проект 15-11-10025).

Литература

1. Зенков В. И. *Пересечение абелевых подгрупп в конечных группах* // Мат. заметки. 1994. Т. 56. № 1–2. С. 150–152.

НЕКОТОРЫЕ АРИФМЕТИЧЕСКИЕ СЛЕДСТВИЯ РАВЕНСТВА ГРАФОВ ГРЮНБЕРГА–КЕГЕЛЯ ДВУХ КОНЕЧНЫХ ПРОСТЫХ КЛАССИЧЕСКИХ ГРУПП НАД ПОЛЯМИ РАЗНЫХ ХАРАКТЕРИСТИК

М.Р. Зиновьева

Институт математики и механики УрО РАН
С. Ковалевской 16, 620016 Екатеринбург, Россия zinovieva-mr@yandex.ru

Графом простых чисел или *графом Грюнберга–Кегеля* $GK(G)$ конечной группы G называется граф, вершинами которого служат простые делители порядка группы G, и две различные вершины r и s смежны тогда и только тогда, когда G содержит элемент порядка rs.

В "Коуровской тетради" [1] А. В. Васильев поставил вопрос 16.26 об описании всех пар неизоморфных конечных простых неабелевых групп с одинаковым графом Грюнберга–Кегеля. Хаги [2] и М. А. Звездина [3] получили такое описание в случае, когда одна из групп совпадает со спорадической и знакопеременной группой соответственно. Автор [4] исследовал этот вопрос для конечных простых групп лиева типа над полями одной характеристики. Гипотеза А.В. Васильева в этих случаях подтверждается.

В данной работе продолжается исследование, начатое автором в [4]–[6].

Хорошо известна теорема Жигмонди [7]: *если q и n — натуральные числа, $q \geq 2$, $n \geq 2$, то существует простое число, делящее $q^n - 1$ и не делящее $q^i - 1$ при любом натуральном $i < n$, кроме следующих случаев: $q = 2$ и $n = 6$; $q = 2^k - 1$ для некоторого простого числа k и $n = 2$.*

Здесь простое число, делящее $q^n - 1$ и не делящее $q^i - 1$ при любом натуральном $i < n$, называется *примитивным простым делителем* числа $q^n - 1$ и обозначается через $r_n(q)$ или

кратко r_n, если q фиксировано. Обозначим также через $R_n(q)$ – множество примитивных простых делителей числа $q^n - 1$.

Далее $q = p^f$ и $q_1 = {p_1}^{f_1}$, где p, p_1 – различные простые числа и f, f_1 – натуральные числа.

Обозначим через $\mathcal{M}$ множество конечных простых классических групп $A^{\pm}_{n-1}(q)$, где $n \geq 7$, $B_n(q)$, где $n \geq 5$, $C_n(q)$, где $n \geq 5$, $D^{\pm}_n(q)$, где $n \geq 5$.

В [6] сформулирована следующая

Теорема. *Пусть G и G_1 – неизоморфные группы из $\mathcal{M}$ над полями порядков q и q_1 соответственно. Если графы $GK(G)$ и $GK(G_1)$ совпадают, то выполнено одно из следующих утверждений:* (1) $\{G, G_1\} = \{A^{\pm}_{n-1}(q), A^{\pm}_{n_1-1}(q_1)\}$, *где* $n_1 \in \{n-1, n, n+1\}$; (2) $\{G, G_1\} = \{B_n(q), B_n(q_1)\}$; (3) $\{G, G_1\} = \{B_n(q), C_n(q_1)\}$; (4) $\{G, G_1\} = \{C_n(q), C_n(q_1)\}$; (5) $\{G, G_1\} = \{D_7(q), D_8(q_1)\}$; (6) $\{G, G_1\} = \{D_n(q), D_n(q_1)\}$; (7) $\{G, G_1\} = \{{}^2D_7(q_1), D_8(q)\}$; (8) $\{G, G_1\} = \{{}^2D_n(q), {}^2D_n(q_1)\}$; (9) $\{G, G_1\} = \{A_7(q), D_6(q_1)\}$; (10) $\{G, G_1\} = \{{}^2A_7(q), D_6(q_1)\}$; (11) $\{G, G_1\} = \{A^{\pm}_{n-1}(q), D_{n_1}(q_1)\}$, *где* $n_1 \in \{2n/3 - 1/3, 2n/3 - 1\}$ *и* $31 \leq n_1 \equiv 3 \pmod 4$.

Целью данной работы является уточнение утверждений этой теоремы. Основания для выделения множества $\mathcal{M}$ дает следующее предложение.

Предложение 1. *Пусть $G \in \mathcal{M}$ и G_1 – конечная простая группа такая, что графы $GK(G)$ и $GK(G_1)$ совпадают. Тогда $G \in \mathcal{M}$ или $(G, G_1) = (A^{\pm}_6(q), {}^2D_4(q_1))$, где q и q_1 нечетны.*

Для утверждений (9) и (10) теоремы можно получить следующие арифметические следствия равенства графов простых чисел.

Предложение 2. *Пусть $G = A_7(q)$, $G_1 = D_6(q_1)$. Если графы $GK(G)$ и $GK(G_1)$ совпадают, то выполнены следующие утверждения:*

(1) $\pi(q^2 - 1) = \pi(q_1^2 - 1)$;

(2) $\pi(q(q^2 + q + 1)/(3, q - 1)) = \pi(q_1(q_1^2 + 1)/2)$, *в частности,* $p_1 \in R_3(q)$ *и* $p \in R_4(q_1)$;

(3) $\{r_3(q_1), r_8(q_1)\} = \{r_5(q), r_6(q)\}$ *для некоторых простых делителей* $r_3(q_1) \in R_3(q_1)$, $r_8(q_1) \in R_8(q_1)$, $r_5(q) \in R_5(q)$ *и* $r_6(q) \in R_6(q)$.

Замечание 1. Автору известно большое число пар (q, q_1), удовлетворяющих утверждению (1) предложения 2, но неизвестно существование хотя бы одной пары чисел, удовлетворяющих утверждениям (1)–(3).

Предложение 3. *Пусть $G = {}^2A_7(q)$, $G_1 = D_6(q_1)$. Если графы $GK(G)$ и $GK(G_1)$ совпадают, то выполнены следующие утверждения:*

(1) $\pi(q^2 - 1) = \pi(q_1^2 - 1)$;

(2) $\pi(q(q^2 - q + 1)/(3, q + 1)) = \pi(q_1(q_1^2 + 1)/2)$, *в частности,* $p_1 \in R_6(q)$ *и* $p \in R_4(q_1)$;

(3) $\{r_3(q_1), r_8(q_1)\} = \{r_3(q), r_{10}(q)\}$ *для некоторых простых делителей* $r_3(q_1) \in R_3(q_1)$, $r_8(q_1) \in R_8(q_1)$, $r_3(q) \in R_3(q)$ *и* $r_{10}(q) \in R_{10}(q)$.

Замечание 2. Автору известна только одна пара (q, q_1), удовлетворяющих утверждению (1) и (2) предложения 3, а именно: $(q, q_1) = (5, 7)$. Если $q = 5$, то $r_3(q) = 31$, $r_{10}(q) = 521$. Если $q_1 = 7$, то $r_3(q_1) = 19$, $r_8(q_1) = 1201$. Таким образом, $\{19, 1201\} \neq \{31, 521\}$ и утверждение (3) для такой пары чисел (q, q_1) не выполнено.

Аналогичные условия на простые делители можно получить и в других случаях теоремы.

Работа выполнена при финансовой поддержке РФФИ (проект 13-01-00469).

Литература

1. Нерешенные вопросы теории групп. Коуровская тетрадь. 16-е изд. Новосибирск: Новосиб. гос. ун-т, 2006.

2. Hagie M. *The prime graph of a sporadic simple group* // Comm. Algebra. 2003. V. 31. No. 9. P. 4405–4424.

3. Звездина М.А. *О неабелевых простых группах с графом простых чисел как у знакопеременной группы* // Сиб. мат. журн. 2013. Т. 54. № 1. С. 65–76.

4. Зиновьева М.Р. *Конечные простые группы лиева типа над полем одной характеристики с одинаковым графом простых чисел* // Тр. Ин-та математики и механики УрО РАН. 2014. Т. 20. № 2. С. 168-183.

5. Зиновьева М.Р. *О графах простых чисел конечных простых классических групп над полями разных характеристик* // Алгебра и приложения. Тр. Межд. конф. по алгебре. Нальчик, 2014. С. 55-57.

6. Зиновьева М.Р. *О совпадении графов Грюнберга–Кегеля двух конечных простых классических групп лиева типа над полями разных характеристик* // Межд. конф. "Мальцевские чтения". Тез. докл. Новосибирск, 2015. С. 101.

7. Zsigmondy K. *Zur Theorie der Potenzreste* // Monatsh. Math. Phys. 1892. Bd 3. S. 265-284.

О ПЕРЕСТАНОВОЧНОСТИ n-МАКСИМАЛЬНЫХ ПОДГРУПП С p-НИЛЬПОТЕНТНЫМИ ПОДГРУППАМИ ШМИДТА

В.Н. Княгина

Гомельский инженерный институт МЧС Республики Беларусь
Речицкое шоссе, 35а, 246035 Гомель, Беларусь knyagina@mail.ru

Рассматриваются только конечные группы. Группой Шмидта называют ненильпотентную группу, все собственные подгруппы которой нильпотентны.

Подгруппа H группы G называется 2-максимальной подгруппой, если существует максимальная подгруппа M в группе G такая, что H содержится в M в качестве максимальной подгруппы. Аналогично определяется 3-максимальная подгруппа и т. д. В общем случае, для натурального $n > 1$ подгруппа K группы G называется n-максимальной подгруппой в G, если существует существует цепочка подгрупп

$$K = K_0 \subset K_1 \subset \ldots \subset K_{n-1} \subset K_n = G,$$

такая, что K_i является максимальной подгруппой в K_{i+1} для каждого $i = 0, 1, \ldots, n-1$.

В работе [1] исследовались группы, в которых максимальные подгруппы перестановочны с некоторыми подгруппами Шмидта. В работе [2] изучались группы, в которых для некоторого фиксированного n все n-максимальные подгруппы перестановочны со всеми подгруппами Шмидта. В частности, при $n \in \{1, 2, 3\}$, установлена метанильпотентность такой группы, а при $n \geq 4$ и условии разрешимости самой группы — ее нильпотентная длина ([2], Теорема 2). В этой работе также были изучены p-разрешимые группы, в которых каждая n-максимальная подгруппа перестановочна с любой p-нильпотентной подгруппой Шмидта. Для каждого фиксированного n установлена p-длина такой группы ([2], Теорема 1).

В настоящей заметке мы дополняем полученные результаты и доказываем, что при тех же условиях, что и в Теореме 1 из [2], факторгруппа $G/F(G)$ p-замкнута. Здесь $F(G)$ — подгруппа Фиттинга группы G. Доказана следующая теорема.

Теорема. *Зафиксируем простое число p и натуральное число $n \in \{1, 2, 3\}$. Если в p-разрешимой группе G каждая n-максимальная подгруппа перестановочна с каждой p-нильпотентной pd-подгруппой Шмидта, то $G/F(G)$ p-замкнута.*

Следствие. *Зафиксируем простое число p и натуральное число $n \in \{1, 2, 3\}$. Если в p-разрешимой группе G каждая n-максимальная подгруппа перестановочна с каждой p-нильпотентной pd-подгруппой Шмидта, то $l_p(G) \leq 1$.*

Литература

1. Княгина В. Н., Монахов В. С. *О перестановочности максимальных подгрупп с подгруппами Шмидта* // Труды Института математики и механики УрО РАН. 2011. Т. 17, № 4. С. 126–133.

2. Княгина В. Н., Монахов В. С. *О перестановочности n-максимальных подгрупп с подгруппами Шмидта* // Труды Института математики механики УрО РАН. 2012. Т. 18, № 3. С. 125–130.

КОНЕЧНЫЕ ГРУППЫ С ОБОБЩЕННО СУБНОРМАЛЬНЫМИ n-МАКСИМАЛЬНЫМИ ПОДГРУППАМИ

В.А. Ковалева

Гомельский государственный университет имени Ф. Скорины, Советская 104, 246019 Гомель, Беларусь
vika.kovalyova@rambler.ru

Все рассматриваемые в сообщении группы являются конечными. Символом $\pi(G)$ обозначается множество всех простых делителей порядка группы G.

Напомним, что собственная подгруппа M группы G называется *максимальной подгруппой* в G, если M не содержится ни в какой другой собственной подгруппе из G.

Результаты, связанные с изучением максимальных подгрупп, составили одно из самых содержательных направлений в теории конечных групп. Прежде всего это связано с тем, что многие известные классы групп допускают описание на основе свойств максимальных подгрупп. Кроме того, максимальные подгруппы лежат в основе многих важных признаков принадлежности группы выделенному классу групп. Наиболее известными среди них являются теорема Дескинса-Янко-Томпсона о разрешимости группы, обладающей нильпотентной максимальной подгруппой, класс нильпотентности 2-силовских подгрупп которой не превосходит двух, а также теоремы О.Ю. Шмидта и Б. Хупперта о разрешимости групп, все максимальные подгруппы которых являются нильпотентными и сверхразрешимыми соответственно.

По мере развития теории максимальных подгрупп авторами стали предприниматься попытки изучения и применения их обобщений. Так, одним из обобщений максимальной подгруппы является понятие n-максимальной подгруппы. Напомним, что подгруппа H группы G называется 2-*максимальной* (*второй максимальной*) подгруппой в G, если H является максимальной подгруппой в некоторой максимальной подгруппе M группы G. Аналогично могут быть определены 3-*максимальные* подгруппы и т.д.

Работы, посвященные изучению n-максимальных подгрупп ($n > 1$), составили обширное направление теории конечных групп, обогащенное большим числом глубоких теорем и содержательных примеров. Наиболее ранние результаты в этом направлении были получены Л. Редеи [1], описавшим неразрешимые группы с абелевыми вторыми максимальными подгруппами, и Б. Хуппертом [2], установившим сверхразрешимость группы, в которой все вторые максимальные подгруппы нормальны. Кроме того, в этой же работе Хупперт доказал, что в случае, когда все 3-максимальные подгруппы группы G нормальны, коммутант G' является нильпотентной группой и главный ранг группы G не превосходит двух. Позже, результаты Редеи и Хупперта получили обобщение и развитие в работах многих других авторов (З. Янко, М. Судзуки, Т.М. Гаген, В.Е. Дескинс, А.Е. Спенсер, А. Манн, Р. Шмидт, В.А. Ведерников, Э.М. Пальчик, Н.П. Конторович, Я.Г. Беркович, Р.К. Агравал, П. Флавелл, А. Баллестер-Болинше, Л.М. Эскуэрро, В. Го, Ш. Го, К.П. Шам, Б. Ли, Ш. Ли, В.А. Белоногов, А.Ф. Васильев, Т.И. Васильева, В.С. Монахов, В.Н. Семенчук, А.Н. Скиба, В.Н. Тютянов, В.Н. Княгина, В.И. Мурашко, Д.П. Андреева, Е.В. Легчекова, Ю.В. Луценко и др.). В этой связи, следует прежде всего отметить не потерявшую свое фундаментальное значение и в настоящее время работу А. Манна [3], в которой отмеченные выше результаты

Хупперта были перенесены не только на субнормальные подгруппы, но и на произвольное n, зависящее только от числа простых делителей порядка группы. В частности, Манном было доказано, что если все n-максимальные подгруппы разрешимой группы G субнормальны и $|\pi(G)| \geq n+1$, то G нильпотентна; если же $|\pi(G)| \geq n-1$, то G является ϕ-дисперсивной для некоторого упорядочения ϕ множества $\pi(G)$. И наконец, в случае, когда $|\pi(G)| = n$, Манн привел полное описание группы G.

Пусть $\mathfrak{F}$ — класс групп. Напомним, что подгруппа H группы G называется $\mathfrak{F}$-*субнормальной в смысле Кегеля* [4] или K-$\mathfrak{F}$-*субнормальной* [5] в G, если найдется такая цепь подгрупп

$$H = H_0 \leq H_1 \leq \cdots \leq H_n = G,$$

что либо H_{i-1} нормальна в H_i, либо

$$H_{i-1}/(H_{i-1})_{H_i} \in \mathfrak{F}$$

для всякого $i = 1, \ldots, n$.

Нами получена полная классификация групп, у которых все вторые либо все третьи максимальные подгруппы K-$\mathfrak{F}$-субнормальны в случае, когда $\mathfrak{F} = \mathfrak{U}$ — класс всех сверхразрешимых групп [6, 7], что позволило обобщить и развить результаты многих из упомянутых выше авторов (Б. Хупперт, Р.К. Агравал, В.Н. Семенчук, В.С. Монахов, В.Н. Княгина, А.Н. Скиба, Ю.В. Луценко и др.). Отметим, что для получения такой классификации ранее в работах [8, 9] было достигнуто расширение отмеченных результатов работы А. Манна [3] до K-$\mathfrak{U}$-субнормальных подгрупп, что, в свою очередь, привело к необходимости развития соответствующих результатов Х. Виландта, К. Дёрка, О.-Ю. Крамера и др.

Литература

1. Rédei L. *Ein Satz uber die endlichen einfachen Gruppen* // Acta Math. 1950. V. 84. P. 129-153.

2. Huppert B. *Normalteiler und maximal Untergruppen endlicher gruppen* // Math. Z. 1954. V. 60. P. 409-434.

3. Mann A. *Finite groups whose n-maximal subgroups are subnormal* // Trans. Amer. Math. Soc. 1968. V. 132. P. 395-409.

4. Kegel O. H. *Zur Struktur mehrfach faktorisierbarer endlicher Gruppen* // Math. Z. 1965. V. 87. P. 409-434.

5. Ballester-Bolinches A., Ezquerro L. M. *Classes of Finite Groups*. Dordrecht: Springer-Verlag, 2006.

6. Ковалева В. А., Йи С. *Finite groups with all n-maximal ($n = 2, 3$) subgroups K-$\mathfrak{U}$-subnormal* // Проблемы физики, математики и техники. 2014. Т. 2. № 19. С. 59-64.

7. Kovaleva V. A., Yi X. *Finite biprimary groups with all 3-maximal subgroups $\mathfrak{U}$-subnormal* // Acta Matematica Hungarica. 2015. V. 146. № 1. P. 47-55.

8. Ковалева В. А., Скиба А. Н. *Конечные разрешимые группы, у которых все n-максимальные подгруппы $\mathfrak{U}$-субнормальны* // Сибирский математический журнал. 2013. Т. 54. № 1. P. 86-97.

9. Kovaleva V. A., Skiba A. N. *Finite soluble groups with all n-maximal subgroups $\mathfrak{F}$-subnormal* // Journal of Group Theory. 2014. V. 17. P. 273-290.

ЗНАЧЕНИЯ ЦЕЛОЧИСЛЕННЫХ МНОГОЧЛЕНОВ БЕЗ ОБЩИХ КОРНЕЙ В ПОЛЯХ КОМПЛЕКСНЫХ И p-АДИЧЕСКИХ ЧИСЕЛ

Э.И. Ковалевская[1], **О.Н. Кемеш, О.В. Рыкова**[2]

Белорусский государственный аграрный технический университет
пр. Независимости 99, 220023 Минск
[1]ekovalevsk@mail.ru, [2]oly8521@yandex.ru

В теории трансцендентных чисел известны неравенства Гельфонда [1] для значений двух многочленов P_1, $P_2 \in \mathbb{Z}[x]$ в трансцендентной точке, при выполнении которых получаем, что P_1 и P_2 обязательно имеют общий корень. Мы обобщаем и усиливаем *лемму Гельфонда* в важных для приложений случаях.

Пусть $P = P(t) \in \mathbb{Z}[t]$, $\deg P = n$ и высота многочлена $H(P)$ равна H, где $H(P)$ — это максимум модулей его коэфициентов. Через $c_i = c_i(n)$, $i = 1, 2, 3, 4$, обозначим некоторые величины, зависящие от n и не зависящие от H. Пусть $p \geq 2$ — простое число, $x \in \mathbb{R}$, $\omega \in \mathbb{Q}_p$ — трансцендентные числа. Если многочлен P приводим над $\mathbb{Z}$, т. е. $P(t) = P_1(t) \cdot P_2(t)$, то хорошо известно (см. [2, с. 26]), что $n = n_1 + n_2$, где $n_1 = \deg P_1$, $n_2 = \deg P_2$, и $c_1 H < H(P_1)H(P_2) < c_2 H$. Положим $H(P_1) = H^{\lambda_1}$ при $0 \leq \lambda_1 \leq 1$, $H(P_2) = H^{1-\lambda_1}$. Приведем *неравенство Гельфонда* для P_1, $P_2 \in \mathbb{Z}[t]$ без общих корней [1, с. 182]:

$$1 \leq c_3(|P_1(t)| + |P_2(t)|) \cdot H(P_1)^{\deg P_2} \cdot H(P_2)^{\deg P_1}, \quad \max_{i=1,2} H(P_i) \leq Q. \tag{1}$$

Отсюда если $\min_{i=1,2} |P_i(t)| \leq Q^{-w}$ при $w > 0$, то $w \leq 2n$, иначе неравенство (1) противоречиво.

Мы получаем неравенство вида (1)для многочленов P_1, $P_2 \in \mathbb{Z}[t]$ без общих корней в поле $\mathbb{C}$ и алгебраическом замыкании $\mathbb{Q}_p^*$ поля $\mathbb{Q}_p$:

$$1 \leq c_4 \max_{i=1,2} |P_i(t)| \cdot \max_{i=1,2} |P_i(\omega)|_p \cdot Q^{\lambda_1(n-n_1)+(1-\lambda_1)n_1}, \quad \max_{i=1,2} H(P_i) \leq Q. \tag{2}$$

Нетрудно показать, что $\lambda_1(n-n_1)+(1-\lambda_1)n_1 \leq n-1$. Поэтому если $\max_{i=1,2} |P_i(x)| < Q^{-w}$, $\max_{i=1,2} |P_i(\omega)|_p < Q^{-v}$, то из (2) следует, что $w + v \leq n - 1$. Неравенство (2) обобщает и усиливает неравенство (1). Отметим, что неравенство (2) в $\mathbb{Q}_p$ было доказано в [3].

Авторы выражают благодарность профессору В.И. Бернику за постановку задачи и полезные обсуждения.

Литература

1. Гельфонд А. О. *Трансцендентные и алгебраические числа.* Гос. изд. тех.-теор. лит., 1952.

2. Спринджук В. Г. *Проблема Малера в метрической теории чисел.* Наука и техника, 1967.

3. Beresnevich V. V., Bernik V. I., Kovalevskaya E. I. *On approximation of p-adic numbers by p-adic algebraic numbers* // J. Number Theory. 2005. V. 111. P. 33–56.

О ПОЛИГОНАХ НАД СИНГУЛЯРНЫМИ ПОЛУГРУППАМИ

И.Б. Кожухов, А.Р. Халиуллина

Национальный исследовательский университет МИЭТ, 124498, Москва, Россия
kozhuhov_i_b@mail.ru, haliullinaar@gmail.com

Полигон (*автомат*) X над полугруппой S (см. [1]) – это множество X, на котором действует полугруппа S, т.е. определено отображение $X \times S \to X$, $(x, s) \mapsto xs$, удовлетворяющее условию $x(st) = (xs)t$ при всех $x \in X$, $s, t \in S$. Для полугрупп относительно несложного строения все полигоны над ними могут быть полностью описаны. Так, в [2] были описаны в теоретико-групповых и теоретико-множественных терминах полигоны над вполне 0-простыми полугруппами $\mathcal{M}^0(G, I, \Lambda, P)$ и вполне простыми полугруппами $\mathcal{M}(G, I, \Lambda, P)$ (здесь G – группа, I и Λ – множества, P – сэндвич-матрица). Вполне простыми полугруппами являются, в частности, *полугруппы левых / правых нулей*, а также их прямые произведения – *прямоугольные связки* (для получения прямоугольной связки нужно взять в качестве G группу из одного элемента, а в качестве сэндвич-матрицы P матрицу из единиц). Прямоугольная связка имеет ряд альтернативных определений: 1) полугруппа, удовлетворяющая тождествам $x^2 = x$, $xyz = xz$; 2) полугруппа с тождеством $xyx = x$; 3) полугруппа, удовлетворяющая квазитождеству $xy = yx \to x = y$. *Сингулярной полугруппой* мы называем полугруппу левых или правых нулей.

Все конгруэнции произвольного полигона над полугруппой левых нулей были описаны в [3], правых нулей – в [4].

Полигон над полугруппой может быть рассмотрен как унарная алгебра, т.е. универсальная алгебра, у которой все операции унарны. Напомним, что универсальная алгебра называется *подпрямо неразложимой*, если она не разлагается в нетривиальное подпрямое произведение алгебр. Интерес к подпрямо неразложимым универсальным алгебрам объясняется хорошо известной теоремой Биркгофа, утверждающей, что всякая алгебра является подпрямым произведением подпрямо неразложимых алгебр. Известно, что нетривиальная подпрямо неразложимая алгебра – это в точности алгебра, решётка конгруэнций которой имеет единственный атом. Подпрямо неразложимые полигоны над сингулярными полугруппами, а также над прямоугольными связками были охарактеризованы в [5].

Полигон A называется *инъективным*, если для любого инъективного гомоморфизма $\alpha : X \to Y$ полигонов и любого гомоморфизма $\varphi : X \to A$ существует гомоморфизм $\psi : Y \to A$ такой, что $\psi\alpha = \varphi$. *Инъективная оболочка* полигона B – это минимальный инъективный надполигон полигона B. Полигон A называется *проективным*, если для любого сюръективного гомоморфизма $\alpha : X \to Y$ полигонов и любого гомоморфизма $\varphi : A \to Y$ существует гомоморфизм $\psi : A \to X$ такой, что $\alpha\psi = \varphi$. *Проективным накрытием* полигона B называется проективный полигон P, для которого существует сюръективный гомоморфизм $\theta : P \to B$ такой, что для любого собственного подполигона $P' \subset P$ ограничение $\theta|_{P'} : P' \to B$ не является сюръективным. Хорошо известно, что, как и в случае модулей над кольцами, инъективная оболочка существует у каждого полигона, а проективное накрытие не у каждого. Также известно необходимое условие инъективности полигона – это наличие у него нулевого элемента (при этом единственности нуля может не быть). Полигон X называется *сепарабельным*, если для любых $x, y \in X$ таких, что $x \neq y$, существует $s \in S \setminus \{1\}$ такое, что $x \neq y$. В работе [6] для сепарабельных полигонов над полугруппой левых нулей были найдены условия инъективности полигона и построена инъективная оболочка полигона. В [7] нахождение условий инъективности и построение инъективной оболочки полигона над полугруппой левых нулей было осуществлено без предположения сепарабельности. Далее, в [7] было доказано, что наличие нуля является необходимым и достаточным условием инъективности полигонов над группами и полигонов над полугруппами правых нулей. Поэтому

построение инъективной оболочки неинъективного полигона над группой или полугруппой правых нулей состоит в присоединении к этому полигону внешним образом нуля. Кроме того, в [7] были получены условия проективности полигонов над группами, полугруппами правых и полугруппами левых нулей и построены проективные накрытия полигонов. В частности, оказалось, что проективное накрытие существует у любого полигона над такими полугруппами. Одним из результатов работы [7] является тот факт, что над полугруппой левых нулей проективными полигонами являются в точности копроизведения (т.е. дизъюнктные объединения) свободных полигонов и полигонов, состоящих из нулей.

Пусть X – полигон над полугруппой S. Будем говорить, что полугруппа S действует на X *эффективно*, если

$$(\forall\ x \in X\ xs = xt) \Rightarrow s = t$$

для всех $s, t \in S$.

В работе [3] были описаны полигоны X над сингулярными полугруппами S, у которых решётка конгруэнций $\mathrm{Con}X$ модулярна, или дистрибутивна, или является цепью. Отметим, что в случае модулярности решётки конгруэнций $\mathrm{Con}X$ полигона X над полугруппой левых нулей S максимальный порядок полигона X равен 5, а максимальный порядок полугруппы S, если она действует эффективно на X, равен 9. Максимальный порядок решётки конгруэнций равен 13. В случае полугруппы правых нулей S порядок модулярной решётки конгруэнций не превышает 200, максимальный порядок полигона X с модулярной решёткой конгруэнций равен 9, максимальный порядок полугруппы S, действующей эффективно на X, равен 27. Работа по описанию полигонов над прямоугольными связками, имеющих модулярную решётку конгруэнций, авторами не завершена, но полученные ими необходимые условия показывают, что порядок полигона X при этом не превышает 9.

Литература

1. Kilp M., Knauer U., Mikhalev A. V. *Monoids, acts and categories*. W. de Gruyter, N.Y. – Berlin, 2000.

2. Avdeyev A. Yu., Kozhukhov I. B. *Acts over completely 0-simple semigroups* // Acta Cybernetica. 2000. V. 14. № 4. P. 523–531.

3. Халиуллина А. Р. *Условия модулярности решётки конгруэнций полигона над полугруппой правых и левых нулей* // Дальневост. матем. журнал. 2015. Т. 15. № 1. С. 102–120.

4. Халиуллина А. Р. *Конгруэнции полигонов над полугруппами правых нулей* // Чебыш. сб. 2015. Т. 14. № 3. С. 142–146.

5. Кожухов И. Б., Халиуллина А. Р. *Характеризация подпрямо неразложимых полигонов* // Прикл. дискр. матем. 2015. № 1. С. 5–16.

6. Moghaddasi G. *On injective and subdirectly irreducible S-acts over left zero semigroups* // Turk. J. Math. 2012. V. 36. P. 359–365.

7. Кожухов И. Б., Халиуллина А. Р. *Инъективность и проективность полигонов над сингулярными полугруппами* // Электронные информационные системы. 2014. Т. 2. № 2. С. 45–56.

О КОНЕЧНЫХ ГРУППАХ G С НЕСВЯЗНЫМ ГРАФОМ ПРОСТЫХ ЧИСЕЛ И ОГРАНИЧЕНИЯМИ НА $\pi_1(G)$

В.А. Колпакова

Институт математики и механики УрО РАН
С. Ковалевской 16, 620990 Екатеринбург, Россия leralid@mail.ru

Пусть G — конечная группа. Обозначим через $\pi(G)$ множество всех простых делителей порядка группы G. *Граф простых чисел* (*граф Грюнберга — Кегеля*) $\Gamma(G)$ группы G определяется как граф с множеством вершин $\pi(G)$, в котором две различные вершины p и q

смежны тогда и только тогда, когда в G есть элемент порядка pq. Группа G называется *n-примарной*, если $|\pi(G)| = n$. Обозначим число компонент связности графа $\Gamma(G)$ через $s(G)$, а множество его связных компонент — через $\{\pi_i(G) \mid 1 \leq i \leq s(G)\}$; для группы G четного порядка считаем, что $2 \in \pi_1(G)$.

В рамках общей задачи изучения конечных групп по свойствам их графов простых чисел наше внимание прежде всего привлекает более подробное изучение класса конечных групп с несвязным графом простых чисел. Это объясняется тем, что указанный класс широко обобщает класс конечных групп Фробениуса, что сразу видно из известной структурной теоремы Грюнберга —Кегеля о конечных группах с несвязным графом простых чисел (см. [1]). Заметим также, что класс конечных групп с несвязным графом простых чисел совпадает с классом конечных групп, имеющих изолированную подгруппу.

В рамках отмеченной задачи А.С. Кондратьев и И.В. Храмцов [4] — [7] изучали конечные группы, имеющие несвязный граф простых чисел с числом вершин, не превосходящим 4. А.С. Кондратьевым были определены конечные почти простые 5-примарные группы и их графы Грюнберга — Кегеля [8]. Автором совместно с А.С. Кондратьевым [9] было получено описание главных факторов коммутантов конечных неразрешимых 5-примарных групп G с несвязным графом Грюнберга—Кегеля в случае, когда $G/F(G)$ — почти простая n-примарная группа для $n \leq 4$. Наша цель — описать 5-примарные группы G с несвязным графом простых чисел в остальных случаях. Естественно начать изучение, накладывая некоторые ограничения на компоненту $\pi_1(G)$. Результатом этой работы является описание 5-примарных групп G с несвязным графом простых чисел таких, что либо $\pi_1(G) = \{2\}$, либо $3 \notin \pi_1(G) \neq \{2\}$ и $3 \in \pi(G)$. Доказаны две теоремы.

Теорема 1. *Пусть G — конечная 5-примарная группа и $\pi_1(G) = \{2\}$. Тогда выполняется одно из следующих утверждений:*

(1) *$G \cong O(G) \leftthreetimes S$ — группа Фробениуса, где $O(G)$ — 4-примарная абелева группа и S — циклическая 2-группа или обобщенная группа кватернионов;*

(2) *G — группа Фробениуса с ядром $O_2(G)$ и 4-примарным дополнительным множителем;*

(3) *$G \cong A \leftthreetimes (B \leftthreetimes C)$ — 2-фробениусова группа, где $A = O_2(G)$, B — циклическая 4-примарная $2'$-группа и C — циклическая 2-группа;*

(4) *$G \cong L_2(r)$, $r \geq 65537$ — простое число Ферма или Мерсенна и $|\pi(r^2 - 1)| = 4$;*

(5) *$\overline{G} = G/O_2(G) \cong L_2(2^m)$, где либо $m \in \{6, 8, 9\}$, либо $m \geq 11$ — простое число. Если $O_2(G) \neq 1$, то $O_2(G)$ является прямым произведением минимальных нормальных подгрупп порядка 2^{2m} в G, каждая из которых как $\overline{G}$-модуль изоморфна естественному $GF(2^m)SL_2(2^m)$-модулю;*

(6) *$\overline{G} = G/O_2(G) \cong Sz(q)$, где $q = 2^p$, $p \geq 7$ и $q - 1$ — простые числа, $|\pi(q - \varepsilon\sqrt{2q} + 1)| = 2$ и $|\pi(q + \varepsilon\sqrt{2q} + 1)| = 1$ для $\varepsilon \in \{+, -\}$, $5 \in \pi(q - \varepsilon\sqrt{2q} + 1)$. Если $O_2(G) \neq 1$, то $O_2(G)$ является прямым произведением минимальных нормальных подгрупп порядка q^4 в G, каждая из которых как $\overline{G}$-модуль изоморфна естественному 4-мерному $GF(q)Sz(q)$-модулю.*

Теорема 2. *Пусть G — конечная 5-примарная группа с несвязным графом простых чисел, $\overline{G} = G/F(G)$ — почти простая 5-примарная группа, $3 \in \pi(G)$ и $3 \notin \pi_1(G) \neq \{2\}$. Тогда выполняется одно из следующих утверждений:*

(1) *G изоморфна $L_2(5^3)$ или $L_2(17^3)$;*

(2) *$G \cong L_2(p)$, где либо $p \geq 65537$ — простое число Ферма или Мерсенна и $|\pi(p^2 - 1)| = 4$, либо $p \geq 41$ — простое число, $|\pi(p^2 - 1)| = 4$ и $3 \in \pi(\frac{p+1}{2})$;*

(3) *G изоморфна $L_2(3^r)$ или $PGL_2(3^r)$, где r — нечетное простое число, $|\pi(3^{2r} - 1)| = 4$ и $r \notin \pi(G)$;*

(4) *$G \cong L_2(p^r)$, где $p \in \{5, 17\}$, r — нечетное простое число, $|\pi(p^{2r} - 1)| = 4$, $3 \in \pi(\frac{p^r+1}{2})$ и $r \notin \pi(G)$.*

Работа выполнена при финансовой поддержке программы РНФ для отдельных научных групп (проект 14-11-00061).

Литература

1. Williams J. S. *Prime graph components of finite groups* // J. Algebra. 1981. V. 69. № 2. P. 487–513.

2. Кондратьев А. С. *О компонентах графа простых чисел конечных простых групп* // Мат. сб. 1989. Т. 180. № 6. С. 787–797.

3. Lucido M. S. *Prime graph components of finite almost simple groups* // Rend. Sem. Mat. Univ. Padova. 1999. V. 102. P. 1–22; addendum, Rend. Sem. Mat. Univ. Padova. 2002. V. 107. P. 189–190.

4. Кондратьев А. С., Храмцов И. В. *О конечных трипримарных группах* // Труды Ин-та математики и механики УрО РАН. 2010. Т. 16. № 3. С. 150–158.

5. Кондратьев А. С., Храмцов И. В. *О конечных четырепримарных группах* // Труды Ин-та математики и механики УрО РАН. 2011. Т. 17. № 4. С. 142–159.

6. Кондратьев А. С., Храмцов И. В. *О конечных непростых трипримарных группах с несвязным графом простых чисел* // Сиб. эл. матем. изв. 2012. Т. 9. С. 472–477.

7. Храмцов И. В. *О конечных непростых* 4*-примарных группах* // Сиб. эл. матем. изв. 2014. Т. 11. С. 695–708.

8. Kondrat'ev A. S. *Finite almost simple* 5*-primary groups и their Gruenberg-Kegel graphs* // Сиб. эл. мат. изв. 2014. Т. 11. С. 634–674.

9. Колпакова В. А, Кондратьев А. С *О конечных неразрешимых 5-примарных группах с несвязным графом Грюнберга — Кегеля таких, что* $|\pi(G/F(G))| \leq 4$ // Фунд. и прикл. матем., в печати.

ПОЛУЦЕПНЫЕ ГРУППОВЫЕ КОЛЬЦА КОНЕЧНЫХ ЛИНЕЙНЫХ ГРУПП И ПРОСТЫХ ГРУПП РИ

А.В. Кухарев, Г.Е. Пунинский

Белорусский государственный университет, механико-математический факультет,
пр. Независимости, 4, 220030 Минск, Беларусь kukharev@mail.ru, punins@mail.ru

Работа посвящена исследованию вопроса о полуцепности групповых колец конечных линейных групп и простых групп лиевского типа. Кольцо R называется *полуцепным*, если оно как левый и как правый R-модуль является прямой суммой цепных модулей. В настоящее время не известно, для каких конечных групп G групповые кольца FG над заданным полем F характеристики $p > 0$ являются полуцепными (см. [1]). Над алгебраически замкнутым полем F характеристики p полуцепность группового кольца FG конечной группы G равносильна тому, что деревья Брауэра всех дефектных p-блоков группы G имеют вид "звезды" с исключительной вершиной в центре [2, следствие VII.2.22]. В работе [3] показано, что в случае циклической дефектной группы дерево Брауэра любого p-блока группы $\mathrm{GL}(n, q)$ при $p \neq 2$, $p \nmid q$ является прямым отрезком с исключительной вершиной на конце. В [4] установлен вид деревьев Браэура групп $\mathrm{PSL}(2, q)$. Общий случай групп вида $\mathrm{PSL}(n, q)$, а также $\mathrm{SL}(n, q)$, остался нерассмотренным.

Нами получен полный ответ на вопрос, для каких чисел n, q и p групповое кольцо групп $\mathrm{GL}(n, q)$, $\mathrm{SL}(n, q)$, $\mathrm{PSL}(n, q)$ и $G_2(q)$ над произвольным полем характеристики p является полуцепным.

Теорема 1. *Пусть* $G = \mathrm{GL}(n, q)$, $n \geq 2$ F *— поле характеристики* p*, делящей* $|G|$*. Тогда групповое кольцо* FG *полуцепное, если и только если выполнено любое из следующих условий:*

1) $n = 2$, $p = q \in \{2, 3\}$*;*

2) $n \in \{2, 3\}$, $p = 3$, $q \equiv 2, 5 \pmod 9$.

Теорема 2. *Пусть* $G = \mathrm{SL}(n, q)$ *или* $\mathrm{PSL}(n, q)$, $n \geq 2$, F *— поле характеристики* p*, делящей* $|G|$*. Тогда групповое кольцо* FG *полуцепное, если и только если выполнено любое из следующих условий:*

1) $n = 2$ *и* $p \mid q - 1$, $p \neq 2$;
2) $n = 2$ *и* $p = q \in \{2, 3\}$;
3) $n \in \{2, 3\}$, $p = 3$ *и* $q \equiv 2, 5 \pmod 9$.

Используя сведения о деревьях Брауэра p-блоков конечных групп Шевалле типа $G_2(q)$ [5,6] и групп Ри ${}^2G_2(q^2)$, ${}^2F_4(q^2)$ [7], легко получить ответ о полуцепности групповых колец этих групп.

Теорема 3. *Если* $G = G_2(q)$ *и* F *— поле положительной характеристики, делящей* $|G|$, *то групповое кольцо* FG *не является полуцепным.*

Теорема 4. *Пусть* $G = {}^2G_2(q^2)$, $q^2 = 3^{2m+1}$, $m \geq 0$ *и* F *— поле характеристики* p, *делящей* $|G|$. *Групповое кольцо* FG *полуцепное, если и только если* $p \mid q^2 - 1$.

Теорема 5. *Если* $G = {}^2F_4(q^2)$, $q^2 = 2^{2m+1}$, $m \geq 0$ *и* F *— поле характеристики* p, *делящей* $|G|$, *то групповое кольцо* FG *не полуцепное.*

Литература

1. Baba Y., Oshiro K. *Classical Artinian Rings*, World Scient. Publ., 2009.
2. Feit W. *The Representation Theory of Finite Groups*, North Holland Mathematical Library, Vol. 25, 1982.
3. Fong P., Srinivasan B. *Blocks with cyclic defect groups in* $\mathrm{GL}(n, q)$ // Bull. Amer. Math. Soc. 1980. Vol. 3. P. 1041–1044.
4. Burkhardt R. *Die Zerlegungsmatrizen der Gruppen* $\mathrm{PSL}(2, p^f)$ // J. Algebra, 40 (1976), 75–96.
5. Shamash J. *Blocks and Brauer trees in the group* $G_2(q)$ *for primes dividing* $q \pm 1$ // Comm. Algebra. 1989. Vol. 17. P. 1901–1949.
6. Shamash J. *Brauer trees for blocks of cyclic defect in the group* $G_2(q)$ *for primes dividing* $q^2 \pm q + 1$ // J. Algebra. 1989. Vol. 123. P. 378–396.
7. Hiss G. *The Brauer trees of the Ree groups* // Comm. Algebra. 1991. Vol. 19. P. 871–888.

ТЕОРЕМА ТИПА ХИНЧИНА ДЛЯ СЛУЧАЯ РАСХОДИМОСТИ В ТРЕХМЕРНОМ ЕВКЛИДОВОМ ПРОСТРАНСТВЕ

А.В. Луневич[1], **А.С. Кудин**[1], **Н.В. Шамукова**[2]

[1]Институт математики НАН Беларуси, Сурганова 11, 220072 Минск, Беларусь
kifeislife@gmail.com, kunixd@gmail.com
[2]Командно-инженерный институт МЧС РБ, Машиностроительная 25, 220118 Минск, Беларусь
shamukova_n@mail.ru

В 1924 году А.Я. Хинчин [1] доказал замечательную теорему, ставшую основой для многих задач метрической теории чисел. Пусть $\Psi(H)$ – положительная монотонно убывающая функция, определенная на $\mathbb{R}_+$ и $I \subset \mathbb{R}$ – некоторый интервал. Множество точек $x \in I$, для которых существует бесконечно много решений $p, q \in \mathbb{Z}$ неравенства $|qx - p| < \Psi(q)$, обозначим как $\mathcal{L}_1(\Psi)$. Теорема Хинчина гласит, что $\mu(\mathcal{L}_1(\Psi)) = 0$, если $\sum_{h=1}^{\infty} \Psi(h) < \infty$, и $\mu(\mathcal{L}_1(\Psi)) = \mu(I)$ в противном случае.

По аналогии обозначим через $\mathcal{L}_n(\Psi)$ множество точек $x \in I$, для которых существует бесконечно много решений неравенства $|P(x)| < H(P)^{-n+1}\Psi(H(P))$ в целочисленных полиномах P степени не более n. При $\Psi(H) = H^{-\lambda}$, $(\lambda \leq 1)$ несложно доказать, используя принцип ящиков Дирихле, что $\mu(\mathcal{L}_n(\Psi)) = \mu(I)$. В 1932 году Малер [2] выдвинул гипотезу, что $\mu(\mathcal{L}_n(\Psi)) = 0$ при $\Psi(H) = H^{-\lambda}$, $(\lambda > 1)$. В 1964 году гипотеза Малера была доказана Спринджуком [3]. В 1966 году Бейкер доказал, что если $\sum_{h=1}^{\infty} \Psi(h) < \infty$, то для почти всех $x \in \mathbb{R}$ неравенство $|P(x)| < \Psi^n(H(P))$ имеет не более чем конечное число решений в целочисленных полиномах P степени не более n, а также предположил, что для $\mathcal{L}_n(\Psi)$ справедлива теорема типа Хинчина, а именно, $\mu(\mathcal{L}_n(\Psi)) = 0$ если $\sum_{h=1}^{\infty} \Psi(h) < \infty$, и $\mu(\mathcal{L}_n(\Psi)) = \mu(I)$ в противном случае. Эта гипотеза в случае сходимости была доказана Берником, а в случае

расходимости – Бересневичем. Аналогичные результаты были получены в полях комплексных и p-адических чисел Берником, Васильевым и Ковалевской.

В данной работе мы рассматриваем теорему типа Хинчина в случае расходимости в пространстве $\mathbb{R}^3$. Отметим, что Берником, Будариной и Дикинсон получен аналог теоремы Хинчина в случае расходимости в пространстве $\mathbb{R}\times\mathbb{C}\times\mathbb{Q}_p$. Пусть $\boldsymbol{v}=(v_1,v_2,v_3)$ и $\boldsymbol{\lambda}=(\lambda_1,\lambda_2,\lambda_3)$ – векторы с действительными координатами, удовлетворяющие условиям

$$\begin{cases} v_i>0,\ \lambda_i>0,\ i=1,2,3,\\ v_1+v_2+v_3=n-3,\\ \lambda_1+\lambda_2+\lambda_3=1. \end{cases}$$

Определим через $\mathcal{L}_{\boldsymbol{v},\boldsymbol{\lambda}}$ множество точек $(x_1,x_2,x_3)\in I=\left(-\frac{1}{2};\frac{1}{2}\right)^3$, для которых существует бесконечно много неприводимых полиномов P степени ровно n, удовлетворяющих системе неравенств

$$\begin{cases} |P(x_1)|<H(P)^{-v_1}\Psi^{\lambda_1}\left(H(P)\right),\\ |P(x_2)|<H(P)^{-v_2}\Psi^{\lambda_2}\left(H(P)\right),\\ |P(x_3)|<H(P)^{-v_3}\Psi^{\lambda_3}\left(H(P)\right). \end{cases}$$

В данной работе доказана следующая

Теорема. *Если* $n\geq 3$ *и* $\sum_{h=1}^{\infty}\Psi(h)=\infty$, *то* $\mu(\mathcal{L}_{\boldsymbol{v},\boldsymbol{\lambda}})=\mu(I)$.

В ходе доказательства теоремы мы доказываем регулярность системы точек сопряженных действительных алгебраических чисел степени ровно n.

Литература

1. Khintchine A. *Einige Satze uber Kettenbruche, mit Anwendungen auf die Theorie der Diophantischen Approximationen* // Math. Ann. 1924. Vol. 92. Issue 1–2. P. 115–125.

2. Mahler K. *Zur Approximation der Exponentialfunktion und des Logarithmus, Teil I* // J. Reine Angew. Math. 1932. Vol. 166. P. 118–150.

3. Спринджук В. Г. *Проблема Малера в метрической теории чисел.* Минск: Наука и Техника, 1967.

ОБ ИНТЕГРАЛЬНЫХ КРИВЫХ ОБОБЩЕННЫХ ЦЕПОЧЕК ТОДЫ С ДВУМЯ ЭКСПОНЕНТАМИ

М.В. Милованов[1], **О.Г. Медведева**[2],

Белорусский государственный педагогический университет
Советская 18, 220030 Минск, Беларусь [1]mvmil@mail.ru, [2]olga_medvedeva@tut.by

Под обобщенной цепочкой Тоды с двумя экспонентами будем понимать гамильтонову систему дифференциальных уравнений с гамильтонианом вида

$$H=\frac{1}{2}(p_1^2+\cdots+p_n^2)+c_1^2e^{\alpha_1q_1+\cdots+\alpha_nq_n}+c_2^2e^{\beta_1q_1+\cdots+\beta_nq_n}. \tag{1}$$

Обобщенные цепочки Тоды возникают при решении многих физических задач.

На каждой орбите коприсоединенного представления произвольной группы Ли определена каноническая симплектическая структура, которая превращает орбиту в симплектическое многообразие. Многие обобщенные цепочки Тоды можно рассматривать как гамильтоновы системы на орбитах коприсоединенного представления борелевских подгрупп вещественных простых расщепимых групп Ли. Такой подход проясняет суть дела и упрощает многие доказательства [1].

В [2] показано, что любая обобщенная цепочка Тоды с двумя экспонентами либо интегрируется в квадратурах, либо сводится к решению нелинейного дифференциального уравнения второго порядка

$$y'' = \left(\lambda - \frac{1}{k}y'^2\right)\left(\frac{k}{y} + \frac{2y}{1-x^2-y^2}\right) \tag{2}$$

в полукруге $1 - x^2 - y^2 > 0$, $y > 0$ с коэффициентами k и λ одного знака. Описание решений уравнения (2) вблизи границы полукруга дает возможность исследовать поведение интегральных кривых цепочек Тоды с гамильтонианом (1) "на бесконечности".

Изучение решений (2) вблизи оси Ox, т.е. при малых $y > 0$, можно провести, положив в (2) $y^2 = 0$. В результате получается уравнение, не содержащее переменной x:

$$yy'' + y'^2 - k\lambda = 0,$$

где $k\lambda > 0$. Его общее решение имеет вид

$$y^2 = k\lambda x^2 + C_1 x + C_2,\ y = \pm\sqrt{k\lambda}x + C, \tag{3}$$

где C_1, C_2, C – произвольные постоянные [3]. Вторая из формул (3) дает точные решения уравнения (2), а первая – приближенные.

С помощью формул (3) получены точные и приближенные решения цепочек Тоды с гамильтонианом (1), позволяющие понять поведение соответствующих интегральных кривых при $t \to \infty$.

Литература

1. Переломов А. М. *Интегрируемые системы классической механики и алгебры Ли* . М.: Наука, 1990.

2. Милованов М. В., Медведева О. Г. *Об обобщенных цепочках Тоды с двумя экспонентами* // Докл. НАН Беларуси. 2013. Т. 57. №3. С. 37–42.

3. Милованов М. В., Медведева О. Г. *Применение методов группового анализа к изучению обобщенных цепочек Тоды с двумя экспонентами* // Докл. НАН Беларуси. 2014. Т. 58. №1. С. 9–15.

КОНЕЧНЫЕ ГРУППЫ С $\mathfrak{U}$-АБНОРМАЛЬНЫМИ И $\mathfrak{U}$-СУБНОРМАЛЬНЫМИ НИЛЬПОТЕНТНЫМИ ПОДГРУППАМИ

В. С. Монахов

Гомельский государственный университет имени Ф. Скорины, Советская 104, 246019 Гомель, Беларусь
Victor.Monakhov@gmail.com

Все рассматриваемые группы предполагаются конечными. Используемая терминология соответствует [1].

Через $\pi(G)$ обозначается множество всех простых делителей порядка группы G. Запись $A \rtimes B$ означает полупрямое произведение нормальной подгруппы A и подгруппы B. Используются также следующие обозначения:

$H \leq G$ — H является подгруппой группы G;

$H < G$ — H является собственной подгруппой группы G;

$H <\cdot\, G$ — H является максимальной подгруппой группы G.

Подгруппой Картера называют нильпотентную самонормализуемую подгруппу.

Подгруппой Гашюца группы G называется подгруппа K, удовлетворяющая следующим двум условиям:

1) K сверхразрешима;

2) если $K \leq K_1 \leq K_2 \leq G$, то $|\, K_2 : K_1 \,|$ — не простое число.

Пусть $\mathfrak{F}$ — формация, G — группа, $\mathfrak{N}$ и $\mathfrak{U}$ — формации всех нильпотентных и сверхразрешимых групп соответственно. Пересечение всех нормальных подгрупп группы G, факторгруппы по которым принадлежат $\mathfrak{F}$, обозначается через $G^{\mathfrak{F}}$ и называется $\mathfrak{F}$-корадикалом группы G. Ясно, что $G^{\mathfrak{H}} \leq G^{\mathfrak{F}}$ для формаций $\mathfrak{F} \subseteq \mathfrak{H}$, в частности, $G^{\mathfrak{U}} \leq G^{\mathfrak{N}}$.

Подгруппа H группы G называется $\mathfrak{F}$-субнормальной, если существует цепочка подгрупп

$$H = H_0 <\cdot H_1 <\cdot \ \ldots <\cdot H_n = G,$$

такая, что $H_i/\mathrm{Core}_{H_i} H_{i-1} \in \mathfrak{F}$ для всех i. Это равносильно тому, что $H_i^{\mathfrak{F}} \leq \mathrm{Core}_{H_i} H_{i-1}$. Здесь $\mathrm{Core}_G H = \bigcap_{g \in G} H^g$ — ядро подгруппы H в группе G.

Класс групп, в которых все примарные циклические подгруппы $\mathfrak{U}$-субнормальны, обозначается через $\mathfrak{X}$. Группы из этого класса полностью описаны в работе В. С. Монахова и В. Н. Княгиной [2]. В частности, группа $G \in \mathfrak{X}$ тогда и только тогда, когда каждая подгруппа с нильпотентным коммутантом сверхразрешима. Группы, в которых все примарные подгруппы $\mathfrak{U}$-субнормальны, составляют класс $\mathrm{w}\mathfrak{U}$, полностью изученный в работе А. Ф. Васильева, Т. И. Васильевой и В. Н. Тютянова [3]. В частности, группа $G \in \mathrm{w}\mathfrak{U}$ тогда и только тогда, когда каждая метанильпотентная подгруппа сверхразрешима. Понятно, что $\mathrm{w}\mathfrak{U} \subset \mathfrak{X}$.

Подгруппа H группы G называется $\mathfrak{F}$-абнормальной, если $L/\mathrm{Core}_L K \notin \mathfrak{F}$ для всех подгрупп K и L таких, что $H \leq K <\cdot L \leq G$. Это равносильно тому, что $L^{\mathfrak{F}}$ не содержится в $\mathrm{Core}_L K$. Поэтому каждая $\mathfrak{H}$-абнормальная подгруппа $\mathfrak{F}$-абнормальна для формаций $\mathfrak{F} \subseteq \mathfrak{H}$, в частности, каждая $\mathfrak{U}$-абнормальная подгруппа $\mathfrak{N}$-абнормальна.

Общие свойства групп, у которых каждая подгруппа $\mathfrak{F}$-субнормальна или $\mathfrak{F}$-абнормальна, для наследственной насыщенной формации $\mathfrak{F}$ исследовались в [4–6]. Полное описание строения группы, в которой каждая подгруппа $\mathfrak{U}$-субнормальна или $\mathfrak{U}$-абнормальна, получили В. Н. Семенчук и А. Н. Скиба [7]. В этой работе они предложили следующую задачу.

Задача. *Какое строение имеет группа, у которой каждая нильпотентная подгруппа $\mathfrak{U}$-субнормальна или $\mathfrak{U}$-абнормальна?*

Решение этой задачи получено в следующей теореме.

Теорема. *В группе G каждая нильпотентная подгруппа $\mathfrak{U}$-абнормальна или $\mathfrak{U}$-субнормальна тогда и только тогда, когда либо $G \in \mathrm{w}\mathfrak{U}$, либо выполняются следующие утверждения:*

1) *силовская p-подгруппа P для некоторого $p \in \pi(G)$ является подгруппой Картера и P является подгруппой Гашюца; если $G \notin \mathfrak{X}$, то P циклическая; если $G \in \mathfrak{X} \setminus \mathrm{w}\mathfrak{U}$, то P нециклическая и p — наименьшее в $\pi(G)$;*

2) *$G^{\mathfrak{U}} = G^{\mathfrak{N}}$ — p'-холлова подгруппа группы G;*

3) *$R \leftthreetimes G^{\mathfrak{N}} \in \mathrm{w}\mathfrak{U}$ для всех $R < P$; в частности, все метанильпотентные подгруппы в $RG^{\mathfrak{N}}$ сверхразрешимы.*

Замечание. Согласно [3] для любого натурального n существует группа $G \in \mathrm{w}\mathfrak{U}$, нильпотентная длина которой равна n. Поэтому в теореме подгруппа $G^{\mathfrak{U}}$ может иметь любую нильпотентную длину. В частности, $G^{\mathfrak{U}}$ может быть несверхразрешимой в отличие от ситуации теоремы из [7].

Литература

1. Шеметков Л. А. *Формации конечных групп.* М.: Наука. 1978.

2. Monakhov V.S., Kniahina V.N. *Finite group with $\mathbb{P}$-subnormal subgroups* // Ricerche di Matematica. 2013. Vol. 62. № 2. P. 307–323.

3. Васильев А. Ф., Васильева Т. И., Тютянов В. Н. *О конечных группах сверхразрешимого типа* // Сибирский математический журнал. 2010. Т. 51. № 6. С. 1270–1281.

4. Förster P. *Finite groups all of whose subgroups are $\mathfrak{F}$-subnormal or $\mathfrak{F}$-subabnormal* // J. Algebra. 1986. Vol. 103. № 1. P. 285–293.

5. Семенчук В. Н. *Строение конечных групп с $\mathfrak{F}$-абнормальными или $\mathfrak{F}$-субнормальными подгруппами* // Вопросы алгебры. Минск: Университетское. 1986. № 2. С. 50–55.

6. Семенчук В. Н., Шевчук С. Н. *Конечные группы, у которых примарные подгруппы либо $\mathfrak{F}$-субнормальны, либо $\mathfrak{F}$-абнормальны* // Известия вузов. Математика. 2011. № 8. С. 46–55

7. Semenchuk V. N., Skiba A. N. *On one generalization of finite $\mathfrak{U}$-critical groups* // ArXiv. org e-Print archive, arXiv:1412.5469v1, 17 Dec 2014.

ВЛИЯНИЕ ОБОБЩЕННО СУБНОРМАЛЬНЫХ ПОДГРУПП НА ПРОИЗВЕДЕНИЯ КОНЕЧНЫХ ГРУПП

В.И. Мурашко, А.Ф. Васильев

Гомельский государственный университет им. Ф.Скорины, Советская 104, 246019 Гомель, Беларусь
mvimath@yandex.ru, formation56@mail.ru

Рассматриваются только конечные группы. Одним из содержательных направлений теории групп является изучение структуры группы, представимой в произведение своих подгрупп, в зависимости от свойств сомножителей. К первым результатам данного направления относится знаменитая теорема Бернсайда о разрешимости бипримарных групп.

Во многих работах изучались формации групп, замкнутые относительно взятия произведений определённого типа подгрупп (произвольных [1], нормальных (субнормальных) [2], абнормальных и контрнормальных [3] и т.д.).

В последние годы активно проводятся исследования формаций, замкнутых относительно произведений обобщенно субнормальных подгрупп. Здесь важную роль играет понятие $\mathfrak{F}$-субнормальной подгруппы, впервые введенное в классе разрешимых групп Т.О. Хоуксом в [4] и распространенное Л.А. Шеметковым в монографии [5] на произвольные группы.

Определение 1. Пусть $\mathfrak{F}$ — непустая формация. Подгруппа H группы G называется $\mathfrak{F}$-субнормальной в G, если либо $H = G$, либо существует максимальная цепь подгрупп $H = H_0 \subset H_1 \subset \cdots \subset H_n = G$ такая, что ${H_i}^{\mathfrak{F}} \subseteq H_{i-1}$ для $i = 1, \ldots, n$.

Формации, замкнутые относительно произведений $\mathfrak{F}$-субнормальных подгрупп, изучались в работах [6–8] и др. Важную роль в этих исследованиях играют формации с условием Шеметкова, т.е. формации $\mathfrak{F}$, у которых всякая минимальная не $\mathfrak{F}$-группа является либо группой Шмидта, либо циклической группой простого порядка.

В работе [9] в классе всех разрешимых групп была получена следующая характеризация формаций с условием Шеметкова.

Теорема 1. *Для наследственной насыщенной формации $\mathfrak{F}$ разрешимых групп следующие условия эквивалентны:*

(1) *$\mathfrak{F}$ содержит всякую разрешимую группу $G = AB$, у которой все циклические примарные подгруппы подгрупп A и B являются $\mathfrak{F}$-субнормальными в G.*

(2) *$\mathfrak{F}$ — формация с условием Шеметкова.*

В [10] Фиттинг показал, что произведение двух нормальных нильпотентных подгрупп нильпотентно, откуда следует, что во всякой группе существует единственная максимальная нормальная нильпотентная подгруппа $F(G)$, которую сейчас называют подгруппой Фиттинга. Эта подгруппа оказывает большое влияние на строение разрешимой группы.

В работе [11] авторами было рассмотрено еще одно обобщение субнормальности — понятие $F(G)$-субнормальной подгруппы.

Определение 2. Подгруппа H группы G называется $F(G)$-субнормальной, если H субнормальна в $HF(G)$.

В [11] изучались произведения $F(G)$-субнормальных подгрупп. В частности, была получена

Теорема 2. *Пусть группа $G = AB$ является произведением своих $F(G)$-субнормальных нильпотентных подгрупп. Тогда группа G нильпотентна.*

Для формулировки следующего результата нам потребуется конструкция прямого произведения наследственных насыщенных формаций групп [12, с. 96]. Пусть I — непустое множество. Для каждого $i \in I$ пусть $\mathfrak{F}_i$ — наследственная насыщенная формация. Предположим, что $\pi(\mathfrak{F}_i) \cap \pi(\mathfrak{F}_j) = \emptyset$ для всех $i, j \in I$, $i \neq j$. Обозначим $\pi_i = \pi(\mathfrak{F}_i)$. Тогда $\underset{i\in I}{\times}\mathfrak{F}_i = (G = O_{\pi_{i_1}}(G) \times \cdots \times O_{\pi_{i_n}}(G) | O_{\pi_{i_j}}(G) \in \mathfrak{F}_{i_j}, 1 \leq j \leq n, \{i_1, \ldots, i_n\} \subseteq I)$.

Теорема 3. *Пусть $\mathfrak{F}$ — насыщенная наследственная формация разрешимых групп и $\pi = \pi(\mathfrak{F})$. Следующие утверждения эквивалентны:*

(1) *$\mathfrak{F}$ содержит всякую разрешимую группу $G = AB$, у которой A и B — $F(G)$-субнормальные $\mathfrak{F}$-подгруппы.*

(2) *Существует такое разбиение $\sigma = \{\pi_i | i \in I\}$ множества простых чисел π на попарно непересекающиеся подмножества, что $\mathfrak{F} = \underset{i\in I}{\times}\mathfrak{S}_{\pi_i}$.*

По известной теореме Дёрка [13] группа сверхразрешима, если она содержит четыре сверхразрешимые подгруппы с попарно взаимно простыми индексами. Фрисен [14] заметил, что если группа G есть произведение двух нормальных (субнормальных) сверхразрешимых подгрупп, имеющих взаимно простые индексы в ней, то она сверхразрешима. Следующий пример показывает, что в теореме Фрисена условие субнормальности нельзя заменить на $F(G)$-субнормальность. Пусть G — группа, изоморфная симметрической группе степени 3. Тогда существует точный неприводимый F_7G-модуль V размерности 2 над полем F_7. Пусть T — полупрямое произведение V и G. Рассмотрим $A = VG_3$ и $B = VG_2$, где G_p — силовская p-подгруппа G и $p \in \{2, 3\}$. Так как $7 \equiv 1 (\mathrm{mod}\ p)$ для $p \in \{2, 3\}$, то нетрудно видеть, что A и B сверхразрешимы. Так как V — точный неприводимый F_7G-модуль, то $F(T) = V$. Таким образом, A и B — $F(T)$-субнормальные подгруппы T. Заметим, что $T = AB$, но T, в силу свойств F_7G-модуля V, не является сверхразрешимой группой. Тем не менее верна следующая

Теорема 4. *Пусть A, B и C — $F(G)$-субнормальные сверхразрешимые подгруппы группы G. Если индексы A, B и C в G попарно взаимно просты, то G сверхразрешима.*

Литература

1. Амберг Б., Казарин Л. С., Хёфлинг Б. *Конечные группы с кратными факторизациями* // Фундамент. и прикл. матем. 1998. Т. 4. Вып. 4. С. 1251–1263.

2. Bryce R. A., Cossey J. *Fitting formations of finite soluble groups* // Math. Z. 1972. Bd. 127. № 3. S. 217–233.

3. Vasil'ev A. F. *On Products of Nonnormal Subgroups of Finite Groups* // Acta Applicandae Mathematicae. 2005. V. 85. № 1. P. 305–311.

4. Hawkes T. *On formation subgroups of a finite soluble group* // J. London Math. Soc. 1969. V. 44. P. 243–250.

5. Шеметков Л. А. *Формации конечных групп.* М.: Наука, 1978.

6. Семенчук В. Н. *Разрешимые F-радикальные формации* // Матем. заметки. 1996. Т. 59. № 2. С. 261–266.

7. Семенчук В. Н., Шеметков Л. А. *Сверхрадикальные формации* // Докл. НАН Беларуси. 2000. Т. 44. № 5. С. 24–26.

8. Каморников С. Ф., Тютянов В. Н. *Об одном классе наследственных насыщенных сверхрадикальных формаций* // Сиб. мат. журн. 2014. Т. 55. № 1. С. 97–108.

9. Мурашко В. И. *Классы конечных групп с обобщенно субнормальными циклическими примарными подгруппами* // Сиб. мат. журн. 2014. Т. 55. № 6. С. 1353–1367

10. Fitting H. *Beiträge zur Theorie der endlichen Gruppen* // Jahresber. Deutsch. Math.-Verein. 1938. Bd. 48. S. 77–141.

11. Мурашко В. И., Васильев А. Ф. *О произведениях частично субнормальных подгрупп конечных групп* // Вестник ВГУ. 2012. Т. 70. № 4. С. 24–27.

12. Ballester-Bolinches A., Ezquerro L. M. *Classes of Finite Groups.* Dordrecht: Springer, 2006.

13. Doerk K. *Minimal nicht überauflösbare, endliche Gruppen* // Math. Z. 1966. Bd. 91. № 3. S. 198–205.
14. Friesen D. K. *Products of Normal Supersolvable Subgroups* // Proc. Amer. Math. Soc. 1971. V. 30. № 1. P. 46–48.

КОМПОЗИЦИОННЫЕ ФОРМАЦИИ *ca*-$\mathfrak{F}$-ГРУПП И ПРОИЗВЕДЕНИЯ ВЗАИМНО ПЕРЕСТАНОВОЧНЫХ ПОДГРУПП

Е.Н. Мысловец

Гомельский государственный университет им. Ф. Скорины, Советская 104, 246019 Гомель, Беларусь
myslovets@gmail.com

Рассматриваются только конечные группы. Важной задачей теории групп является изучение формаций. Напомним, что формацией называется класс групп, замкнутый относительно взятия гомоморфных образов и подпрямых произведений. В 1963 году в работе [1] Гашюц положил начало систематическому изучению формаций групп. Он ввел понятие насыщенной формации, которое в настоящее время является классическим и активно применяется в исследовании различных вопросов теории групп и ее приложений в теории формальных языков и автоматов (см. [2]).

В связи с вопросом построения насыщенных формаций в работе [3] было введено понятие локальной формации. В дальнейшем было доказано, что всякая непустая формация является насыщенной тогда и только тогда, когда она является локальной [4, IV, Теорема 4.6].

Наряду с локальными формациями важную роль играют композиционные формации. Впервые композиционные формации были введены и рассматривались Л.А. Шеметковым в [5]. Пусть J — класс всех простых групп, а $\mathcal{K}_G$ — множество всех композиционных факторов группы G, взятых с точностью до изоморфизма. Отображение $f : \mathfrak{J} \to \{\text{формации}\}$ называется композиционным экраном. Формация $\mathfrak{F}$ называется композиционной, если она имеет хотя бы один композиционный экран f такой, что $\mathfrak{F} = (G \in \mathfrak{G} \mid G/C_G(H/K) \in f(A)$ для любого главного фактора H/K и $A \in \mathcal{K}_{H/K})$. Наряду с этим, композиционные формации рассматривались в другой терминологии Р. Бэром в неопубликованной рукописи (отмечено в [4, IV, стр. 370]). Р. Бэр ввел понятие разрешимо насыщенной формации. Напомним, что формация $\mathfrak{F}$ называется разрешимо насыщенной, если из того, что $G/\Phi(G_{\mathfrak{S}}) \in \mathfrak{F}$, всегда следует, что $G \in \mathfrak{F}$. Эквивалентность двух понятий дает теорема Бэра [4, IV, Теорема 4.17] о том, что непустая формация является композиционной тогда и только тогда, когда она разрешимо насыщенная. Каждая локальная формация является композиционной. Класс всех квазинильпотентных групп является примером композиционной формации, не являющейся локальной.

Композиционные формации нашли применение при изучении формационной стабильности при действии групп автоморфизмов, свойств корадикалов, гиперцентров, исследовании алгебры формаций и других вопросов. Однако, в отличие от локальных формаций применение композиционных формаций при изучении произведений групп до последнего времени оставалось незначительным. Это объясняется отсутствием достаточного количества конкретных конструкций и примеров композиционных формаций. Поэтому возникает задача конструирования новых примеров композиционных формаций, полезных для изучения факторизаций групп. Пример такой конструкции был предложен Го Вэньбинем и А.Н. Скибой в работах [6, 7]. В настоящей работе продолжены исследования в данном направлении.

В.А. Ведерников в [8] ввел понятие c-сверхразрешимой группы. Напомним, что группа G называется c-сверхразрешимой, если она обладает главным рядом, все факторы которого изоморфны простым группам. Свойства класса $\mathfrak{U}_c$ всех c-сверхразрешимых групп были изучены А.Ф. Васильевым и Т.И. Васильевой в работе [9]. В частности, они доказали, что

класс $\mathfrak{U}_c$ является композиционной, но ненасыщенной формацией. В работе [10] Д. Робинсон установил структурные свойства c-сверхразрешимых групп (в терминологии [10] SC-групп).

В работе [11] было введено понятие конечной ca-$\mathfrak{F}$-группы, являющееся обобщением c-сверхразрешимости. Были установлены основные свойства класса $\mathfrak{F}_{ca}$ всех ca-$\mathfrak{F}$-групп и произведений нормальных ca-$\mathfrak{F}$-подгрупп.

Определение [11]. Пусть $\mathfrak{F}$ — класс групп. Будем говорить, что группа G является ca-$\mathfrak{F}$-группой, если ее каждый неабелевый главный фактор является простой группой, а для каждого ее абелевого главного фактора H/K выполняется $H/K \leftthreetimes C_G(H/K) \in \mathfrak{F}$.

Теорема 1 [11]. *Пусть $\mathfrak{F}$ — насыщенная формация и f — ее максимальный внутренний локальный экран. Тогда формация $\mathfrak{F}_{ca}$ является композиционной и имеет максимальный внутренний композиционный экран h такой, что $h(N) = \mathfrak{F}_{ca}$, если N — простая неабелева группа и $h(N) = f(p)$, если N — простая p-группа, где p — простое число.*

Следующая теорема описывает структурные свойства конечной ca-$\mathfrak{F}$-группы.

Теорема 2. *Пусть $\mathfrak{F}$ — разрешимая насыщенная формация. Группа G является ca-$\mathfrak{F}$-группой тогда и только тогда, когда G удовлетворяет следующим утверждениям:*

1) $G^{\mathfrak{S}} = G^{\mathfrak{F}}$;

2) если $G^{\mathfrak{S}} \neq 1$, то $G^{\mathfrak{S}}/Z(G^{\mathfrak{S}})$ является прямым произведением G-инвариантных простых групп;

3) $Z(G^{\mathfrak{S}}) \subseteq Z_{\mathfrak{F}}(G)$.

Следуя [12, с. 149], группу $G = HK$ будем называть произведением взаимно перестановочных подгрупп H и K, если H перестановочна с любой подгруппой из K, а K перестановочна с любой подгруппой из H.

Теорема 3. *Пусть $\mathfrak{F}$ — насыщенная формация, содержащая класс $\mathfrak{U}$ всех сверхразрешимых групп. Если группа $G = HK$ — произведение взаимно перестановочных ca-$\mathfrak{F}$-подгрупп H и K и коммутант G' группы G квазинильпотентен, то G — ca-$\mathfrak{F}$-группа.*

Если $\mathfrak{F} = \mathfrak{U}$, то справедливо следующее

Следствие 3.1 [13]. *Пусть $G = HK$ — произведение взаимно перестановочных подгрупп H и K. Если H и K c-сверхразрешимы и коммутант G' группы G квазинильпотентен, тогда G — c-сверхразрешимая группа.*

Литература

1. Gaschütz W. *Zur Theorie der endlichen auflösbaren Gruppen* // Math. Z. 1963. Bd. 80. № 4. S. 300–305.

2. Ballester-Bolinches A., Pin J.-E., Soler-Escriva X. *Languages associated with saturated formations of groups* // Forum Mathematicum. 2013. V. 27. № 3. P. 1471–1505.

3. Gaschütz W., Lubeseder U. *Kennzeichnung gesättigter Formationen* // Math. Z. 1963. Bd. 82. S. 198–199.

4. Doerk K., Hawkes T. *Finite soluble groups*. Berlin; New York: Walter de Gruyter, 1992.

5. Шеметков Л. А. *Два направления в развитии непростых конечных групп (доклад, прочитанный на XII Всесоюзном алгебраическом коллоквиуме в Свердловске в сентябре 1973 г.)* // Успехи мат. наук. 1975. Т. 30. № 2. С. 179–198.

6. Guo W., Skiba A. N. *On finite quazi-$\mathfrak{F}$-groups* // Communication in Algebra. 2009. V. 37. P. 470–481.

7. Guo W., Skiba A. N. *On some classes of finite quazi-$\mathfrak{F}$-groups* // Journal of Group Theory. 2009. V. 12. P. 407–417.

8. Ведерников В. А. *О некоторых классах конечных групп* // Докл. АН БССР. 1988. Т. 32. № 10. С. 872–875.

9. Васильев А. Ф., Васильева Т. И. *О конечных группах, у которых главные факторы являются простыми группами* // Изв. вузов. Сер. Математика. 1997. Т. 426. № 11. С. 10–14.

10. Robinson D. J. S. *The structure of finite groups in which permutability is a transitive relation* // J. Austral. Math. Soc. 2001. V. 70. P. 143-149.

11. Мысловец Е. Н. *О конечных ca-$\mathfrak{F}$-группах* // Проблемы физики, математики и техники. 2014. Т. 2. № 19. С. 64-68.

12. Ballester-Bolinches A., Esteban-Romero R., Asaad M. *Products of Finite Groups*. Berlin: Walter de Gruyter, 2010.

13. Ballester-Bolinches A., Cossey J., Pedraza-Aguilera M. C. *On mutually permutable products of finite groups* // Journal of Algebra. 2005. V. 294. P. 127-135.

О КОНГРУЭНЦИЯХ НА ПОЛУГРУППЕ ЛИНЕЙНЫХ ОТНОШЕНИЙ

М.И. Наумик

Витебский государственный университет имени П.М. Машерова
Московский пр-т 33, 210038 Витебск, Беларусь naumik@tut.by

Пусть V — векторное пространство над телом. Напомним, что линейное отношение [1] на V — это подпространство пространства $V \oplus V$, и обозначается мультипликативная полугруппа всех линейных отношений на V через $LR(V)$. В [2] были описаны все конгруэнции полугруппы $LR(V)$. В данной работе доказана следующая

Теорема. *Решетка конгруэнций на полугруппе $LR(V)$ является дистрибутивной решеткой.*

Следствие. *Решетка конгруэнций полугруппы линейных преобразований является дистрибутивной решеткой.*

Литература

1. Маклейн С. *Алгебра аддитивных отношений* // Сб. переводов. Математика. 1963. № 7:6. С. 3–12.

2. Наумик М. И. *Полугруппа линейных отношений* // Докл. НАН Беларуси. 2004. Т. 48. № 3. С. 34–37.

О ПРОНОРМАЛЬНОСТИ И СИЛЬНОЙ ПРОНОРМАЛЬНОСТИ ХОЛЛОВЫХ ПОДГРУПП

М.Н. Нестеров

Новосибирский государственный университет, Механико-математический факультет
Пирогова 2, 630090 Новосибирск, Россия mauk00@mail.ru

Всюду через π обозначается некоторое фиксированное множество простых чисел. Подгруппа H конечной группы G называется **π-холловой**, если она является π-группой (т.е. все простые делители ее порядка лежат в π), а ее индекс не делится на числа из π. Подгруппа H называется **холловой** подгруппой, если она является π-холловой для некоторого множества π (эквивалентно, если $|H|$ и $|G : H|$ взаимно просты).

Говорят, что подгруппа H группы G **пронормальна**, если для любого элемента $g \in G$ подгруппы H и H^g сопряжены в подгруппе $\langle H, H^g \rangle$.

В «Коуровской тетради» записана следующая проблема [1, 18.32]: всегда ли холлова подгруппа конечной группы пронормальна в своём нормальном замыкании? Отрицательное решение проблемы даёт следующая

Теорема. *Пусть множество простых чисел π таково, что*

(1) *существует простая группа X, содержащая более одного класса сопряжённых π-холловых подгрупп;*

(2) *существует простая группа Y, содержащая π-холлову подгруппу, отличную от своего нормализатора в Y.*

Тогда в регулярном сплетении $G = X \wr Y$ существует непронормальная π-холлова подгруппа, нормальное замыкание которой совпадает с G.

Условиям теоремы удовлетворяет, например, множество $\{2,3\}$: группа $X = PSL_3(2)$ содержит два класса сопряжённых $\{2,3\}$-холловых подгрупп и группа $Y = PSL_2(16)$ содержит $\{2,3\}$-холлову подгруппу, отличную от своего нормализатора в Y.

Подгруппу H группы G называют **сильно пронормальной**, если для любой подгруппы $K \leq H$ и любого элемента $g \in G$ подгруппа K^g сопряжена с некоторой подгруппой из H (но необязательно с K) с помощью элемента из $\langle H, K^g \rangle$.

Получено также отрицательное решение проблемы [1, 17.45(б)]: верно ли, что холловы подгруппы простых групп сильно пронормальны? А именно, показано, что $PSp_{10}(7)$ содержит $\{2,3\}$-холлову подгруппу, не являющуюся сильно пронормальной. Отметим, что ранее не было известно примеров пронормальных, но не сильно пронормальных холловых подгрупп.

Работа выполнена при финансовой поддержке РНФ (проект 14-21-00065).

Литература

1. *Коуровская тетрадь: нерешённые вопросы теории групп.* Изд. 18. Новосибирск, 2014.

О СИЛОВСКИХ СИСТЕМАХ КОНЕЧНЫХ ГРУПП

Э.М. Пальчик

Полоцкий государственный университет
Блохина 29, 211440 Новополоцк, Витебская обл., Беларусь bashunsviat@mail.ru

Обозначения и терминология стандартные [1 – 3].

Ф. Холл ввел понятие силовской системы для конечной разрешимой группы G [1, определение VI.2.1 b)]. Это набор силовских подгрупп группы G, взятых по одной для каждого $p \in \pi(G)$, которые попарно перестановочны.

В связи с прогрессом теории конечных групп были получены фундаментальные результаты в области теорем силовского типа для холловых подгрупп конечных групп, полученные в основном трудами Ф. Гросса, Е.Р. Вдовина и Д.О. Ревина [3].

С использованием этих результатов появилась возможность обобщить понятие силовской системы для разрешимых групп.

Определение 1. Множество $\mathfrak{S} = \{G_s, ..., G_t\}$, где $\{s, ..., t\}$ — все различные простые делители порядка $|G|$ конечной группы G, назовем специальной силовской системой группы G, если G_s перестановочна со всеми подгруппами множества $\mathfrak{S}$ (кратко: CCG_s–система).

Если $s = 2$, то может быть доказан следующий результат.

Теорема 1. *Следующие свойства конечной группы эквивалентны:* (1) *G–разрешимая группа;* (2) *G имеет силовскую систему в смысле Ф. Холла;* (3) *G имеет CCG_2–систему.*

Доказательство. То, что (1) $\Leftrightarrow$ (2) доказано Ф. Холлом [1, теорема VI.2.3]. Докажем, что (3) $\Leftrightarrow$ (1). Ясно, что достаточно доказать, что (3) $\Rightarrow$ (1).

Предположим, что G — простая неабелева группа. Если $G \in \{A_n, n \geq 5\}$, то G не имеет CCG_2–системы [3, теорема 8.1, табл.2]. Если $G \in Spor$, то G не имеет CCG_2–системы [3, теорема 8.2, табл.4; 4, гл.5, раздел 5.3].

Предположим, что $\overline{G} \in Chev(q)$, $q = p^f$, $G = \overline{G}/Z(\overline{G})$, $p > 2$. По условию в G и $\overline{G}$ есть холлова $\{2,p\}$–подгруппа $\overline{T}$. По [3, теорема 8.3] $\overline{T}$ лежит в подгруппе Бореля $\overline{B}$ группы $\overline{G}$ (так как $\overline{T}$ — разрешимая группа, то она не отличная от $\overline{B}$ параболическая подгруппа [2, с.87 и следствие 2.16, с.86]). Если $p > 2$, то $\overline{G}_2$ — абелева группа [2, с.61]. По теореме Дж.Уолтера [2, теорема 4.126] $G \in \{L_2(2^f); L_2(q), q \equiv \pm 3 \pmod 8, J_1, {}^2G_2(q)\}$. Эти группы не имеют CCG_2–систем [1, теорема II.8.27; 3, табл.10; 3, табл.4; 3, табл.9]. (Например, у групп ${}^2G_2(q)$ по [3, табл.9] все простые делители $t \neq 2, 3$ лежали бы в $\pi(q-1)$, или в $\pi(q+1)$,

или в $\{7\}$, что невозможно). Если же $p = 2$, то по [3, теорема 8.3] все силовские подгруппы нечетного порядка должны лежать в подгруппе Бореля $\overline{B}$. Но тогда $\overline{G}_2 \lhd \overline{G}$ и $G' \neq G$. Итак, G — не простая группа. Пусть $1 \neq M \lhd G$, $M \subset G$. Тогда $G_2G_t \cap M = M_2M_t$ для всех $t \in \pi(G) \cap \pi(M)$. По заключению индукции (3) $\Leftrightarrow$ (1) в M. Точно так, ввиду [1, лемма I.7.7], $G/M = G^*$ имеет CCG_2^*–систему и (3) $\Leftrightarrow$ (1). Но тогда и группа G разрешима. Теорема доказана.

Группа G с CCG_3–системой может быть и простой. Например, $G \cong L_3(q)$, $12|(q+1)$, $9 \nmid (q+1)$.

Теорема 2. *Пусть s — наибольший простой делитель порядка конечной группы G. Если G имеет CCG_s–систему, то она является s–разрешимой группой.*

Доказательство. Как и в доказательстве теоремы 1, сразу считаем, что $\overline{G} \in Chev(q)$, $q = p^f$, $G = \overline{G}/Z(\overline{G})$.

По условию в G и $\overline{G}$ есть холловы $\{t, s\}$–подгруппы T и $\overline{T}$ для всех $t \notin \{2, p\}$, $t \in \pi(G)$. Пусть $s \neq p$. Так как $t < s$, то по [5, теорема 1] $\overline{T}_s \lhd \overline{T}$. Поэтому $\overline{N} = N_{\overline{G}}(\overline{T}_s)$ имеет в $\overline{G}$ примарный или бипримарный индекс i (ввиду $\overline{T}_s \not\lhd \overline{G}$) и $\pi(i) \subset \{2, p\}$. Если индекс примарный, то по [6, теорема 5.8] G такая группа, что не имеет CCG_s–систем. Если N имеет в G бипримарный индекс, то по [7] N есть разрешимая подгруппа в $G \in \{L_2(q), L_3(3), L_3(5), PSp_4(3), U_3(3), U_3(4), U_3(7), U_5(2), M_{11}, M_{12}\}$. По [3, табл.3, 4, 7] эти группы не имеют CCG_s–систем. Если $s = p$, то, как и в доказательстве теоремы 1, $G_s \lhd G$. Поэтому G — не простая группа и утверждение доказывается как и в теореме 1. Теорема доказана.

С использованием теорем 1, 4, леммы 14 в [5], теорем 8.3, 8.8, 8.9 в [3] и теоремы Жигмонди (частный случай теоремы Фейта [7, лемма 2.1]) доказывается следующий общий факт.

Теорема 3. *Пусть s — простой делитель порядка конечной группы G, $s > 3$. Если G имеет CCG_s–систему, то она является s–разрешимой группой.*

Из теорем 1 и 3 не сложно получить

Следствие. *Пусть G — конечная группа с CCG_s–системой, $s \neq 3$. Пусть $\pi \subset \pi(G)$ и $s \notin \pi$. Если индексы нормализаторов силовских подгрупп G_t, $t \in \pi$, взаимно просты с s, то в G есть G_s–инвариантная s'–подгруппа $K = \langle G_t / t \in \pi \rangle$.*

Литература

1. Huppert B. *Endliche Gruppen*, I. Berlin: Springer-Verlag, 1967.

2. Горенстейн Д. *Конечные простые группы. Введение в их классификацию*. М.: Мир, 1985.

3. Вдовин Е. П., Ревин Д. О. *Теоремы силовского типа* // Успехи мат.н. 2011. Т. 66. № 5(401). С. 3–46.

4. Gorenstein D., Lyons R., Solomon R. *The classification of the finite simple groups* // Math. Surveys and Monogr. 1998. Vol. 40. No 3. P. 1–419.

5. Вдовин Е. П., Ревин Д. О. *Холловы подгруппы нечетного порядка в конечных группах* // Алгебра и логика. 2002. Т. 41. № 1. С. 15–56.

6. Arad Z., Fisman E. *On finite factorizable group* // J. Algebra. 1984. Vol. 86. No 2. P. 522–548.

7. Li C. H., Li X. *On permutation groups of degree a product of two prime-powers* // Commun. Algebra. 2014. Vol. 42. P. 4722–4743.

КОНЕЧНЫЕ ПРОСТЫЕ ГРУППЫ, В КОТОРЫХ НОРМАЛИЗАТОР СИЛОВСКОЙ s–ПОДГРУППЫ ИМЕЕТ БИПРИМАРНЫЙ ИНДЕКС

Э.М. Пальчик, С.Ю. Башун

Полоцкий государственный университет
Блохина 29, 211440 Новополоцк, Витебская обл., Беларусь bashunsviat@mail.ru

Обозначения и терминология стандартные [1, 2].

Бипримарное число i — число вида $i = t^a \cdot r^b$, $a > 0$, $b > 0$, t и r — различные простые числа. Пусть $\mathfrak{M}$ обозначает множество следующих групп G с указанными свойствами их разрешимых максимальных подгрупп $M <\cdot G$ индекса i (всюду ниже $k \geq 0$):

$\mathfrak{M}(1)$ $L_2(q)$, $q = 2^{2^k}$, $M \cong D_{2(q-1)}$, $i = 2^{2^k-1}(q+1)$, $q+1$ — простое число Ферма;

$\mathfrak{M}(2)$ $L_2(q)$, $q = 2^f$, $M \cong D_{2(q+1)}$, $i = 2^{f-1}(q-1)$, $q-1$ — простое число Мерсенна;

$\mathfrak{M}(3)$ $L_2(q)$, $q = p^{2^k}$, $M \cong D_{q-1}$, $i = q(q+1)/2$, $p > 2$, $(q+1)/2$ — степень простого числа;

$\mathfrak{M}(4)$ $L_2(p)$, $M \cong D_{p+1}$, $i = p \cdot (p-1)/2$, $(p-1)/2$ — степень простого числа, $p > 2$;

$\mathfrak{M}(5)$ $L_2(q)$, $q = p^f$, $p \geq 2$, $M = N_G(G_p)$, $i = q+1$, $f = 2^k \cdot f_0$, $f_0 = 1$ или простое число.

В работе [3] описаны неабелевы композиционные факторы конечных групп, у которых нормализатор силовской s–подгруппы имеет примарный индекс ($i = t^a$).

В этой заметке доказывается похожий результат.

Теорема. *Пусть s — простое число и нормализатор N силовской s–подгруппы в конечной простой группе G имеет бипримарный индекс $i = t^a \cdot r^b$. Тогда*

(1) $s = 2$, $G \in \{A_6; L_2(q) \in \mathfrak{M}(5)$ *с* $p = 2$; $L_2(11)$, $N \cong A_4$; $L_2(13)$, $N \cong A_4$; $L_3(3)$; $L_3(8)$, $i = 3^2 \cdot 73$; $U_3(3)$, $i = 3^3 \cdot 13$; $U_3(8)$, $i = 3^3 \cdot 19$; $PSp_4(3)$, $i = 3^3 \cdot 5$; $Sz(8)$, $i = 5 \cdot 13$; $Sz(32)$, $i = 5^2 \cdot 41\}$;

(2) $s = 3$, $G \in \{A_5$; A_6; M_{11}, $N \cong E_9.QD_{16}$; $L_2(q) \in \mathfrak{M}(1)$, $3|(q-1)$, $N = M$; $L_2(q) \in \mathfrak{M}(2)$, $3|(q+1)$, $N = M$; $L_2(q) \in \mathfrak{M}(3)$, $3|(q-1)$, $N = M$; $L_2(q) \in \mathfrak{M}(4)$, $3|(p+1)$, $N = M$; $L_2(q) \in \mathfrak{M}(5)$ *с* $p = 3$, $M = N$; $PSp_4(3)$, $i = 2^5 \cdot 5$; $U_3(3)$, $N = G_3 \leftthreetimes Z_8$; $L_3(3)$, $i = 2^2 \cdot 13\}$;

(3) $s > 3$, $G \in \{A_5$, $s = 5$; A_6, $s = 5$; M_{11}, $s = 11$; M_{12}, $s = 11$; $L_3(3)$, $s = 13$; $L_3(5)$, $s = 31$; $U_3(3)$, $s = 7$; $U_3(4)$, $s = 5, 13$; $L_2(q) \in \mathfrak{M}(1)$, $s|(q-1)$, $N = M$; $L_2(q) \in \mathfrak{M}(2)$, $s|(q+1)$, $N = M$; $L_2(q) \in \mathfrak{M}(3)$, $s|(q-1)$, $N = M$; $L_2(q) \in \mathfrak{M}(4)$, $s|(p+1)$, $N = M$; $L_2(q) \in \mathfrak{M}(5)$, $N = M$, $U_3(7)$, $s = 43$, $i = 2^7 \cdot 7^3$; $U_5(2)$, $s = 11$, $i = 2^{10} \cdot 3^5$; $PSp_4(3)$, $s = 5\}$.

Доказательство. Так как N есть s–разрешимая подгруппа бипримарного индекса в простой группе G, то из лемм 3.1, 4.1, 4.2, 4.3, 4.4, 4.5, 5.1 в [4] непосредственно видно какие группы G имеют s–разрешимые подгруппы K бипримарного индекса, $s \in \pi(K)$. В этих леммах указано и строение таких подгрупп. Среди таких подгрупп нормализаторами силовских s–подгрупп являются те, которые указаны в заключении теоремы. Теорема доказана.

Литература

1. Huppert B. *Endliche Gruppen*, I. Berlin: Springer-Verlag, 1967.

2. Горенстейн Д. *Конечные простые группы. Введение в их классификацию.* М.: Мир, 1985.

3. Кондратьев А. С., Го В. *Конечные группы, в которых нормализаторы силовских* 3*–подгрупп имеют нечетные или примарные индексы* // Сиб. матем.ж. 2009. Т. 50. № 2. С. 344–349.

4. Li C. H., Li X. *On permutation groups of degree a product of two prime-powers* // Commun. Algebra. 2014. Vol. 42. P. 4722–4743.

О СОБСТВЕННЫХ ПОДФОРМАЦИЯХ ОДНОПОРОЖДЕННОЙ НАСЛЕДСТВЕННОЙ ω-НАСЫЩЕННОЙ ФОРМАЦИИ

В.М. Селькин

Гомельский госуниверситет им.Ф.Скорины, Советская 104, 246019 Гомель, Беларусь
selkin69@mail.ru

Все рассматриваемые группы предполагаются конечными. Используется общепринятая терминология [1–4].

Пусть ω — произвольное непустое множество простых чисел. Всякая функция вида $f : \omega \cup \{\omega'\} \to \{\text{формации групп}\}$ называется ω-локальным спутником [4]. Символом $LF_\omega < f >$ обозначим класс групп $(G|G/O_\omega(G) \in f(\omega')$ и $G/F_p(G) \in f(p)$ для всех $p \in \omega \cap \pi(G))$. Если для формации $\mathfrak{F}$ мы имеем равенство $\mathfrak{F} = LF_\omega < f >$, то говорим, что f — ω-локальный V-спутник формации $\mathfrak{F}$. В этом случае, мы называем $\mathfrak{F}$ ω-насыщенной формацией.

Формация $\mathfrak{F}$ называется однопорожденной наследственной ω-насыщенной формацией, если в $\mathfrak{F}$ найдется такая группа G, что $\mathfrak{F}$ совпадает с пересечением всех тех наследственных ω-насыщенных формаций, которые содержат G.

Максимальная наследственная ω-насыщенная подформация формации $\mathfrak{F}$ — такая собственная наследственная ω-насыщенная подформация $\mathfrak{M}$ формации $\mathfrak{F}$, что для любой наследственной ω-насыщенной формации $\mathfrak{H}$ с условием $\mathfrak{M} \subseteq \mathfrak{H} \subset \mathfrak{F}$ имеет место $\mathfrak{M} = \mathfrak{H}$.

Теорема. *Всякая собственная наследственная ω-насыщенная подформация однопорожденной наследственной ω-насыщенной формации $\mathfrak{F}$ содержится в некоторой максимальной наследственной ω-насыщенной подформации формации $\mathfrak{F}$.*

Литература

1. Шеметков Л. А. *Формации конечных групп.* М.: Наука, 1978.
2. Шеметков Л. А., Скиба А. Н. *Формации алгебраических систем.* М.: Наука, 1989.
3. Скиба А. Н. *Алгебра формаций.* Мн.: Беларуская навука, 1997.
4. Shemetkov L. A., Skiba A. N. *Multiply ω-local formations and Fitting classes of finite groups* // Matem. Trudy. 1999. №2. P. 114–147.

О ПЕРЕСЕЧЕНИИ НЕНИЛЬПОТЕНТНЫХ МАКСИМАЛЬНЫХ ПОДГРУПП

М.В. Селькин, Р.В. Бородич, Е.Н. Бородич, С.Н. Быков

Гомельский государственный университет имени Ф. Скорины
Советская 104, 246019 Гомель, Беларусь {Selkin, Borodich, EBorodich}@gsu.by

Все рассматриваемые группы конечны. Исследование пересечений максимальных подгрупп является одной из классических задач восходящих к работе Фраттини [1]. В 50-х годах теорема Фраттини получила развитие в работах Гашюца [2], Дескинса [3]. Дальнейший интерес к подгруппам фраттиниевого типа, в значительной степени, связан с развитием теории формаций (см. монографию [4]).

Теорема. *В любой неразрешимой группе подгруппа, равная пересечению всех ненильпотентных абнормальных максимальных подгрупп, не сопряжённых с данной ненильпотентной абнормальной максимальной подгруппой, метанильпотентна.*

Следствие. *В любой неразрешимой группе подгруппа, равная пересечению всех абнормальных максимальных подгрупп, не сопряжённых с данной абнормальной подгруппой, метанильпотентна.*

Литература

1. Frattini G. *Intorno alla generasione dei gruppi di operazioni* // Atti Acad. Dei Lincei. 1885. Vol. 1. P. 281–285.

2. Gaschütz W. *Über die* Φ*-Untergruppen endlicher Gruppen* // Math. Z. 1953. Bd. 58. S. 160–170.

3. Deskins W. E. *A condition for the solvability of a finite group* // III.J.Math. 1961. Vol. 5. № 2, P. 306–313.

4. Селькин М. В. *Максимальные подгруппы в теории классов конечных групп.* Мн.: Беларуская навука, 1997.

КОНЕЧНЫЕ ГРУППЫ, У КОТОРЫХ ВСЕ СОБСТВЕННЫЕ ПОДГРУППЫ ЛИБО ОБОБЩЕННО СУБНОРМАЛЬНЫ, ЛИБО ОБОБЩЕННО АБНОРМАЛЬНЫ

В. Н. Семенчук

Гомельский государственный университет имени Ф. Скорины, Советская 104, 246019 Гомель, Беларусь
semenchuk@gsu.by

Рассматриваются только конечные группы. В работе [1] Фаттахи изучил группы, у которых любая собственная подгруппа либо нормальна, либо абнормальна. Затем Эберт и Бауман в работе [2] изучили группы, у которых любая собственная подгруппа либо субнормальна, либо абнормальна. В теории классов конечных групп естественным обобщением понятия субнормальности и абнормальности являются понятия $\mathfrak{F}$-субнормальности и $\mathfrak{F}$-абнормальности. Здесь $\mathfrak{F}$ — некоторая формация, т. е. класс групп, замкнутых относительно гомоморфных образов и подпрямых произведений.

В 1986 году соответственно в работах [3,4] Ферстер и В. Н. Семенчук изучали группы, у которых собственные подгруппы $\mathfrak{F}$-субнормальны или $\mathfrak{F}$-абнормальны. Дальнейшее развитие данного направления связано с работой В. Н. Семенчука и С. Н. Шевчука [5], в которой ограничения накладывались только на примарные подгруппы.

Важный шаг в развитии данного направления связан с работой В. Н. Семенчука и А. Н. Скибы [6], где описаны группы, у которых собственные подгруппы $\mathfrak{U}$-субнормальны или $\mathfrak{U}$-абнормальна для формации $\mathfrak{U}$ всех сверхразрешимых групп.

Формация называется наследственной, если она замкнута относительно взятия подгрупп, и насыщенной, если она замкнута относительно фраттиниевых расширений.

Группа называется минимальной не $\mathfrak{F}$-группой, если она не принадлежит $\mathfrak{F}$, но все ее собственные подгруппы принадлежат $\mathfrak{F}$. В частности, ненильпотентная группа, у которой все собственные подгруппы нильпотентны, называется группой Шмидта.

Важную роль в дальнейших исследованиях сыграли формации Шеметкова, т. е. формации $\mathfrak{F}$, у которых все минимальные не $\mathfrak{F}$-группы являются группами Шмидта или группами простых порядков.

Теорема. *Пусть $\mathfrak{F}$ — насыщенная наследственная формация Шеметкова, содержащая все нильпотентные группы. Тогда и только тогда любая собственная подгруппа группы $G \notin \mathfrak{F}$ либо $\mathfrak{F}$-субнормальна, либо $\mathfrak{F}$-абнормальная, когда G имеет следующее строение:*

1) *G — разрешимая группа;*

2) *$G = G_{q'} \leftthreetimes G_q$, где $G_{q'} = G^{\mathfrak{F}} \in \mathfrak{F}$, G_q — циклическая подгруппа Картера группы G;*

3) *максимальная подгруппа из G_q нормальна в G.*

Следствие 1. *Пусть $\mathfrak{F}$ — формация всех p-нильпотентных групп. Тогда и только тогда любая собственная подгруппа не p-нильпотентной группы G либо $\mathfrak{F}$-субнормальна, либо $\mathfrak{F}$-абнормальна, когда $G = G_p \leftthreetimes G_q$, где G_q — циклическая подгруппа Картера группы G и максимальная подгруппа из G_q нормальна в G, а $G_p = G^{\mathfrak{F}}$.*

Следствие 2. *Пусть $\mathfrak{F}$ — формация всех p-разложимых групп. Тогда и только тогда любая собственная подгруппа не p-разложимой группы G либо $\mathfrak{F}$-субнормальна, либо $\mathfrak{F}$-абнормальна, когда G — разрешимая группа одного из следующих типов:*

1) $G = G_p \leftthreetimes G_q$, *где G_q — циклическая подгруппа Картера группы G и максимальная подгруппа из G_q нормальна в G, а $G_p = G^{\mathfrak{F}}$.*

2) $G = G_{p'} \leftthreetimes G_p$, *где G_p — циклическая подгруппа Картера группы G и максимальная подгруппа из G_p нормальна в G, а $G_{p'} = G^{\mathfrak{F}}$.*

Литература

1. Fattahi A. *Groups with only normal and abnormal subgroups* // J. Algebra. 1974. Vol. 28. № 1. P. 15–19.

2. Ebert G., Bauman S. *A note on subnormal and abnormal chains* // J. Algebra. 1975. Vol. 36. № 2. P. 287–293.

3. Förster P. *Finite groups all of whose subgroups are $\mathfrak{F}$-subnormal or $\mathfrak{F}$-subabnormal* // J. Algebra. 1986. № 1. P. 285–293.

4. Семенчук В. Н. *Строение конечных групп с $\mathfrak{F}$-абнормальными или $\mathfrak{F}$-субнормальными подгруппами* // Вопросы алгебры. Минск: Изд-во "Университетское". 1986. № 2. С. 50–55.

5. Семенчук В. Н., Шевчук С. Н. *Конечные группы, у которых примарные подгруппы либо $\mathfrak{F}$-субнормальны, либо $\mathfrak{F}$-абнормальны* // Известия вузов. Математика. 2011. № 8. С. 46–55.

6. Semenchuk V. N., Skiba A. N. *On one generalization of finite $\mathfrak{U}$-critical groups* // ArXiv. org e-Print archive, arXiv:1412.5469v1, 17 Dec 2014.

КОНЕЧНЫЕ ГРУППЫ С НИЛЬПОТЕНТНЫМИ НОРМАЛЬНЫМИ ПОДГРУППАМИ

И.Л. Сохор

Гомельский государственный университет имени Ф. Скорины
Советская, 104, 246019 Гомель, Беларусь Irina.Sokhor@gmail.com

Рассматриваются только конечные группы. Используемая терминология соответствует [1]. Через $\mathfrak{N}$ обозначается формация всех нильпотентных групп. Формация называется наследственной, если она замкнута относительно подгрупп. Формация называется радикальной, если она является классом Фиттинга. $G^{\mathfrak{N}}$ — $\mathfrak{N}$-корадикал группы G — пересечение всех нормальных подгрупп группы G, фактор-группа по которым нильпотентна; $[A]B$ — полупрямое произведение нормальной подгруппы A и подгруппы B.

Пусть $\mathfrak{F}$ — некоторый класс групп. Группа G называется минимальной не $\mathfrak{F}$-группой, если G не принадлежит $\mathfrak{F}$, а каждая собственная подгруппа из G принадлежит $\mathfrak{F}$. Минимальные не $\mathfrak{N}$-группы называют группами Шмидта и их свойства хорошо известны [2].

Естественно возникает задача изучения свойств группы, в которой классу $\mathfrak{F}$ принадлежат лишь некоторые собственные подгруппы, например, нормальные.

Доказана следующая теорема.

Теорема. *Пусть $\mathfrak{F}$ — некоторая наследственная радикальная формация. Если в разрешимой группе G, не принадлежащей $\mathfrak{F}$, каждая собственная нормальная подгруппа принадлежит $\mathfrak{F}$, то справедливы следующие утверждения:*

1) $G_p^G = G$, *где $p = |G : M|$, M — нормальная максимальная подгруппа G;*

2) $G/G^{\mathfrak{N}}$ — *циклическая p-группа;*

3) $G = G^{\mathfrak{N}} < x >$, *где $x \in G_p$;*

4) $G^{\mathfrak{N}} < x^p > \in \mathfrak{F}$;

5) $G^{\mathfrak{N}} = G'$.

Обратно, если разрешимая группа G удовлетворяет условиям 4)–5), то каждая собственная нормальная подгруппа группы G принадлежит $\mathfrak{F}$.

При доказательстве используется следующая лемма, представляющая самостоятельный интерес.

Лемма. *Пусть $\mathfrak{F}$ — некоторая наследственная формация. Если в разрешимой группе G каждая собственная подгруппа, содержащая коммутант G', принадлежит $\mathfrak{F}$, то каждая собственная нормальная подгруппа группы G принадлежит $\mathfrak{F}$.*

При $\mathfrak{F} = \mathfrak{N}$ получаем обобщение групп Шмидта.

Следствие. *Пусть M — нормальная максимальная подгруппа разрешимой ненильпотентной группы G и $|G : M| = p$. Каждая собственная нормальная подгруппа группы G нильпотентна тогда и только тогда, когда $G = [G^{\mathfrak{N}}] < x >$, где $< x >$ — силовская p-подгруппа группы G и $[G^{\mathfrak{N}}] < x^p >$ нильпотентна.*

Литература

1. Huppert, B. *Endliche Gruppen I.* Berlin-Heidelberg-New York: Springer, 1967.

2. Монахов, В. С. *Подгруппы Шмидта, их существование и некоторые приложения* // Труды Украинского математического конгресса–2001. Киев: Институт математики НАН Украины, 2001. С. 81–90.

АЛГОРИТМЫ ОПРЕДЕЛЕНИЯ ЭЛЕМЕНТОВ ИНКАПСУЛИРОВАННЫХ КОЛЕЦ ВЫЧЕТОВ

А.В. Трепачева

Южный федеральный университет
Большая Садовая 105/42, 344006 Ростов-на-Дону, Россия
alina1989malina@ya.ru

Инкапсулированные (black-box) представления алгебраических структур помогают оценить сложность алгоритмов, которые строятся безотносительно конкретного представления элемента [1, 2, 3].

Практическая ценность инкапсулированных колец состоит в том, что они дают оценки на сложность криптоанализа полностью гомоморфных криптосистем в атаке на основе шифртекстов [4, 5].

Определение 1. *Инкапсулированное кольцо вычетов – это шестерка (n, k, h, F, G, T) в которой $n \in \mathbb{N}$ – определяет количество элементов в кольце, $k \in \mathbb{N}$ – определяет длину битового представления кодировки. Функции h, F, G, T определены следующим образом.*

1. *Функция $h : \{0,1\}^k \to \mathbb{Z}_n$ сопоставляет элемент из кольца каждой k-битной двоичной строке. Функция h сюръективна, т. е. каждый элемент кольца представлен по меньшей мере одной битовой строкой.*

2. *Функции $F, G : \{0,1\}^k \times \{0,1\}^k \to \{0,1\}^k$ выполняют сложение и умножение. Они удовлетворяют следующим соотношениям $h(F(x,y)) = h(x) + h(y)$ и $h(G(x,y)) = h(x)h(y)$.*

3. *Функция $T : \{0,1\}^k \times \{0,1\}^k \to \{\texttt{true}, \texttt{false}\}$ проверяет равенство двух инкапсулированных элементов: $T(x,y) = \texttt{true}$ тогда и только тогда, когда $h(x) = h(y)$.*

Определение 2. *Пусть(n, k, h, F, G, T) – инкапсулированное кольцо вычетов. Обозначим отображение, сопоставляющее элементу x некоторое представление $[x]$ как $[]$. **Проблема инкапсулированного кольца вычетов** состоит в следующем: найти алгоритм $\mathcal{A}$ который по данному n и оракулам $F, G, T, []$ и представлению $\alpha \in \mathbb{Z}_n$ находит α в явном виде.*

Искомый алгоритм $\mathcal{A}$ может быть представлен в виде последовательности ответов на вопросы вида « $f([x]) = 1?$ » , где $f([x])$ – полином, эффективно вычислимый в инкапсулированном кольце (n, k, h, F, G, T).

Определение 3. *Функцию (полином) $f([x])$ будем называть эффективно вычислимой в инкапсулированном кольце вычетов (n, k, h, F, G, T), если её можно вычислить, пользуясь оракулами F, G и T лишь $O(\log n)$ раз.*

Определение 4. *Полином $f([x])$ будем называть разреженным в инкапсулированном кольце вычетов (n, k, h, F, G, T), если количество его ненулевых коэффициентов равно $O(\log n)$.*

Разреженный полином в кольце (n, k, h, F, G, T) всегда является эффективно вычислимой функцией.

Лемма 1. *Если $f([x])$ – эффективно вычислимая функция, то $f([x])^d$ – также эффективно вычислимая функция.*

Возводить полином в степень, большую чем n не имеет смысла, поэтому достаточно возвести его в степень $d' = d \bmod n$. Для этого можно воспользоваться алгоритмом быстрого возведения в степень: сначала получить двоичное представление числа $d' = d'_{\log_2 n}...d'_1 d'_0$, далее последовательным возведением в квадрат получаем $f([x])^2, f([x])^4, f([x])^8, f([x])^{16}, \ldots,$ $f([x])^{2^{\lceil \log_2 n \rceil}}$. Результат получается перемножением тех степеней, при которых в двоичном разложении d' стояла единица, т.е.

Теорема. *В случае кольца вычетов по простому модулю существует такая последовательность эффективно вычислимых функций $f_i([x])$, $0 \le i \le O(\log_2 n)$ (которую будем называть классифицирующей), что последовательными ответами на вопросы вида $f_i([x]) = 1?$ элемент инкапсулированного кольца определяется по своему представлению однозначно.*

Идея доказательства состоит в том, что $x^{\frac{n-1}{2}} \bmod n$ в случае, если n – простое число является символом Лежандра и в половине случаев равен 1, что позволяет удачно классифицировать элемент x.

Свойства разреженных полиномов похожи на свойства случайных перестановок в $\mathbb{Z}_n$ и можно показать что при количестве этих полиномов с подавляющей вероятностью найдется такой, который принимает значение 1 на приблизительно половине элементов произвольно выбранного множества.

Таким образом, получается, что на каждом шаге с помощью некоторого разреженного полинома возможно с подавляющей вероятностью «сузить» область поиска примерно вдвое, что можно представить в виде бинарного дерева поиска в листьях которого находятся элементы инкапсулированного кольца вычетов и это дерево будет сбалансировано.

Работа выполнена при финансовой поддержке гранта РФФИ №15-07-00597 А.

Литература

1. Arvind V., Das B., Mukhopadhyay P. *The complexity of black-box ring problems* // Computing and Combinatorics, Springer, 2006. P. 126–135.

2. Boneh D., Lipton R. J. *Algorithms for black-box fields and their application to cryptography* // Advances in Cryptology—CRYPTO'96, Springer, 1996. P. 283–297.

3. Zumbragel J., Maze G., Rosenthal J. *Efficient recovering of operation tables of black box groups and rings* // IEEE International Symposium on Information Theory, 2008 (ISIT 2008). IEEE, 2008. P. 639–643.

4. Maurer U. *Abstract models of computation in cryptography* // Cryptography and Coding. Springer Berlin Heidelberg, 2005. P. 1-12.

5. Jager T. *Black-Box Models of Computation in Cryptology*. Springer Science & Business Media, 2012.

О КОНЕЧНЫХ РАЗРЕШИМЫХ ГРУППАХ С МАЛЫМ НОРМАЛЬНЫМ РАНГОМ СИЛОВСКИХ ПОДГРУПП НЕКОТОРЫХ ФАКТОРОВ

А.А. Трофимук

Брестский государственный университет имени А.С. Пушкина,
бульвар Космонавтов 21, 224016 Брест, Беларусь
alexander.trofimuk@gmail.com

Рассматриваются только конечные группы. Все обозначения и используемые определения соответствуют [1]. Напомним, что бициклической называют группу, которая является произведением двух циклических подгрупп.

В. С. Монахов [2] ввел понятие нормального ранга p-группы P следующим образом:

$$r_n(P) = \max_{X \lhd P} \log_p |X/\Phi(X)|.$$

Здесь $\Phi(X)$ – подгруппа Фраттини группы X, а запись $X \lhd P$ означает, что X — нормальная подгруппа группы P.

Очевидно, что p-группа P имеет нормальный ранг 1 тогда и только тогда, когда P циклическая. Из теоремы III.11.5 [3] следует, что нормальный ранг примарной бициклической группы нечетного порядка не превышает 2. Обратное неверно. Так, $r_n(S) = 2$ для экстраспециальной группы S порядка 27, но S не является бициклической. Кроме того, из [3, теоремы III.7.6, III.12.4, III.12.5] следует, что всякая 2-группа нормального ранга ≤ 2 является бициклической. Однако, существуют бициклические 2-группы, которые имеют нормальный ранг 3. В статье Хупперта [4] построена бициклическая группа порядка 2^5

$$G = \langle a, b, c \mid a^2 = b^8 = c^2 = 1,\ [a, b] = c,\ [b, c] = b^4, [a, c] = 1\rangle,$$

у которой $r_n(G) = 3$.

В работе [5] получены оценки инвариантов (производной длины, нильпотентной длины и p-длины) разрешимой группы, обладающей нормальным рядом, силовские подгруппы в факторах которого являются бициклическими.

Рассмотрим для группы G цепочку подгрупп

$$\Phi(G) = G_0 \subset G_1 \subset \ldots \subset G_{m-1} \subset G_m = F(G), \quad G_i \lhd G. \tag{1}$$

Здесь $F(G)$ — подгруппа Фиттинга группы G.

Развитием результатов работы [5] стала работа [6], в которой исследовались разрешимые группы, у которых силовские подгруппы в факторах цепочки (1) бициклические.

Продолжением результатов, рассмотренных выше, является следующая

Теорема. *Пусть в разрешимой группе G существует цепочка подгрупп* (1) *такая, что $r_n(P) \leq 2$ для каждой силовской подгруппы P из факторов G_i/G_{i-1}, $i = 1, 2, \ldots, m$. Тогда нильпотентная длина группы G не превышает 4, а производная длина фактор-группы $G/\Phi(G)$ не превышает 5.*

Работа выполнена при финансовой поддержке БРФФИ (грант № Ф15РМ-025).

Литература

1. Монахов В. С. *Введение в теорию конечных групп и их классов.* Минск: Вышэйшая школа, 2006.

2. Монахов В. С. *О разрешимых конечных группах с силовскими подгруппами малого ранга* // Доклады Национальной академии наук Беларуси. 2002. Т. 46. № 2. С. 25–28.

3. Huppert B. *Endliche Gruppen I.* Springer: Berlin, Heidelberg, New York, 1967.

4. Huppert B. *Über das Produkt von paarweise vertauschbaren zyklischen Gruppen* // Math. Z. 1953. Vol. 58. P. 243–264.

5. Monakhov V. S., Trofimuk A. A. *On a finite group having a normal series whose factors have bicyclic Sylow subgroups* // Communications in algebra. 2011. № 39 (9). P. 3178–3186.

6. Трофимук А. А. *Конечные группы с бициклическими силовскими подгруппами в фиттинговых факторах* // Труды Института математики и механики УрО РАН. 2013. № 3(19). С. 304–307.

О p-СВЕРХРАЗРЕШИМОСТИ КОНЕЧНОЙ ФАКТОРИЗУЕМОЙ ГРУППЫ С НОРМАЛЬНЫМИ СОМНОЖИТЕЛЯМИ

И.К. Чирик

Гомельский инженерный институт МЧС Республики Беларусь
проспект Речицкий 35а, 246023 Гомель, Беларусь chyrykira@mail.com

В конечной группе произведение двух нормальных сверхразрешимых подгрупп в общем случае не является сверхразрешимой подгруппой. Соответствующие примеры хорошо известны [1, стр. 159-160]. Поэтому для получения сверхразрешимости конечной группы $G = AB$ с нормальными сомножителями A и B необходимы дополнительные ограничения.

Бэр [2, стр. 186] установил сверхразрешимость конечной группы $G = AB$ с нормальными сверхразрешимыми подгруппами A и B при условии, что коммутант G' — нильпотентная подгруппа. Условие нильпотентности коммутанта А. Ф. Васильев и Т. И. Васильева [3, следствие 3] заменили требованием существования нильпотентной нормальной подгруппы W такой, что в G/W все силовские подгруппы абелевы. В работе Фризен [4] установлена сверхразрешимость конечной группы $G = AB$ при условии, что A и B — нормальные сверхразрешимые подгруппы взаимно простых индексов.

В этом направлении получены «p-аналоги» данных результатов. Доказана следующая теорема.

Теорема. *Пусть p — простое число, A и B — нормальные p-сверхразрешимые подгруппы конечной группы G и $G = AB$. Если существует p-нильпотентная нормальная подгруппа W такая, что в G/W все силовские подгруппы абелевы, то G p-сверхразрешима.*

Следствие 1. *Пусть p — простое число, A и B — нормальные p-сверхразрешимые подгруппы конечной группы G и $G = AB$. Если коммутант G' p-нильпотентен, то G p-сверхразрешима.*

Следствие 2. *Пусть p — простое число, A и B — нормальные p-сверхразрешимые подгруппы конечной группы G и $G = AB$. Если $(|G : A|, |G : B|) = 1$, то G p-сверхразрешима.*

Следствие 3. *Пусть p — простое число, A и B — нормальные p-сверхразрешимые подгруппы конечной группы G и $G = AB$. Если в $A \cap B$ силовская p-подгруппа циклическая, то G p-сверхразрешима.*

Следствие 4. *Пусть p — простое число, A и B — нормальные сверхразрешимые подгруппы конечной группы G и $G = AB$. Если A холлова, то G сверхразрешима.*

Из теоремы следуют также отмеченные выше результаты работ [2–4].

Литература

1. Монахов В. С. *Введение в теорию конечных групп и их классов.* Минск: Вышэйшая школа. 2006.

2. Baer R. *Classes of finite groups and their properties* // Illinois J. Math. 1957. Vol. 1. P. 115–187.

3. Васильев А. Ф., Васильева Т. И. *О конечных группах, у которых главные факторы являются простыми группами* // Известия высших учебных заведений. Математика. 1997. № 11 (426). С. 10–14.

4. Friesen D. *Products of normal supersolvable subgroups* // Proceedings of the American Mathematical Society. 1971. Vol. 30, № 1. P. 46–48.

5. Bray H. G., Deskins W. E., Johnson D., Humphreys J. F., Puttaswamaian B. M., Venzke P., Walls G. L., Weinstein M. *Between nilpotent and solvable.* Passaic: Polygonal Publ. House, 1982.

О МНОГООБРАЗИЯХ ПРЕДСТАВЛЕНИЙ СВОБОДНЫХ АБЕЛЕВЫХ ГРУПП

А.А. Шаромет

Белгосуниверситет, механико-математический факультет
Независимости 4, 220050 Минск, Беларусь sharomet@mail.ru

Для многообразия $\mathcal{M} \subseteq M_n = M_n(P)$ определим многообразие перестановочных матриц

$$C(m, \mathcal{M}) = \{(a_1, \ldots, a_m) \in \mathcal{M} | a_i a_j = a_j a_i, i, j = \overline{1, m}\},$$

которое можно интерпретировать как многообразие представлений свободной абелевой группы ранга m [1,2]. Обычно $\mathcal{M}$ — это M_n или линейная алгебраическая группа.

В качестве основной задачи рассматривается доказательство неприводимости многообразия $C(m, \mathcal{M})$ или описание его неприводимых компонент. Большое количество работ посвящено изучению многообразий $C(m, \mathrm{M}_n)$. Чтобы воспользоваться этими результатами для многообразий $C(m, \mathrm{GL}_n)$ и $C(m, \mathrm{SL}_n)$, рассмотрим взаимосязи между неприводимостью коммутаторных многообразий $C(m, n)$, $C(m, \mathrm{GL}_n)$ и $C(m, \mathrm{SL}_n)$

Нетрудно убедиться, что $C(m, \mathrm{GL}_n)$ является открытым плотным множеством в $C(m, \mathrm{M}_n)$ и, значит они неприводимы одновременно.

Что касается многообразий $C(m, \mathrm{GL}_n)$ и $C(m, \mathrm{SL}_n)$, то их одновременная неприводимость следует из следующего более общего результата.

Теорема 1. *Пусть $G = TH$ – почти прямое произведение одномерного тора T и (связной) редуктивной группы H. Тогда многообразие $C(m, H)$ неприводимо тогда и только тогда, когда неприводимо многообразие $C(m, G)$.*

Отметим последние результаты о неприводимости многообразий $C(m, \mathrm{M}_n)$, не претендуя на полноту обзора. Первый результат, состоящий в доказательстве неприводимости многообразия $C(2, M_n)$, содержится в известной работе [3]. Хорошо известно, что при $m, n \geq 4$ многообразие $C(m, n)$ приводимо, а при $n = 3$ неприводимо при любом m. Значительное количество работ касается неприводимости $C(3, n)$; так, в работе [4] доказано, что $C(3, n)$ приводимо для $n \geq 32$. Авторы [5] заметили, что из рассуждений Гуральника в [4] легко следует, что $C(3, n)$ приводимо для $n \geq 29$. Наконец, в работе [6] доказано, что $C(3, n)$ неприводимо при $n \leq 10$ в предположении, что характеристика поля нулевая. Вопрос о неприводимости $C(3, n)$ при $10 < n < 29$ пока остается открытым.

Эти результаты, как показано выше, влекут за собой соответствующие следствия для односвязной группы SL_n, которые мы соберем в следующее предложение. Поскольку в большинстве указанных работ характеристика основного поля предполагается нулевой, то и мы сохраним это ограничение.

Предложение. *Многообразие $C(m, \mathrm{SL}_n)$ над полем нулевой характеристики неприводимо в случаях $1 - 3$ и приводимо в случаях $4, 5$.*

1. *$m = 2$, а n – любое;*
2. *$n = 3$, а m – любое;*
3. *$m = 3, n \leq 10$;*

4. $m \geq 4, n \geq 4$*;*

5. $m = 3, n \geq 29$*.*

Все сказанное выше можно считать развернутой мотивировкой задачи описания зависимости неприводимости многообразия $C(m, G)$ от параметра m и ранга группы G для односвязной группы.

В работе [7] доказано, что для неодносвязной группы G многообразие $C(m, G)$ не является неприводимым для $m \geq 2$, что вместе с теоремой Ричардсона [8] показывает, что над полем комплексных чисел односвязность группы G является необходимым и достаточным условием неприводимости многообразия $C(2, G)$. Для неодносвязной группы G остается найти неприводимые компоненты для $C(m, G)$. Если ограничиться случаем $m = 2$, то естественными кандидатами на роль неприводимых компонент в $C(2, G)$ являются $p(W(\tilde{G}, \gamma))$, где $\pi : \tilde{G} \to G$ — универсальное накрытие, $p : \tilde{G} \times \tilde{G} \to G \times G$ — его квадрат, а γ — элемент фундаментальной группы.

Таким образом, для неприводимости множеств $\theta^{-1}(\gamma)$ достаточно убедиться в неприводимости подмножества $p(W(\tilde{G}, \gamma))$, в частности, достаточно доказать неприводимость $W(\tilde{G}, \gamma)$. Единственный известный нам результат, касающийся неприводимости многообразия $W(\tilde{G}, \gamma)$ для односвязной группы, содержится в [5], и состоит в том, что многообразие

$$W(\mathrm{SL}_n, \varepsilon) = \{(a, b) \in \mathrm{SL}_n^2 | [a, b] = \varepsilon E\}$$

неприводимо, если ε – примитивный корень из единицы степени n. Отметим, что это решает задачу описания неприводимых компонент в многообразиях $C(2, G)$ для групп типа A_n, если $n + 1$ – простое число.

Опишем неприводимые компоненты многообразия $C(2, G)$ для групп типа A_n в общем случае. Через $\mathcal{C}_d$ будем обозначать группу всех корней из 1 степени d. Основным результатом является следующая теорема.

Теорема 2. *Пусть G алгебраическая группа типа A_n, а $\pi : \mathrm{SL}_{n+1} \to G$ – универсальное накрытие, а $F = \{\zeta E | \zeta \in \mathcal{C}_d\}$ – фундаментальная группа. Тогда неприводимыми компонентами для $C(2, G)$ являются множества $p(W(\mathrm{SL}_n, \zeta))$, где $\zeta \in \mathcal{C}_d$.*

Литература

1. Lubotzky A., Magid A. *Varieties of representations of finitely generated groups* // Memoirs of the American Mathematical Society. 1985. V. 58. P. 1–116.

2. Платонов В. П., Рапинчук А. С. *Алгебраические группы и теория чисел.* М.: Наука, 1991.

3. Motskin T., Taussky O. *Pairs of matrices with property L. II* // Trans. Amer. Math. Soc. 1955. V. 80. P. 387–401.

4. Guralnick R. *A note on commuting pairs of matrices*// Linear and Multilinear Algebra. 1992. V. 31. P. 71–75.

5. Rapinchuk A. S., Benyash-Krivetz V. V., Chernousov V. I. *Representation varietes of the fundamental grjups of cjmpact orientable surfases* // Izrael J.of Math. 1996. V. 93, P. 29–71.

6. Šivic K. *On varieties of commuting triples* // Linear Algebra and its Applications. 2012. V. 437. P. 393–460.

7. Шаромет А. А. *О многообразии пар перестановочных матриц неодносвязной алгебраической группы* // XI Белорусская математическая конференция: Тезисы докладов. Минск: Институт математики НАН Беларуси, 2012. Ч.5. С. 57–58.

8. Richardson R. W. *Commuting varieties of semisimple Lie algebras and algebraic groups* // Compositio Math. 1979. V. 38, No. 3. P. 311–327.

КОНЕЧНЫЕ П-РАЗРЕШИМЫЕ НЕПРИВОДИМЫЕ КОМПЛЕКСНЫЕ ЛИНЕЙНЫЕ ГРУППЫ С П-ХОЛЛОВОЙ TI-ПОДГРУППОЙ

А.А. Ядченко

Институт математики НАН Беларуси, Кирова 32^a, 246050 Гомель, Беларусь
yadchenko_56@mail.ru

Пусть π — некоторое множество простых чисел, G — конечная π-разрешимая группа, которая имеет точный комплексный характер χ степени n и содержит π-холлову TI-подгруппу H. Если $\pi = \{p\}$, p — простое число, то Окуяма [1] показал, что H нормальна в G, когда $n < |H|/\varepsilon - 1$, где $\varepsilon = 1$ при $p > 2$ и $\varepsilon = 2$ при $p = 2$. Ядченко [2] рассмотрел случай, когда π — произвольное множество простых чисел и $n \leq |H|/\varepsilon - 1$, где $\varepsilon = 1$, когда силовская 2-подгруппа группы H не является обобщенной группой кватернионов, и $\varepsilon = 2$ в противном случае. Оказалось, что либо подгруппа H нормальна в G, либо $n = |H|/\varepsilon - 1 = q^\alpha = f$. Здесь q — простое π'-число, α — некоторое натуральное число. Если же π — множество простых нечетных чисел, группа G разрешима и характер χ неприводим, то в [3] утверждается. что либо $H \lhd G$, либо n делится на $|H|$ или на такую степень $f > 1$ некоторого простого числа, что $f \equiv -1$ или $1(\mathrm{mod}|H|)$. Там же установлено, что, когда $n < 2|H|$ и $H \not\lhd G$, то $n = |H| - 1$, $|H|$, $|H| + 1$, $2(|H| - 1)$ или $2|H| - 1$ и n — степень простого числа за исключением, может быть, случая, когда $n = |H|$.

В серии статей [4-6] доказывается, что приведенное выше утвекржение справедливо и для π-разрешимых групп. В последней статье этой серии поставлена

Задача. Справедливо ли следующее утверждение?

Пусть G — π-разрешимая неприводимая линейная группа степени n и H – ее π-холлова TI-подгруппа нечетного порядка. Если n не делится на $|H|$ и n не делится на такую степень $f > 1$ некоторого простого числа, что $f \equiv \pm 1(mod|H|)$, то $H \lhd G$.

Для разрешимых групп это утверждение верно [3]. Доказанная в [4-6] теорема дает положительный ответ на поставленный вопрос без применения теоремы о классификации простых групп, если $n < 2|H|$. В [7] в некоторых частных случаях утверждение доказано для произвольного n, также без применения теоремы о классификации простых групп.

При $|H| = p$ эта задача совпадает с поставленной в [8] задачей Айзекса о переносе теоремы о разрешимых неприводимых линейных группах на p-разрешимые группы.

В [9] поставленная задача решается положительно без применения теоремы о классификации конечных простых групп, если 2-подгруппа Силова в G абелева.

В [10] она решается положительно с применением теоремы о классификации конечных простых групп.

При доказательстве этих результатов основным является случай, когда $G = HO_{\pi'}(G)$. В этом случае условие, что H — TI-подгруппа в G, равносильно тому, что $C_{O_{\pi'}(G)}(H) = C_{O_{\pi'}(G)}(h)$ для каждого неединичного элемента $h \in H$ [10]. Полезными при доказательстве некоторых из приведенных результатов оказались следующие утверждения.

Лемма 1 ([8]). *Если $\Gamma = AB$ — группа, где $B \lhd \Gamma$ и $(|A|, |B|) = 1$, то $B = [B, A]C_B(A)$.*

Лемма 1 в литературе встречается только для случая, когда группа B примарна.

Лемма 2 ([10], стр. 152-153). *Пусть $\Gamma = AB$ — группа, где $B \lhd \Gamma$, $(|A|, |B|) = 1$ и $C_B(a) = C_B(A)$ для каждого элемента $a \in A^\#$. Предположим, что для некоторой A-инвариантной подгруппы $B_1 \subseteq B$ число $|B : B_1|$ не делится на такую степень $f > 1$ простого числа, что $f \equiv 1(mod\ |A|)$. Тогда $B = B_1C_B(A)$.*

Условие В. Скажем, что для Γ, A, G, C, χ и n выполнено условие В, если $\Gamma = AG$, где G – нормальная в Γ подгруппа, $(|A|, |G|) = 1$, A – группа нечетного порядка, большего 3, которая не является нормальной в группе Γ, $C_G(a) = C_G(A) = C$ для каждого элемента

$a \in A^{\#}$, и G имеет точный неприводимый комплексный характер χ степени n, который является a-инвариантным хотя бы для одного элемента $a \in A^{\#}$.

Теорема 1. *Пусть для* Γ, A, G, C, χ *и* n *выполнено условие* B. *Тогда справедливо каждое из следующих утверждений:*

(1) если $n = |A| + 1$, *то* $G = O_2(G)C$ *и подгруппа* C *абелева;*

(2) если $n = 2|A|-1$, *то* $G = O_q(G)C$, q *– нечетное простое число,* C *разрешима и* $|A|-1$ *делит* $|C|$, *если* C *не абелева;*

(3) если $n = 2(|A|-1)$, *то* $G = O_2(G)C$ *и либо* C *не абелева, но разрешима, либо* $C/Z(\Gamma) \cong PSL(2,5)$ *и* Γ *имеет единственный не циклический композиционный фактор.*

Теорема 2. *Пусть для* Γ, A, G, C, χ *и* n *выполнено условие* B *и* $n < 2|A|$. *Тогда справедливо каждое из следующих утверждений:*

(1) n *является степенью простого числа* q;

(2) $G = O_q(G)C$, *где* q *из (1);*

(3) если группа G *не разрешима, то* $n = 2(|A| - 1)$, $C/Z(\Gamma) \cong PSL(2,5)$ *и* Γ *имеет единственный не циклический композиционный фактор.*

Теорема 3. *Пусть* G *–* π *-разрешимая неприводимая линейная группа степени* $n < 2|H|$ *с* π*-холловой* TI*-подгруппой* H *нечетного порядка, большего 3, и* $H \not\lhd G$. *Тогда справедливо каждое из следующих утверждений:*

(1) $n = |H| - 1, |H|, |H| + 1, 2(|H| - 1)$ *или* $2|H| - 1$ *и* n *– степень простого числа* q, *за исключением случая, когда* $n = |H|$;

(2) факторгруппа $G/O_{\pi',\pi}(G)$ *абелева;*

(3) если $n = |H|$, *то* $G = [O_{\pi'}(G), H]N_G(H)$ *с абелевой подгруппой* $[O_{\pi'}(G), H]$ *и* $[O_{\pi'}(G), H] \cap N_G(H) = 1$, *если же* $n \neq |H|$, *то* $G = O_q(G)N_G(H)$, *где* q *из (1);*

(4) если группа G *не разрешима, то* $n = 2(|H| - 1)$, $(C_G(H))_{\pi'}/Z(G) \cong PSL(2,5)$ *и* G *имеет единственный не циклический композиционный фактор.*

Для случая, когда $|\pi| > 1$, доказательство этих теорем приводится в [11] и [12].

Литература

1. Okuyama T. *On finite groups whose Sylow p-subgroup is a T.I. set* // Hokkaido Math. J. 1975. V. 4. № 2. P. 303-305.

2. Ядченко А. А. *О конечных* π*-разрешимых линейных группах* // Арифметическое и подгрупповое строение конечных групп. Минск: Наука и техника. 1986. С. 181-207.

3. Ядченко А. А. *Разрешимые неприводимые линейные группы произвольной степени с холловской TI-подгруппой* // Матем. заметки. 1990. Т. 48. В. 2. С. 137-144.

4. Ядченко А. А. *О* π*-разрешимых неприводимых линейных группах с холловой* $TI-$*подгруппой нечетного порядка . I* // Труды Института математики НАН Беларуси. 2008. Т. 16. № 2. С. 118-130.

5. Ядченко А. А. *О* π*-разрешимых неприводимых линейных группах с холловой* $TI-$*подгруппой нечетного порядка . II* // Труды Института математики НАН Беларуси. 2009. Т. 17. № 2. С. 94-104.

6. Ядченко А. А. *О* π*-разрешимых неприводимых линейных группах с холловой* $TI-$*подгруппой нечетного порядка . III* // Труды Института математики НАН Беларуси. 2010. Т. 18. № 2. С. 99-114.

7. Ядченко А.А. *Об автоморфизмах и нормальных холловских подгруппах линейных групп* // Весці НАН Беларусі. Серыя фіз.-мат. навук. 2007. № 3. С. 49-54.

8. Isaacs I. M. *Characters of solvable groups*, in: The Santa Cruz Conference on Finite Groups. Proc. Symp. Pure Math. 1980. V. 37. P. 377-384.

9. Ядченко А.А. *Об автоморфизмах неприводимых линейных групп с абелевой силовской 2-подгруппой* // Матем. заметки (принята в печать).

10. Ядченко А.А. *К проблеме Айзекса* // Матем. сборник. 2013. Т. 204. № 12. С. 147-156.

11. Ядченко А.А. *О факторизации* π*-разрешимых неприводимых линейных групп* // Доклады НАН Беларуси. 2014. Т. 58. № 5. С. 5-11.

12. Yadchenko A.A. *On solvability of certain irreducible linear groups* // Asian Journal of Mathematics and Computer Research. 2015. V. 5. No. 1. P. 20-37.

INTERSECTION OF CONJUGATED SOLVABLE SUBGROUPS IN A SYMMETRIC GROUP

Anton Baykalov

Sobolev Institute of Mathematics, Siberian Branch of the Russian Academy of Sciences
4 Acad. Koptyug avenue, 630090, Novosibirsk, Russia
Novosibirsk State University
2 Pirogova Str., 630090, Novosibirsk, Russia
anton188@bk.ru

Assume that a finite group G acts on a set Ω. An element $x \in \Omega$ is called a *G-regular point* if $|xG| = |G|$, i.e. if the stabilizer of x is trivial. Define the action of the group G on Ω^k by the rule

$$g : (i_1, \ldots, i_k) \mapsto (i_1 g, \ldots, i_k g).$$

If G acts faithfully and transitively on Ω, then the minimal number k such that the set Ω^k contains a G-regular point is called the *base size* of G and is denoted by $b(G)$. For a positive integer m the number of G-regular orbits on Ω^m is denoted by $Reg(G, m)$ (this number equals 0 if $m < b(G)$). If H is a subgroup of G and G acts by the right multiplication on the set Ω of right cosets of H then G/H_G acts faithfully and transitively on the set Ω. (Here $H_G = \cap_{g \in G} H^g$.) In this case, we denote $b(G/H_G)$ and $Reg(G/H_G, m)$ by $b_H(G)$ and $Reg_H(G, m)$ respectively.

Thus $b_H(G)$ is the minimal number k such that there exist elements $x_1, \ldots, x_k \in G$ for which $H^{x_1} \cap \ldots \cap H^{x_k} = H_G$.

Consider the problem 17.41 from "Kourovka notebook" [1]:

Let H be a solvable subgroup of finite group G and G does not contain nontrivial normal solvable subgroups. Are there always exist five subgroups conjugated with H such that their intersection is trivial?

The problem is reduced to the case then G is almost simple in [2]. Specifically, it is proved that if for each almost simple group G and solvable subgroup H of G condition $Reg_H(G, 5) \geq 5$ holds then for each finite nonsolvable group G and solvable subgroup H of G condition $Reg_H(G, 5) \geq 5$ holds.

We have proved the following theorem

Theorem 1. *Let H be a solvable subgroup of an almost simple group G whose socle is isomorphic to A_n, $n \geq 5$. Then $Reg_H(G, 5) \geq 5$. In particular $b_H(G) \leq 5$.*

References

1. *Kourovka notebook*. Edition 18. Novosibirsk, 2014.

2. Vdovin E.P. *On the base size of a transitive group with solvable point stabilizer* // Journal of Algebra and Application. 2012. Vol. 11. No. 1. 1250015 (14 pages).

THE JORDAN BLOCK STRUCTURE OF IMAGES OF REGULAR UNIPOTENT ELEMENTS FROM SUBSYSTEM SUBGROUPS OF TYPE C_2 IN IRREDUCIBLE REPRESENTATIONS OF GROUPS OF TYPE C_n WITH LOCALLY SMALL HIGHEST WEIGHTS

T.S. Busel[1], I.D. Suprunenko[2]

Institute of Mathematics, National Academy of Belarus, 11 Surganov str., 220072, Minsk, Belarus
[1]tbusel@gmail.com, [2]suprunenko@im.bas-net.by

The Jordan block structure of images of regular unipotent elements from subsystem subgroups of type C_2 in irreducible representations of groups of type C_n in characteristic $p \geq 11$ with locally small highest weights is determined.

In what follows K is an algebraically closed field of characteristic $p \geq 11$, $G = C_n(K)$, $n > 2$, $\omega(\varphi)$ is the highest weight of an irreducible representation φ, $J_\varphi(x)$ is the set of Jordan block sizes of element $\varphi(x)$ (without multiplicities), $\mathbf{N}_a$ is the set of integers i with $1 \leq i \leq a$, ω_i, $1 \leq i \leq n$, are the fundamental weights of G.

Theorem 1. *Let $p \geq 11$, $G = G_n(K)$, $n > 2$, φ be a p-restricted irreducible representation of G, $\omega(\varphi) = \omega = a_1\omega_1 + ... + a_n\omega_n$, and $x \in G$ be a regular unipotent element from a subsystem subgroup of type C_2. Assume that $a_{n-1} + 2a_n < p$. Set $S = 3a_1 + 4(a_2 + ... + a_n)$.*

1) Let $S < p$. Then $J_\varphi(x) = \mathbf{N}_{S+1}$ or one of the following holds:
(i) $\omega = \omega_i$, $2 \leq i \leq n$, $J_\varphi(x) = \mathbf{N}_{S+1} \setminus \{2, 3\}$;
(ii) $\omega = a_1\omega_1$, $a_1 > 1$, $J_\varphi(x) = \mathbf{N}_{S+1} \setminus \{2, 3a_1 - 4, 3a_1 - 1, 3a_1\}$;
(iii) $\omega = \omega_1$, $J_\varphi(x) = \{1, 4\}$;
(iv) $\omega = \omega_i + \omega_n$, $2 \leq i \leq n - 1$, $J_\varphi(x) = \mathbf{N}_{S+1} \setminus \{1\}$;
(v) $n = 3$ and ω is a weight from Items a)-d) below:
(a) $\omega = \omega_3$, $J_\varphi(x) = \mathbf{N}_{S+1} \setminus \{1, 2, 3\}$;
(b) $\omega \in \{\omega_2 + \omega_3, 2\omega_1 + \omega_3, \omega_1 + \omega_3, \omega_1 + 2\omega_3, 5\omega_3\}$, $J_\varphi(x) = \mathbf{N}_{S+1} \setminus \{1\}$;
(c) $\omega = 3\omega_3$, $J_\varphi(x) = \mathbf{N}_{S+1} \setminus \{2\}$;
(d) $\omega = 2\omega_3$, $J_\varphi(x) = \mathbf{N}_{S+1} \setminus \{1, 4\}$.

2) Assume that $S \geq p$. Then $J_\varphi(x) = \mathbf{N}_p$ or one of the following holds:
(i) $\omega = \frac{p-4}{3}\omega_1 + \omega_j$, $2 \leq j \leq n$, $J_\varphi(x) = \mathbf{N}_p \setminus \{p - 1\}$;
(ii) $\omega = a_1\omega_1$, $a_1 > \frac{p}{3}$, $J_\varphi(x) = \mathbf{N}_p \setminus \{2, p - 2\}$;
(iii) $\omega = a_{i-1}\omega_{i-1} + a_i\omega_i$, $a_{i-1} + a_i = p - 1$, $i \leq n - 1$, $\mathbf{N}_p \setminus \{2, p - 2\} \subset J_\varphi(x) \subset \mathbf{N}_p$.

Hence $|J_\varphi(x)| \geq p - 2$ when $S \geq p$.

These results can be applied for investigating the behaviour of unipotent elements in modular representations of simple algebraic groups and recognizing representations and linear groups.

The proof of Theorem 1 is based on constructing direct summands with prescribed properties in restrictions of a module under consideration to subsystem subgroups of type C_2 and subgroups of type A_1 containing relevant unipotent elements. In many cases we can construct certain direct summands in such restrictions to subgroups of type A_1 that are tilting modules with highest weights not too large with respect to the characteristic. The results of A.A. Osinovskaya [1] on the block structure of images of regular unipotent elements in irreducible representations of the group $C_2(\mathbb{C})$ and the information of the structure of tilting modules for the group of type A_1 with highest weights less than $2p - 2$ [2] are used essentially.

This research has been supported by the State Research Programme "Convergance"(2011-2015) and by the Belarusian Republican Foundation for Fundamental Research, project F14-043.

References

1. Osinovskaya A.A. Nilpotent elements in irreducible representations of simple Lie algebras of small rank // Preprint, National Academy of Sciences of Belarus. Institute of Mathematics. 1999. V. 554. No 5. P. 31.

2. Seitz G.M. Unipotent elements, tilting modules, and saturation // Invent. math. 2000. V. 141. P. 467-502.

ON THE ISOMORPHISM PROBLEM FOR GENERALIZED BAUMSLAG–SOLITAR GROUPS

F.A. Dudkin

Sobolev Institute of Mathematics, Siberian Branch of the Russian Academy of Sciences
4 Acad. Koptyug avenue, 630090, Novosibirsk, Russia
Novosibirsk State University, Ministry of Education and Science of the Russian Federation
2 Pirogova Str., 630090, Novosibirsk, Russia
DudkinF@ngs.ru

A finitely generated group G is called a *generalized Baumslag-Solitar group* or a GBS group if G can act on a tree so that the stabilizers of vertices and edges are infinite cyclic groups. By the Bass-Serre theorem, G can be represented as $\pi_1(\mathbb{A})$, the fundamental group of a graph of groups $\mathbb{A}$ (see [1]).

For a GBS group G, we can present the corresponding graph of groups $\mathbb{A}$ by a labeled graph (A, λ), where A is a finite connected graph and $\lambda\colon E(A) \to \mathbb{Z} \setminus \{0\}$ labels the edges of A. The label λ_e of an edge e with the source vertex v determines an embedding $\alpha_e\colon e \to v^{\lambda_e}$ of the cyclic edge group $\langle e \rangle$ into the cyclic vertex group $\langle v \rangle$. Using the notion of expansion for labeled graphs, we can easily see that every GBS group can be presented by infinitely many labeled graphs.

Recently GBS groups have been quite actively studied [2–4]. In particular, the isomorphism problem for GBS groups has been discussed: to find out algorithmically when two given labeled graphs determine isomorphic GBS groups. This problem is solved only in several special cases [5–7], the general solution is not found.

If two labeled graphs $\mathbb{A}$ and $\mathbb{B}$ determine isomorphic GBS groups $\pi_1(\mathbb{A}) \cong \pi_1(\mathbb{B})$ and $\pi_1(\mathbb{A})$ is not isomorphic to $\mathbb{Z}, \mathbb{Z}^2$ or the Klein bottle group, then there exists a finite sequence of *expansion* and *collapse* (see fig.1) moves connecting $\mathbb{A}$ and $\mathbb{B}$ [8]. A labeled graph is called *reduced* if it admits no collapse move (equivalently, the labeled graph contains no edges with distinct endpoints and labels ± 1).

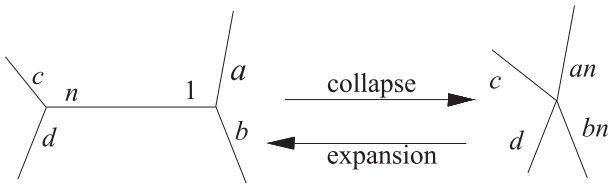


Fig. 1: Expansion and collapse moves.

For labeled graph $\mathbb{A}$ (a GBS group G), denote the set of reduced labeled graphs with the fundamental group isomorphic to $\pi_1(\mathbb{A})$ (resp. G) by $R(\mathbb{A})$ (resp. $R(G)$).

Three types of transformations of labeled graphs play an important role in studying GBS groups: slides (see fig. 2), inductions, and $\mathscr{A}^{\pm}$–moves.

Theorem (Clay M., Forester M. [2]). *Let G be a GBS group and $\mathbb{A}, \mathbb{B} \in R(G)$. Then $\mathbb{A}$ and $\mathbb{B}$ are connected by a finite sequence of slides, inductions and $\mathscr{A}^{\pm 1}$–moves with all intermediate labeled graphs reduced.*

An edge e of a labeled graph $\mathbb{A}$ is called *mobile* (see [6]) if there exists $t \in \pi_1(\mathbb{A})$ such that $G_e^t \subset G_e$. Here G_e is an edge cyclic group, corresponding to the edge e. In [6] it is proved that there is an algorithm to find out whether a given edge e mobile or not.

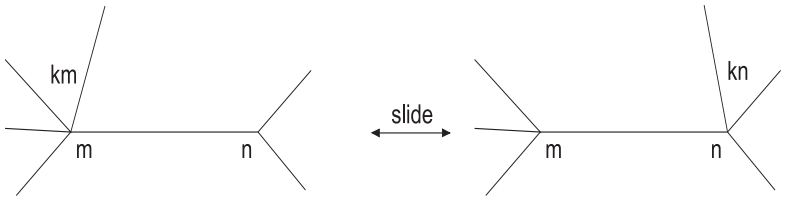


Fig. 2: A slide.

The main result of this talk is another piece of the isomorphism problem for GBS groups:

Theorem. *Let $\mathbb{A}$ and $\mathbb{B}$ be labeled graphs. Suppose that $\mathbb{A}$ has at most one mobile edge. Then there is an algorithm to find out whether the groups $\pi_1(\mathbb{A})$ and $\pi_1(\mathbb{B})$ are isomorphic.*

References

1. Serre J. P. *Trees*. Berlin/Heidelberg/New York: Springer, 1980. 164 p.

2. Clay M., Forester M. *Whitehead moves for G-trees*. Bull. London Math. Soc. 2009. Vol 41. No. 2. P. 205–212.

3. Forester M. *On uniquenes of JSJ decomposition of finitely generated groups*. Comm. Math. Helv. 2003. Vol. 78. P. 740–751.

4. Clay M. *Deformation spaces of G–trees and automorphisms of Baumslag–Solitar groups*. Groups Geom. Dyn. 2009. No. 3. P. 39–69.

5. Forester M. *Splittings of generalized Baumslag-Solitar groups*. Geometriae Dedicata. 2006. Vol. 121. No. 1. P. 43–59.

6. Clay M., Forester M. *On the isomorphism problem for generalized Baumslag–Solitar groups*. Algebraic & Geometric Topology. 2008. No. 8. P. 2289–2322.

7. Levitt G. *On the automorphism group of generalized Baumslag-Solitar groups*. Geometry & Topology. 2007. Vol. 11. P. 473–515.

8. Forester M. *Deformation and rigidity of simplicial group actions on trees*. Geometry & Topology. 2002. No. 6. P. 219–267.

ON SPLITTING OF THE NORMALIZER OF A MAXIMAL TORUS IN CHEVALLEY GROUPS

Alexey Galt

Sobolev Institute of Mathematics, Siberian Branch of the Russian Academy of Sciences,
4 Acad. Koptyug avenue, 630090 Novosibirsk, Russia galt84@gmail.com

Let $\overline{G}$ be a simple connected linear algebraic group over an algebraically closed field $\overline{\mathbb{F}}_p$ of positive characteristic p. Let σ be a Steinberg endomorphism and $\overline{T}$ a maximal σ-invariant torus of $\overline{G}$. It is well known that all maximal tori are conjugate in $\overline{G}$ and the quotient $N_{\overline{G}}(\overline{T})/\overline{T}$ is isomorphic to the Weyl group W of $\overline{G}$.

Problem 1. Describe groups $\overline{G}$, in which $N_{\overline{G}}(\overline{T})$ splits over $\overline{T}$.

The similar question arises in simple groups of Lie type. Let $T = \overline{T} \cap G$ be a maximal torus in a finite group of Lie type G and $N = N_{\overline{G}}(\overline{T}) \cap G$ be the algebraic normalizer of G.

Problem 2. Describe groups G and their maximal tori T, in which N splits over T.

Problem 1 was solved for Chevalley groups. It is convenient to present the results in the following table:

Group	Existence of a complement
$SL_n(\overline{\mathbb{F}}_p)$	$p = 2$ or n is odd
$PSL_n(\overline{\mathbb{F}}_p)$	Always
$Sp_{2n}(\overline{\mathbb{F}}_p)$	$p = 2$
$PSp_{2n}(\overline{\mathbb{F}}_p)$	$p = 2$ or $n \leq 2$
$SO_{2n+1}(\overline{\mathbb{F}}_p)$	Always
$SO_{2n}(\overline{\mathbb{F}}_p)$	Always
$PSO_{2n}(\overline{\mathbb{F}}_p)$	Always
$E_8(\overline{\mathbb{F}}_p)$	$p = 2$
$E_7(\overline{\mathbb{F}}_p)$	$p = 2$
$E_6(\overline{\mathbb{F}}_p)$	$p = 2$
$F_4(\overline{\mathbb{F}}_p)$	$p = 2$
$G_2(\overline{\mathbb{F}}_p)$	Always

Problem 2 was solved for classical Chevalley groups. Let $\{n_1, \ldots, n_m\}$ be a partition of n. We assume that

$$n_1 = \ldots = n_{l_1} < n_{l_1+1} = \ldots = n_{l_1+l_2} < \ldots < n_{l_1+\ldots+l_{r-1}+1} = \ldots = n_{l_1+\ldots+l_r},$$

and let $a_1 = n_{l_1} l_1, a_2 = n_{l_1+l_2} l_2, \ldots, a_r = n_{l_1+\ldots+l_r} l_r$.

Theorem. *Let T be a maximal torus of $G = SL_n(q)$ with the cycle-type $(n_1)(n_2)\ldots(n_m)$, $m \geqslant 5$. Let $\widetilde{T}$ and $\widetilde{N}$ be the images of T and N in $\widetilde{G} = PSL_n(q)$. Then $\widetilde{T}$ has a complement in $\widetilde{N}$ if and only if one of the following holds:*
(1) q is even;
(2) a_i is odd for some $1 \leqslant i \leqslant r$;
(3) $(n)_2 < (q-1)_2$.

Similar results were obtained all classical Chevalley groups [1, 2].

References

1. Gal't A.A. *On the splitting of the normalizer of a maximal torus in symplectic groups* // Izvestiya: Mathematics 78:3 443–458.

2. Galt A.A. *On splitting of the normalizer of a maximal torus in linear groups* // Journal of Algebra and its Applications. 2015. V. 14. No. 7. 1550114 (20 pages).

ORDERS OF ELEMENTS IN THE EXTENSION OF THE SPECIAL LINEAR GROUP BY THE INVERSE TRANSPOSE INVOLUTION

M.A. Grechkoseeva

Sobolev Institute of Mathematics, 4 Koptyuga av., 630090, Novosibirsk, Russia
grechkoseeva@gmail.com

If G is a finite group, then we refer to the set of the orders of elements of G as the spectrum of G and denote this set by $\omega(G)$. Groups whose spectra coincide are said to be isospectral. Recently, the following assertion known as Mazurov's conjecture was proved: if L is a finite simple sporadic group, or an alternating group, or an exceptional group of Lie type, other than J_2, A_6, A_{10} and ${}^3D_4(2)$, or if L is a finite simple classical group of dimension larger than 60, and G is a finite group isospectral to L, then up to isomorphism $L \leqslant G \leqslant \operatorname{Aut} L$ (see [1]).

A natural question arising in this context is when exactly $\omega(G) = \omega(L)$ provided that L is a finite nonabelian simple group and $L < G \leqslant \operatorname{Aut} L$ (cf. [2, Question 17.36]). The answer is known for sporadic and alternating groups, and is of prime interest for groups of Lie type. Every finite group of Lie type can be realized as $\overline{G}_\sigma = C_{\overline{G}}(\sigma)$ for some suitable simple linear algebraic group $\overline{G}$ and a surjective endomorphism σ of $\overline{G}$. The spectra of certain extensions of $\overline{G}_\sigma$ can be computed using the following lemma due to Zavarnitsine [3, Proposition 13].

Lemma 1 (Zavarnitsine). *Let $\overline{G}$ be a connected linear algebraic group over an algebraically closed field of a positive characteristic. Let σ be a surjective endomorphism of $\overline{G}$ and set $\overline{G}_k = C_{\overline{G}}(\sigma^k)$. If G_k is finite for some k, then σ is an automorphism of G_k and $\omega(G_k\sigma) = k \cdot \omega(G_1)$, where $G_k\sigma$ is a coset in $G_k \rtimes \langle\sigma\rangle$.*

Lemma 1 is a powerful tool which allows one to handle extensions by diagonal and field automorphisms, but it cannot be applied to the extension of $PSL_n(q)$ by the involutory graph automorphism, or equivalently, by the inverse transpose automorphism. Recall that the inverse transpose automorphism of $GL_n(q)$ is the automorphism τ acting by $g^\tau = (g^\top)^{-1}$, where $g^\top$ denotes the transpose of g. Calculating the spectrum of $G = PSL_n(q) \rtimes \langle\tau\rangle$ is finding the orders of the elements of the coset $PSL_n(q)\tau$. Since $(g\tau)^2 = gg^\tau$, the latter problem is closely related to the equation $h = gg^\tau$ where h is a given element of $GL_n(q)$ and $g \in GL_n(q)$. This equation has been exhaustively studied by Fulman and Guralnick in [4]. Starting from their work, we first determine for what $h \in SL_n(q)$ there is $g \in SL_n(q)$ such that $gg^\tau = h$ and then resolve the question of isospectrality.

Theorem 1. *Let n and q be odd, $L = PSL_n(q)$, and let τ be the inverse transpose automorphism of L. Then $\omega(L\tau) = 2\cdot\omega(Sp_{n-1}(q))$. If q is a power of a prime p and $G = L\rtimes\langle\tau\rangle$, then $\omega(G) = \omega(L)$ unless one of the following holds:*

(1) *$q \equiv -1 \pmod 4$, $n = 2 + p^{k-1}$ for some $k \geqslant 1$, and $4p^k \in \omega(G) \setminus \omega(L)$;*

(2) *$n = 2^k + 1$ for some $k \geqslant 1$, $(n, q-1) \neq 1$, and $2(q^{(n-1)/2} - 1) \in \omega(G) \setminus \omega(L)$.*

Theorem 2. *Let $n \geqslant 4$ be even, q be a power of an odd prime p, $L = PSL_n(q)$, τ be the inverse transpose automorphism of L, and let $G = L \rtimes \langle\tau\rangle$. Then $\omega(G)$ is the union of $\omega(L)$ and the set of all divisors of the following numbers:*

(i) *$2(q^{n/2} \pm 1)/(4, q^{n/2} \pm 1)$;*

(ii) *$2[q^{n_1} - \varepsilon_1, q^{n_2} - \varepsilon_2]/\delta$, where $2(n_1 + n_2) = n$, $\varepsilon_1, \varepsilon_2 \in \{+1, -1\}$, $\delta = 2$ if $(q^{n_1} - \varepsilon_1)_2 = (q^{n_2} - \varepsilon_2)_2$, and $\delta = 1$ otherwise;*

(iii) *$2p^k$ if $n = 1 + p^{k-1}$, $k \geqslant 2$.*

Furthermore, $\omega(G) = \omega(L)$ unless one of the following holds:

(1) *$q \equiv 1 \pmod 4$, $(n)_2 \leqslant (q-1)_2$, and $q^{n/2} + 1 \in \omega(G) \setminus \omega(L)$;*

(2) *$n = 1 + p^{k-1}$, $k \geqslant 2$, and $2p^k \in \omega(G) \setminus \omega(L)$;*

(3) *$(n, q-1)_{2'} \neq 1$, $(n)_{2'} > 3$, and $\omega(G) \setminus \omega(L)$ contains $2[q^{n_1} - 1, q^{n_2} + 1]$, where $n_1 = (n)_2$, $n_2 = n/2 - (n)_2$.*

In the theorems above (a, b) and $[a, b]$ denote the greatest common divisor and the least common multiple of positive integers a and b, respectively. Also we write $(a)_2$ to denote the highest power of 2 dividing a and $(a)_{2'}$ to denote $a/(a)_2$.

Observe that similar results can be obtained for unitary groups since there is a one-to-one correspondence between the conjugacy classes in the coset $PSL_n(q)\tau$ and those in the coset $PSU_n(q)\tau$ (under some proper definition of $GU_n(q)$), and this correspondence preserves the order of the elements in a conjugacy class [5, Section 2].

References

1. Grechkoseeva M.A., Vasil'ev A.V. *On the structure of finite groups isospectral to finite simple groups* // J. Group Theory. DOI: 10.1515/jgth-2015-0019.

2. *The Kourovka notebook. Unsolved problems in group theory.* 17th edition. Institute of Mathematics, Novosibirsk, 2010.

3. Zavarnitsine A.V. *Recognition of the simple groups $U_3(q)$ by element orders* // Algebra Logic. 2006. V. 45. No. 2. P. 106–116.

4. Fulman J., Guralnick R. *Conjugacy class properties of the extension of $GL(n, q)$ generated by the inverse transpose involution* // J. Algebra. 2004. V. 275. No. 1. P. 356–396.

5. Gow R., Vinroot C.R. *Extending real-valued characters of finite general linear and unitary groups on elements related to regular unipotents* // J. Group Theory. 2008. V. 11. P. 299–331.

CONSTRUCTION OF SELF-DUAL BINARY CODES

C. Hannusch

Institute of Mathematics, University of Debrecen, Egyetem tér 1., H-4032, Debrecen, Hungary
carolin.hannusch@science.unideb.hu

Results stated in this talk were obtained by the author in a joint work with Piroska Lakatos (University of Debrecen, Hungary).

Let $K = GF(p)$ and G be an elementary abelian p-group of order p^m. We regard the p^k-dimensional subspace C of the modular group algebra $K[G] = \mathcal{A}_{p,m}$ as linear codes. We will denote the Jacobson radical of $\mathcal{A}_{p,m}$ by J. The class of codes in the radical of the group algebra $\mathcal{A}_{p,m}$ has a significant practical value. If the minimum (Hamming) weight of a k-dimensional subspace C is d, then the linear code C is referred to as a (p^m, p^k, d)-code.

For abelian G Berman [1] initiated the study of the Jacobson radical of the group algebra $\mathcal{A}_{p,m}$. For $\mathcal{A}_{2,m}$ he has proved that the well known Reed-Muller (RM)-codes are the powers of the radical of the group algebra. A code C in $\mathcal{A}_{p,m}$ is called a *monomial code* [2] if it is generated by some monomials of the form $X_1^{b_1} X_2^{b_2} \dots X_m^{b_m}$, where $0 \le b_i \le p-1$. We will present codes which are ideals in J. These codes are monomial codes. Some of them are isomorphic to well-known codes and some of them are not. We give a new method to construct self-dual binary codes with parameters $(2^m, 2^{m-1}, 2^{\frac{m}{2}})$ for arbitrary even m. These codes are self-dual and they have some very good properties. The construction is introduced using "complement free" sets of binary m-tuples as the exponents of the generator elements. For $m = 2k$ denote the set of all k-subsets of $\{1, 2, \dots, 2k\}$ by X. The elements of X can be described with the help of binary sequences $(k_1, k_2, \dots, k_m)$ consisting of k zeros and k ones in any order. Clearly the cardinality of the set X is $\binom{2k}{k}$. We say that a subset Y of binary m-tuples in X is *complement free* if $y \in Y$ implies $\mathbf{1} - y \notin Y$, where $\mathbf{1} = (1, 1, \dots, 1)$. Then a maximal complement free subset of X has cardinality $\frac{1}{2}\binom{2k}{k} = \binom{2k-1}{k-1}$.

The construction is described in the following theorem:

Theorem. *Let C be a binary code with* $\mathrm{RM}(k-1, 2k) \subset C \subset \mathrm{RM}(k, 2k)$. *Suppose that a basis of the quotient space $C/\mathrm{RM}(k-1, 2k)$ is*

$$\left\{ \prod_{i=1}^{m} X_i^{k_i} + \mathrm{RM}(k-1, 2k), \ \textit{where } 0 \le k_i \le 1 \textit{ and } \sum_{i=1}^{m} k_i = k \right\},$$

where the set of the exponents $(k_1, k_2, \dots, k_m)$ is a maximal complement free subset among the k-subsets of $\{1, 2, 3, \dots, 2k\}$.

Then C forms a $[2^{2k}, 2^{2k-1}, 2^k]$ self-dual doubly-even code.

Along with investigating these codes and pointing out their good properties, we will also provide some other codes in J.

References

1. Berman S.D. *On the theory of group codes* // Kibernetika. 1967. Vol. 3. No. 1. P. 31–39.

2. Drensky V., Lakatos P. *Monomial ideals, group algebras and error correcting codes* // Lecture Notes in Computer Science, Springer Verlag. 1989. Vol. 357. P. 181–188.

ON INTERSECTION OF TRIPLE OF PREFRATTINI SUBGROUPS IN FINITE SOLUBLE GROUP

S.F. Kamornikov

Gomel Branch of International University MITSO, 46A Oktyabrya str., 246019, Gomel, Belarus
sfkamornikov@mail.ru

In this paper we consider finite groups only, so the term "group" always means "a finite group".

D.S. Passman in [1] has proved that a p-soluble group G always possesses three Sylow p-subgroups such that their intersection is equal to $O_p(G)$. Later V.I. Zenkov [2] has proved the same statement for an arbitrary group. In [3–4] S. Dolfi has proved that in every π-soluble group G there exist elements $x, y \in G$ such that the equality $H \cap H^x \cap H^y = O_\pi(G)$ holds.

In connection with these results, in the *Kourovka Notebook* [5] the author formulated the following Problem 17.55:

Does there exist an absolute constant k such that for any prefrattini subgroup H in any finite soluble group G there exist k conjugates of H whose intersection is $\Phi(G)$, the Frattini subgroup of G?

The main goal of this paper is to give an affirmative answer to this question.

Theorem. *Let H be a prefrattini subgroup of a soluble group G. Then there exist elements $x, y \in G$ such that the equality $H \cap H^x \cap H^y = \Phi(G)$ holds.*

Corollary 1. *Let H be a prefrattini subgroup of a soluble group G. If $\Phi(G) = 1$, then there exist elements $x, y \in G$ such that the equality $H \cap H^x \cap H^y = 1$ holds.*

Corollary 2. *Let H be a prefrattini subgroup of a soluble group G. Then the inequalities $|H| \leq \sqrt[3]{|G|^2 \cdot |\Phi(G)|}$ and $|H/\Phi(G)| \leq |G : H|^2$ hold.*

Corollary 3. *Let H be a prefrattini subgroup of a soluble group G. If $\Phi(G) = 1$, then the inequalities $|H| \leq \sqrt[3]{|G|^2}$ and $|H| \leq |G : H|^2$ hold.*

The concept of a prefrattini subgroup of a soluble group was introduced by Gaschütz in [6]. Considering a complemented chief factor L/K of a soluble group G as a G-module, Gaschütz has proved that G has a normal section that is a completely reducible G-module whose composition components are G-isomorphic to L/K, and the composition length m is equal to the number of complemented and G-isomorphic to L/K factors of a chief series of G. This section is denoted by $Cr_G(L/K)$ and called the *crown of G corresponding to L/K*. A constructive definition of the crown of a soluble group G corresponding to a complemented chief factor L/K is given below:

$$Cr_G(L/K) = C_G(L/K)/R,$$

where R is the intersection of the cores of maximal subgroups complementing L/K.

A crown of a soluble group G is the crown corresponding to a complemented chief factor of G. The set of all crowns of G is denoted by $Cr(G)$. The Jordan-Hölder theorem implies that for the construction of $Cr(G)$ it suffices to consider some chief series of G and to choose in it a maximal system $L_1/K_1, \ldots, L_t/K_t$ of pairwise non-G-isomorphic complemented chief factors. Then we have $Cr(G) = \{Cr_G(L_1/K_1), ..., Cr_G(L_t/K_t)\}$.

Definition. Let G be a soluble group, and $Cr(G) = \{Cr_G(L_1/K_1), ..., Cr_G(L_t/K_t)\}$. Let G_i be a complement of $Cr_G(L_i/K_i)$ in G, where $i \in I = \{1, 2, ..., t\}$. Then the subgroup $\bigcap_{i \in I} G_i$ is called a prefrattini subgroup of G.

By Definition, every soluble group has at least one prefrattini subgroup.

The following theorem gives basic properties of prefrattini subgroups.

Theorem [6]. *For a soluble group G, the following conditions hold*:

1) *if H is a prefrattini subgroup of G and $N \lhd G$, then*:

a) *H^x is a prefrattini subgroup of G for any element $x \in G$;*

b) HN/N *is a prefrattini subgroup of* G/N;

c) H *covers all Frattini chief factors of* G *and avoids all complemented chief factors of* G;

d) $Core_G(H) = \Phi(G)$;

e) $|H|$ *is the product of the orders of all Frattini chief factors in a chief series of* G;

2) *any two prefrattini subgroups of* G *are conjugate in* G.

References

1. Passman D.S. *Groups with normal solvable Hall p′-subgroups* // Trans. Amer. Math. Soc. 1966. V. 123. No. 1. P. 99–111.

2. Zenkov V.I. *Intersections of nilpotent subgroups in finite groups* // Fundam. Prikl. Mat. 1996. V. 2. No. 1. P. 1–92.

3. Dolfi S. *Intersections of odd order Hall subgroups* // Bull. London Math. Soc. 2005. V. 37. No. 1. P. 61–66.

4. Dolfi S. *Large orbits in coprime actions of solvable groups* // Trans. Amer. Math. Soc. 2008. V. 360. No. 1. P. 135–152.

5. Mazurov V.D., Khukhro E.I. *Unsolved problems in group theory: The Kourovka Notebook*. Novosibirsk: Russian Academy of Sciences, Siberian Branch, Institute of Mathematics, 2010.

6. Gaschütz W. *Praefrattinigruppen* // Arch. Math. 1962. V. 13. No. 3. P. 418–426.

SUBGROUP-CLOSED LATTICE AND K-LATTICE FORMATIONS

S.F. Kamornikov[1], Xiaolan Yi[2]

[1]Gomel Branch of International University MITSO, 46A Oktyabrya str., 246019, Gomel, Belarus
sfkamornikov@mail.ru
[2] Zhejiang Sci-Tech University, 310018, Hangzhou, China
yixiaolan2005@126.com

All considered groups are finite.

One of the most striking results in the theory of subnormal subgroups is the celebrated "join" theorem, proved by H. Wielandt in 1939: the subgroup generated by two subnormal subgroups of a finite group is itself subnormal. As a result, the set $sn(G)$ of all subnormal subgroups of a group G is a sublattice of the subgroup lattice.

The Wielandt theorem was developed in the formation theory using concepts of $\mathfrak{F}$-subnormality and K-$\mathfrak{F}$-subnormality.

The first concept was proposed by R. Carter and T. Hawkes. Let $\mathfrak{F}$ be a non-empty formation. A subgroup H of a group G is said to be $\mathfrak{F}$-*subnormal* in G if either $H = G$ or there exists a maximal chain of subgroups

$$H = H_0 \subset H_1 \subset \cdots \subset H_n = G$$

such that $H_i^{\mathfrak{F}} \subseteq H_{i-1}$ for all $i = 1, \ldots, n$. The set of all $\mathfrak{F}$-subnormal subgroups of a group G is denoted by $sn_{\mathfrak{F}}(G)$.

It is rather clear that the $\mathfrak{N}$-subnormal subgroups of a group G for the formation $\mathfrak{N}$ of all nilpotent groups are subnormal, and they coincide in the soluble universe. However the equality $sn_{\mathfrak{N}}(G) = sn(G)$, does not hold in general.

To avoid the above situation, O.H. Kegel introduced a little bit different notion of $\mathfrak{F}$-subnormality. It unites the notions of subnormal and $\mathfrak{F}$-subnormal subgroup.

A subgroup H of a group G is called $\mathfrak{F}$-*subnormal in sense of Kegel* (or simply K-$\mathfrak{F}$-*subnormal*) in G if there exists a chain of subgroups

$$H = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G$$

such that H_{i-1} is either normal in H_i or $H_i^{\mathfrak{F}} \subseteq H_{i-1}$ for all $i = 1, \ldots, n$. We shall write $H \in sn_{K-\mathfrak{F}}(G)$ and denote by $sn_{K-\mathfrak{F}}(G)$ the set of all K-$\mathfrak{F}$-subnormal subgroups of a group G.

Obviously, $sn_{K-\mathfrak{N}}(G) = sn(G)$ for every group G.

Let $\mathfrak{F}$ be a formation. One might wonder whether the set of $\mathfrak{F}$-subnormal subgroups of a group forms a sublattice of the subgroup lattice. As simple examples show, the answer to this question, in general, is negative.

Therefore the following question naturally arises:

Which are the formations $\mathfrak{F}$ for which the set $sn_{\mathfrak{F}}(G)$ is a sublattice of the subgroup lattice of G for every group G?

This question was first proposed by L.A. Shemetkov in his monograph [1, Problem 12] in 1978 and it appeared in the Kourovka Notebook [2, Problem 9.75] in 1984.

In 1992, A. Ballester-Bolinches, K. Doerk, and M.D. Perez-Ramos [3] gave the answer to that question in the soluble universe for subgroup-closed saturated formations. In 1993, A.F. Vasil'ev, S.F. Kamornikov, and V.N. Semenchuk [4] published the solution of the Shemetkov problem in the general finite universe for subgroup-closed saturated formations. The following important result was obtained in 2002. A.F. Vasil'ev and the first author in [5] characterized the subgroup-closed lattice formations which are soluble.

In 1978, O.H. Kegel [6] showed that if $\mathfrak{F}$ is a subgroup-closed formation such that $\mathfrak{F}\mathfrak{F} = \mathfrak{F}$, then the set of all K-$\mathfrak{F}$-subnormal subgroups of a group G is a sublattice of the subgroup lattice of G for every group G. He also asks in [6] for other formations enjoying the lattice property for K-$\mathfrak{F}$-subnormal subgroups:

Which are the formations $\mathfrak{F}$ for which the set $sn_{K-\mathfrak{F}}(G)$ is a sublattice of the subgroup lattice of G for every group G?

In 1993, A.F. Vasil'ev, the first author, and V.N. Semenchuk [4] gave the answer to that question in the general finite universe for subgroup-closed saturated formations.

We say that $\mathfrak{F}$ is a *lattice* (respectively, K-*lattice*) formation if the set of all $\mathfrak{F}$-subnormal (respectively, K-$\mathfrak{F}$-subnormal) subgroups is a sublattice of the lattice of all subgroups in every group.

The following theorem gives the solution to the Shemetkov and Kegel problems for the case of all subgroup-closed formations.

Theorem. *Let $\mathfrak{F}$ be a subgroup-closed formation. The following statements are pairwise equivalent:*

1. *The set of all K-$\mathfrak{F}$-subnormal subgroups is a sublattice of the subgroup lattice of every group.*
2. *The set of all $\mathfrak{F}$-subnormal subgroups is a sublattice of the subgroup lattice of every group.*
3. *$\mathfrak{F} = \mathfrak{M} \times \mathfrak{K} \times \mathfrak{L}$ for some subgroup-closed formations $\mathfrak{M}$, $\mathfrak{K}$ and $\mathfrak{L}$ satisfying the following conditions:*

(a) *$\pi(\mathfrak{M}) \cap \pi(\mathfrak{K}) = \emptyset$, $\pi(\mathfrak{K}) \cap \pi(\mathfrak{L}) = \emptyset$ and $\pi(\mathfrak{M}) \cap \pi(\mathfrak{L}) = \emptyset$.*

(b) *$\mathfrak{M} = \mathfrak{S}_{\pi(\mathfrak{M})}\mathfrak{M}$ is a saturated formation, and it is an $\mathfrak{M}^2$-normal Fitting class.*

(c) *Every non-cyclic $\mathfrak{M}$-critical group G with $\Phi(G) = 1$ is a primitive group of type 2 such that $G/Soc(G)$ is a cyclic group of prime power order.*

(d) *There exists a partition $\{\pi_j | j \in J\}$ of $\pi(\mathfrak{K})$ such that $\mathfrak{K} = \times_{j\in J}\mathfrak{S}_{\pi_j}$ and $|\pi_j| > 1$ for all $j \in J$.*

(e) *$\mathfrak{L} \subseteq \mathfrak{N}_{\pi(\mathfrak{L})}$.*

References

1. Shemetkov L.A. *Formations of finite groups.* Moscow: Nauka, 1978.

2. Mazurov V.D., Khukhro E.I. *Unsolved problems in group theory: The Kourovka Notebook.* Novosibirsk: Russian Academy of Sciences, Siberian Branch, Institute of Mathematics, 2010.

3. Ballester-Bolinches A., Doerk K., Perez-Ramos M.D. *On the lattice of $\mathfrak{F}$-subnormal subgroups* // J. Algebra. 1992. V. 148. No. 1. P. 42–52.

4. Vasil'ev A.F., Kamornikov S.F., Semenchuk V.N. *On lattices of subgroups of finite groups* // *Infinite groups and related algebraic structures.* Kiev: Institute of Mathematics of National Academy of Sciences of Ukraine, 1993. P. 27–54.

5. Vasil'ev A.F., Kamornikov S.F. *The Kegel-Shemetkov problem on lattices of generalized subnormal subgroups of finite groups* // Algebra and Logic. 2002. V. 41. No. 4. P. 28–236.

6. Kegel O.H. *Subgroup lattices of finite groups which properly contain the lattice of subnormal subgroups* // Arch. Math. 1978. V. 30. No. 3. P. 225–228.

A RECURRENCE FORMULA FOR JACK CONNECTION COEFFICIENTS

A.L. Kanunnikov[1], **E.A. Vassilieva**[2]

[1]Moscow State University, Faculty of Mechanics and Mathematics, Moscow, Russia
andrew.kanunnikov@gmail.com
[2] LIX, Ecole Polytechnique, Palaiseau, France
ekaterina.vassilieva@lix.polytechnique.fr

This report is devoted to Jack connection coefficients, a generalization of the connection coefficients of the classical subalgebras of the group algebra of the symmetric group closely related to the theory of Jack symmetric functions. First introduced by Goulden and Jackson (1996) these numbers indexed by three partitions of a given integer n and the Jack parameter α are defined as the coefficients in the power sum expansion of some Cauchy sum for Jack symmetric functions. Goulden and Jackson [1] conjectured that they are polynomials in $\beta = \alpha - 1$ with non negative integer coefficients of combinatorial significance, the *Matchings-Jack conjecture.*

We show that Jack connection coefficients satisfy a recurrence formula when two of the partitions are equal to the single part (n) and prove the Matchings-Jack conjecture in this case.

The ring of symmetric functions Λ has the following bases indexed by partitions λ of integer numbers: monomial basis m_λ, power sums p_λ, Schur polynomials s_λ, zonal polynomials Z_λ (see [2]). Let $\langle \cdot, \cdot \rangle$ be the scalar product on Λ such that $\langle p_\lambda, p_\mu \rangle = z_\lambda \delta_{\lambda\mu}$ where $z_\lambda = \prod_i i^{m_i(\lambda)} m_i(\lambda)!$ ($m_i(\lambda)$ is a number of i-parts of λ). The Schur polynomials are characterized by the fact that they form an orthonormal basis of Λ for $\langle \cdot, \cdot \rangle$ and the transition matrix between Schur and monomial symmetric functions is upper triangular. The zonal polynomials directly linked with the theory of the zonal spherical functions and verify the same properties as the s_λ (except the unit length property) if the scalar product is replaced by $\langle \cdot, \cdot \rangle_2$ with $\langle p_\lambda, p_\mu \rangle_2 = 2^{\ell(\lambda)} z_\lambda \delta_{\lambda\mu}$ where $\ell(\lambda)$ is the number of parts of λ. These functions are linked with classical subalgebras of the group algebra:

I. Class algebra, i. e. the center of $\mathbb{C}S_n$ with the basis $(C_\lambda)_{\lambda \vdash n}$ where C_λ is a sum of permutations of cycle type λ.

II. Double coset algebra, i. e. **Hecke algebra of the Gelfand pair** (S_{2n}, B_n), where B_n is a centralizer of $f_\star = (12)(34)\dots(2n-1, 2n)$, with basis $(K_\lambda)_{\lambda \vdash n}$ where K_λ is a sum of all permutations $\omega \in S_{2n}$ such that $f_\star \omega f_\star \omega^{-1}$ has cycle type $\lambda\lambda$ (see [2]).

Let $c_{\mu\nu}^\lambda$ and $b_{\mu\nu}^\lambda$ be the connection coefficients of these algebras:

$$C_\mu C_\nu = \sum\nolimits_{\lambda \vdash n} c_{\mu\nu}^\lambda C_\lambda, \qquad K_\mu K_\nu = \sum\nolimits_{\lambda \vdash n} b_{\mu\nu}^\lambda K_\lambda.$$

Using an additional parameter α, Henry Jack [3] introduced the bases of **Jack symmetric functions** J_λ^α which are characterized by two properties: (1) $\langle J_\lambda^\alpha, J_\mu^\alpha \rangle_\alpha = j_\lambda(\alpha)\delta_{\lambda\mu}$ where the scalar product $\langle \cdot, \cdot \rangle_\alpha$ is defined by $\langle p_\lambda, p_\mu \rangle_\alpha = \alpha^{\ell(\lambda)} z_\lambda \delta_{\lambda\mu}$ and $j_\lambda(\alpha)$ is some normalizing factor; (2) the transition matrix between J_λ^α and m_λ is upper triangular. So $J_\lambda^1 = \sqrt{j_\lambda(1)} s_\lambda$ and $J_\lambda^2 = Z_\lambda$.

Goulden and Jackson [1] showed that

$$\sum_{\lambda,\mu,\nu \vdash n} z_\lambda^{-1} c_{\mu\nu}^\lambda p_\lambda(x) p_\lambda(y) p_\lambda(z) = \sum_{\gamma \vdash n} h_\gamma(1) s_\gamma(x) s_\gamma(y) s_\gamma(z),$$

$$\sum_{\lambda,\mu,\nu \vdash n} 2^{-\ell(\lambda)} z_\lambda^{-1} \frac{b_{\mu\nu}^\lambda}{|B_n|} p_\lambda(x) p_\lambda(y) p_\lambda(z) = \sum_{\gamma \vdash n} \frac{Z_\gamma(x) Z_\gamma(y) Z_\gamma(z)}{\langle Z_\gamma, Z_\gamma \rangle_2}$$

and introduced the coefficients $a^{\lambda}_{\mu\nu}(\alpha)$ by the equality

$$\sum_{\lambda,\mu,\nu\vdash n} \alpha^{-\ell(\lambda)} z_{\lambda}^{-1} a^{\lambda}_{\mu\nu}(\alpha) p_{\lambda}(x) p_{\mu}(y) p_{\nu}(z) = \sum_{\gamma\vdash n} \frac{J^{\alpha}_{\gamma}(x) J^{\alpha}_{\gamma}(y) J^{\alpha}_{\gamma}(z)}{\langle J^{\alpha}_{\gamma}, J^{\alpha}_{\gamma}\rangle_{\alpha}}.$$

Computations of $a^{\lambda}_{\mu\nu}(\alpha)$ for all $\lambda,\mu,\nu \vdash n \leq 8$ showed that the $a^{\lambda}_{\mu\nu}(\alpha)$ are polynomials in $\beta = \alpha - 1$ with non negative integer coefficients and of degree at most $n - \min\{\ell(\mu), \ell(\nu)\}$. Goulden and Jackson conjectured this property for arbitrary λ, μ, ν. Moreover, following the combinatorial interpretation in Proposition 1, they also suggest the stronger **Matchings-Jack conjecture.** Dołęga and Féray [4] proved that the $a^{\lambda}_{\mu\nu}(\alpha)$ are polynomials in α with rational coefficients.

Graph interpretation. For a partition $\lambda = (\lambda_1, \ldots, \lambda_p) \vdash n$, consider the graph G on $2n$ vertices consisting of p cycles of lengths $2\lambda_1, \ldots, 2\lambda_p$. A matching in G is a set of edges without common vertices that contains all the vertices of G. Coloring successively the edges of the cycles of G in gray and black colors, we get two matchings: **g** (gray edges) and **b** (black edges). We also colour successively vertices of G in two colours and call a matching of G by *bipartite* if the ends of each its edge have different colors. We call such graph induced by λ **a λ-graph**.

Proposition 1 [1]. *The quantity $b^{\lambda}_{\mu\nu}/|B_n|$ (resp. $c^{\lambda}_{\mu\nu}$) is the number of matchings (resp. bipartite matchings) δ such that $\mathbf{b} \cup \delta$ is a μ-graph and $\mathbf{g} \cup \delta$ is a ν-graph.*

Matchings-Jack Conjecture [1]. *There exists a function* wt *on matchings such that*

$$a^{\lambda}_{\mu\nu}(\beta + 1) = \sum\nolimits_{\delta} \beta^{\mathrm{wt}_{\lambda}(\delta)}$$

for all $\lambda, \mu, \nu \vdash n$ where the summation is over all matchings as in Proposition 1, and $\mathrm{wt}_{\lambda}(\delta) \in \{0, 1, \ldots, n - \min\{\ell(\mu), \ell(\nu)\}\}$, $\mathrm{wt}_{\lambda}(\delta) = 0 \iff \delta$ *is bipartite.*

We prove Matchings-Jack conjecture in the case $\mu = \nu = (n)$ (Theorem 2) using the recurrence formula in Theorem 1. Define the following operations on matchings:

$$\lambda_{\downarrow(k)} = \lambda \setminus k \cup (k-1), \quad \lambda_{\downarrow(k,l)} = \lambda \setminus (k,l) \cup (k+l-1), \quad \lambda^{\uparrow(k,l)} = \lambda \setminus (k+l+1) \cup (k,l).$$

Theorem 1. *For integer n and partition $\lambda \vdash n+1$, the Jack connection coefficients a^{λ}_{nn} verify the following recurrence formula for any $i \in \{1, \ldots, \ell(\lambda)\}$:*

$$a^{\lambda}_{n+1,n+1}(\alpha) = (\alpha - 1)(\lambda_i - 1) a^{\lambda_{\downarrow(\lambda_i)}}_{nn}(\alpha) + \sum_{d=1}^{\lambda_i - 2} a^{\lambda^{\uparrow(\lambda_i - 1 - d, d)}}_{nn}(\alpha) + \alpha \sum_{j \neq i} \lambda_j a^{\lambda_{\downarrow(\lambda_i, \lambda_j)}}_{nn}(\alpha).$$

This formula admits a nice combinatorial interpretation in terms of graphs in the special cases $\alpha = 1, 2$ that provided us with the intuition for the general case and that we used in the proof of Theorem 2. We call a matching δ such that both $\mathbf{b} \cup \delta$ and $\mathbf{g} \cup \delta$ are $2n$-cycles ((n)-graphs) *a good matching*. Denote by $\mathcal{G}(\lambda)$ the set of all good matchings of the λ-graph G.

Theorem 2. *Let λ be a partition of n and G a λ-graph. Then there exists a function* $\mathrm{wt}_{\lambda} \colon \mathcal{G}(\lambda) \to \{0, 1, \ldots, n-1\}$ *such that*

$$a^{\lambda}_{nn}(\beta + 1) = \sum_{\delta \in \mathcal{G}(\lambda)} \beta^{\mathrm{wt}_{\lambda}(\delta)}, \quad \mathrm{wt}_{\lambda}(\delta) = 0 \iff \delta \text{ is bipartite.}$$

As a consequence, the quantity $a^{\lambda}_{nn}(\beta+1)$ is a nonnegative integer polynomial in β with constant term $c^{\lambda}_{nn} = a^{\lambda}_{nn}(1)$ and sum of coefficients equal to $b^{\lambda}_{nn}/|B_n| = a^{\lambda}_{nn}(2)$.

References

1. Goulden I.P., Jackson D.M. *Connection coefficients, matchings, maps and combinatorial conjectures for Jack symmetric functions.* Transactions of the American Mathematical Society. 1996. Vol. 348 (3). P. 873–892.

2. Macdonald I. *Symmetric functions and Hall polynomials.* Oxford University Press, 1999.

3. H. Jack. *A class of symmetric polynomials with a parameter.* Proc. R. Soc. Edinburgh (A). 1970. Vol. 69. P. 1–18.

4. Dołęga and V. Féray. *Gaussian fluctuations of Young diagrams and structure constants of Jack characters* // Preprint, arXiv:1402.4615. 2014.

A CHARACTERIZATION OF NILPOTENT NONASSOCIATIVE ALGEBRAS BY INVERTIBLE LEIBNIZ-DERIVATIONS

I. Kaygorodov, Yu. Popov

Institute of Mathematics, Novosibirsk, Russia
kaygorodov.ivan@mail.com, yuri.ppv@gmail.com

In 1955, Jacobson has proved that a finite-dimensional Lie algebra over a field of characteristic zero admitting a non-singular (invertible) derivation is nilpotent. The problem of whether the inverse of this statement is correct remained open until a paper of Dixmier and Lister, where an example of nilpotent Lie algebra all of which derivations are nilpotent (and hence, singular), was constructed. For Lie algebras in prime characteristic the situation is more complicated. In this case there exist non-nilpotent Lie algebras, even simple ones, which admit nonsingular derivations (Benkart, Kostrikin and Kuznetsov).

In a paper of Moens the notion of a Leibniz-derivation of order k is introduced as a generalization of derivations and pre-derivations of Lie algebras. Moens has proved that a finite-dimensional Lie algebra over a field of characteristic zero is nilpotent if and only if it admits an invertible Leibniz-derivation. After that, Fialowski, Khudoyberdiyev and Omirov have proved that a finite-dimensional Leibniz algebra is nilpotent if and only if it admits an invertible Leibniz-derivation. It should be noted that there exist non-nilpotent Filippov (n-Lie) algebras with invertible derivations. The authors have showed that the same result holds for alternative algebras (in particularly, for associative algebras) [1]. Also, in this article an example of nilpotent alternative (non-associative) algebra over a field of positive characteristic possessing only singular derivations was provided.

The main purpose of this talk is to discuss the analogues of Moens' theorem for Jordan, $(-1,1)$- and Malcev algebras.

Acknowledgements. The authors are grateful to RFBR, project 14-01-31122.

References

1. Kaygorodov I., Popov Yu. *Alternative algebras admitting derivations with invertible values and invertible derivations* // Izvestiya: Math. 2014. V. 78. No. 5. P. 922–935.

CRITICAL GROUPS WITH SPECTRA COINCIDING WITH THE SPECTRUM OF $U_3(3)$

Y.V. Lytkin

Siberian State University of Telecommunications and Informatics,
Novosibirsk, Russia jurasicus@gmail.com

All groups in this talk are finite. The *spectrum* $\omega(G)$ of a group G is the set of its element orders. By a *section* of G we mean a quotient group H/N, where $N, H \leq G$ and $N \trianglelefteq H$. Groups G and H are called *isospectral*, if $\omega(G) = \omega(H)$. Let ω be a subset of natural numbers. Following [1], we call a group G *critical with respect to* ω (or ω*-critical*), if ω coincides with the spectrum of G and does not coincide with the spectrum of any proper section of G.

If a simple group L has infinitely many groups isospectral to L, then it is important to study critical groups isospectral to L. In [2, 3] the complete description is given of critical groups isospectral to non-abelian simple alternating and sporadic groups and also the special linear group $SL_3(3)$.

In this work we study groups critical with respect to the spectrum of the projective special unitary group $U_3(3)$. In particular, we prove the following

Theorem. *Let G be a group isospectral to $U_3(3)$ that contains a normal subgroup N, such that $G/N \simeq PGL_2(7)$. Then N is a 2-group and every G-chief factor of N is isomorphic to a 6-dimensional module of the group $PGL_2(7)$. Also $G = NH$ for some subgroup $H \simeq PGL_2(7)$. If in addition G is critical with respect to $\omega(U_3(3))$, then $|N| = 2^6$.*

Moreover, H has a representation $\langle a, b, c \mid a^2 = b^3 = c^2 = (ab)^7 = (ac)^2 = (bc)^2 = [a, b]^4 = 1\rangle$ and if we regard N as a vector space over $GF(2)$ then a base of N can be chosen in such a way that the action of H on N is defined by the following matrices:

$$a \sim \begin{pmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & 1 \end{pmatrix}, \; b \sim \begin{pmatrix} \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot \end{pmatrix}, \; c \sim \begin{pmatrix} \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot \end{pmatrix}.$$

This work was partially supported by RFBR Grants 13-01-00505 and 14-01-90013.

References

1. Mazurov V. D., Shi W. J. *A criterion of unrecognizability by spectrum for finite groups* // Algebra and Logic. 2012. V. 51. No. 2. P. 239–243.

2. Lytkin Y. V. *On groups critical with respect to a set of natural numbers* // Siberian Electronic Mathematical Reports. 2013. V. 10. P. 666–675; `http://semr.math.nsc.ru/`.

3. Lytkin Y. V. *Groups critical with respect to the spectra of alternating and sporadic groups* // Siberian Mathematical Journal. 2015. V. 56, No. 1. P. 101–106.

ON GROUPS OF PERIOD 12

D.V. Lytkina[1], V.D. Mazurov[2]

[1]Siberian State University of Telecommunication and Information Sciences, 86 Kirova str., 630102, Novosibirsk, Russia daria.lytkin@gmail.com
[2] Sobolev Institute of Mathematics
4 Koptjug Av., 630090, Novosibirsk, Russia mazurov@math.nsc.ru

We consider groups of period 12. In particular, we give a criterion for such groups to be locally finite.

It is well known that groups of period 4 and groups of period 6 are locally finite [1–4]. The local finiteness of groups of period 12 with some additional conditions has been proved in [1, 5–7].

For groups of period 12, we reduce the question of the local finiteness to a question of the finiteness of their subgroups generated by three elements of order 3. Our main result is as follows.

Theorem. *A group of period* 12 *is locally finite if and only if every its subgroup that satisfies one of the assumptions* 1 *or* 2 *below, is finite.*

(1) *H is generated by an element a of order* 3 *and elements b and c of order* 2 *such that* $(ab)^3 = (bc)^3 = 1$.

(2) *H is generated by elements a and b of order* 3 *and an element c of order* 2 *such that* $(ac)^2 = 1$.

For the proof of the theorem we first prove the following facts.

Lemma 1. *If G is a finite group of period* 12 *and $p \in \{2, 3\}$, then the p-length of G is at most two, and this bound is exact. Furthermore, if the* 2*-length of G equals* 2 *and the* 2*-length of every proper subgroup of G is less than two, then G is isomorphic to either S_4, or the semidirect product of a non-cyclic group of order* 4 *by the group $B = \langle a, x \mid a^3 = x^4 = 1, a^x = a^{-1}\rangle$. In particular, G contains a subgroup isomorphic to A_4.*

Lemma 2. *If G is a locally finite group of period* 12*, then*

$$G = O_{2,3,2,3,2}(G) = O_{3,2,3,2,3}(G).$$

The proof of the theorem also uses computations with the help of GAP [8]. A good example is given by

Lemma 3. *Suppose that G is a group of period* 12 *generated by an element a of order* 3 *and involutions b, c such that $(ab)^3 = (bc)^3 = 1$. Then G is a semidirect product of the subgroup $H = \langle (bc)^G\rangle$ coinciding with its commutator subgroup, and a group $A = \langle a, b\rangle$ isomorphic to A_4. The subgroup H is generated by elements $x_1 = bc$, $x_2 = x_1^a$, $x_3 = x_2^a$, $x_4 = x_2^b$, $x_5 = x_3^b$, $x_6 = x_5^a$, and the action of A on H is determined by the following equalities:*

$$x_1^a = x_2, x_2^a = x_3, x_3^a = x_1, x_4^a = x_5^{-1}, x_5^a = x_6, x_6^a = x_4; \tag{1}$$

$$x_1^b = x_1^{-1}, x_2^b = x_4, x_3^b = x_5, x_4^b = x_2, x_5^b = x_3, x_6^b = x_6^{-1}. \tag{2}$$

Proof of Lemma 3. Computations in GAP [8] show that in the group

$$K = \langle a, b, c \mid 1 = a^3 = b^2 = c^2 = (ab)^3 = (abc)^3 = (ac)^{12} = (abc)^{12}\rangle$$

the subgroup $H = \langle (bc)^K\rangle$ coincides with its commutator subgroup, and $K/H \simeq A_4$. It is clear that G is a homomorphic image of K, and the kernel of the corresponding homomorphism lies in H. The equality $x_1^b = x_1^{-1}$ follows from the fact that b and c are involutions and $x_1 = bc$. Other equalities from (1) and (2) follow from the definitions of elements x_i, $i = 1, \ldots, 6$, and the defining relations of the group A.

The research of the first author was supported by RFBR, project 13-01-00505 and that of the second author by RFBR, project 14-01-90013.

References

1. Sanov I.N. *Solution of Burnside's problem for exponent 4* // Leningrad State University Annals (Uchenye Zapiski) Math. Ser. 1940. No. 55. P. 166–170 (in Russian).

2. Hall M. *Solution of the Burnside problem for exponent six* // Illinois J. Math. 1958. V. 2. P. 764–786.

3. Newman M.F. *Groups of exponent six* // Computational group theory (Durham, 1982), London: Academic Press. 1984. P. 39–41.

4. Lysenok I.G. *Proof of a theorem of M. Hall concerning the finiteness of the groups* $B(m, 6)$ // Math. Notes. 1987. V. 41. No. 3. P. 241–244.

5. Mamontov A.S. *Groups of exponent 12 without elements of order 12* // Siberian Mathematical Journal. 2013. V. 54, No. 1. P. 114–118.

6. Lytkina D.V., Mazurov V.D., Mamontov A.S. *On local finiteness of some groups of period 12* // Siberian Mathematical Journal. 2012. V. 53, No. 6. P. 1105–1109.

7. Mazurov V.D., Mamontov A.S. *Involutions in groups of exponent 12* // Algebra and Logic. 2013. V. 52, No. 1. P. 67–71.

8. *GAP: Groups, algorithms and programming* // An electronic resource. Mode of access: http://www/gap-system.org.

SOME REPRESENTATIONS OF FINITE GROUPS

Dmitry Malinin
Minsk dmalinin@gmail.com

We consider the arithmetic background of integral representations of finite groups over the maximal orders of local and algebraic number fields.

Some infinite series of integral pairwise inequivalent absolutely irreducible representations of finite p-groups with the additional congruence conditions are constructed. Certain problems concerning integral two-dimensional representations over number rings are discussed.

In his recent publication [9] J.-P. Serre emphasized remarkable connections between integral irreducible representations of the group of quaternions and the genus theory of Gauss and Hilbert, and the theory of Hilbert's symbol. This was also considered in our recent paper [7] as an application to the description of globally irreducible representations over arithmetic rings which was earlier introduced by F. Van Oystaeyen and A. E. Zalesskii, see [8]. This is also motivated by the following question considered by J.-P. Serre, W. Feit and other mathematicians (see also [1, 2, 6, 9]):

Let $\rho : G \to GL_n(K)$ be a linear representation of a finite group G over a number field K. Is it possible to realize ρ over O_K, the ring of integers of K, i. e. is ρ conjugate to a homomorphism of G into $GL_n(O_K)$?

Another approach to generalization of integral representations of finite groups was proposed by D. K. Faddeev in [3] (see also [4] and [5]) where a generalization of the theory of Steinitz and Chevalley has been suggested.

References

1. Cliff G., Ritter J., Weiss A. *Group representations and integrality* // J. fur die reine und angew. Math. 1992. Vol. 426. P. 193–202.

2. Cram G.- M., Neisse O. *On Integral Representations over Cyclotomic Fields* // J. of Number Theory. 1996 Vol. 61, No. 1. P. 44–51.

3. Faddeev D.K. *On generalized integral representations over Dedekind rings* // Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov (POMI); Voprosy Teor. Predstav. Algebr i Grupp. 1995. Vol. 227. Part 4. P. 113 – 118 (in Russian); English translation in J. Math. Sci. (New York). 1998. Vol. 89. No. 2. P. 1154–1158.

4. Faddeev D.K. *Tables of the fundamental unitary representations of the Fedorov groups* // Trudy Mat. Steklov Inst. 1961. P. 3–174.

5. Faddeev D.K. *An introduction to the multiplicative theory of modules of integral representations* // Trudy Mat. Inst. Steklov. 1965. Vol. 80. P. 145–182 (in Russian).

6. Knapp W., Schmidt P. *An extension theorem for integral representations* // J. Austral. Math. Soc. (Ser. A). 1997. Vol. 63, P. 1–15.

7. Malinin D., Van Oystaeyen F. *Realizability of two-dimensional linear groups over rings of Integers of algebraic number fields* // Algebras and Representation Theory. 2011. Vol. 14. No. 2. P. 201–211.

8. Van Oystaeyen F., ZalesskiĭA.E. *Finite groups over arithmetic rings and globally irreducible representations* // J. Algebra. 1999. Vol. 215. P. 418–436.

9. Serre J.-P. *Three letters to Walter Feit on group representations and quaternions* // J. Algebra. 2008. Vol. 319. No. 2. P. 549–557.

PERIODIC GROUPS WHOSE ELEMENT ORDERS ARE SMALL

A. Mamontov

Institute of Mathematics, Novosibirsk, Russia

andreysmamontov@gmail.com

A group G is said to be *periodic* if, for every $g \in G$ there exists a natural n such that $g^n = 1$. If there exists a common n with $g^n = 1$ for all $g \in G$ then n is called a *period* of G and the smallest such n is said to be the *exponent* of G. A group G is *locally finite* if every finite set of its elements is contained in a finite subgroup. The class C_n of groups of period n is a *variety*, i.e. it is closed under taking subgroups, factor groups and cartesian products.

The set $\omega(G)$ consisting of all orders of elements of G is called the *spectrum* of G. If $\omega(G)$ is finite then $\mu(G)$ is the set of maximal elements of $\omega(G)$ with respect to division.

We consider the following general question. If $\omega(G)$ is given, what can we say about G, in particular, is such G locally finite? Some recent results here are the following:

- (E. Jabara, D. V. Lytkina, V. D. Mazurov, A. S. Mamontov, 2014) Suppose that $\mu(G) = \{4, 5, 6\}$. Then G is locally finite and one of the following statements holds:
  1. $N = O_5(G)$ is a non-trivial elementary Abelian group, $G = NC$, where C is isomorphic to $\langle x, y \mid x^3 = y^4 = 1, x^y = x^{-1} \rangle$, or $SL_2(3)$, and C acts freely on N.
  2. $T = O_2(G)$ is a non-trivial elementary Abelian group, and $G/T \simeq A_5$.
  3. G is isomorphic to S_5 or S_6.
- (E. Jabara A. S. Mamontov, 2015) Suppose that $\mu(G) = \mu(L_3(4)) = \{3, 4, 5, 7\}$ then $G \simeq L_3(4)$.
- (A. S. Mamontov, 2015) If $\mu(G) = \{6, 7\}$, then G is an extension of a locally finite group by a group of odd order.

COMMUTATIVE MATRIX ALGEBRAS OF LENGTH $n-2$

O.V. Markova

Lomonosov Moscow State University, Department of Mechanics and Mathematics
1 Leninskie Gory, 119991, Moscow, Russia
ov_markova@mail.ru

Definition. The *length of a finite system of generators* $\mathcal{S}$ for a finite-dimensional associative algebra $\mathcal{A}$ over an arbitrary field is defined as the minimal nonnegative integer $l(\mathcal{S})$ such that the words in $\mathcal{S}$ of length not exceeding $l(\mathcal{S})$ span this algebra (as a vector space). The maximal length for the systems of generators of an algebra is referred to as the *length of the algebra*, we denote it by $l(\mathcal{A})$ (see [1]).

The problem of computing the length of the full matrix algebra $M_n(\mathbb{F})$ over a field as a function of the matrix size n was stated by A. Paz in [2] and is still open in general. On the other hand, for a commutative subalgebra in the matrix algebra of order n an upper bound linear on n is known. In particular, for algebras over the field of complex numbers $\mathbb{C}$ A. Paz has shown that this length is at most $n-1$. Later it has been proved in [3-4] that this bound also holds for commutative matrix subalgebras over arbitrary fields and that a commutative subalgebra $\mathcal{A}$ in the matrix algebra $M_n(\mathbb{F})$ satisfies the equation $l(\mathcal{A}) = n-1$ if and only if $\mathcal{A}$ is generated by a *nondegenerate* matrix C, i.e. by such a matrix $C \in M_n(\mathbb{F})$, that $\dim_{\mathbb{F}}(\langle C^0 = I_n,\ C,\ C^2, \ldots,\ C^{n-1}\rangle) = n$.

In the present talk we describe commutative subalgebras of length $n-2$ (closest to the maximal one) in the algebra $M_n(\mathbb{F})$ over fields which contain at least $n+1$ elements.

The following theorem shows that this question can be reduced to the case of nilpotent commutative subalgebras:

Theorem 1. *Let $\mathbb{F}$ be an algebraically closed field, $n \in \mathbb{N}$, $n \geq 2$, and let $\mathcal{A}$ be a commutative subalgebra in $M_n(\mathbb{F})$ with $l(\mathcal{A}) = n-2$. Then there exist a number $m \in \mathbb{N}$, $2 \leq m \leq n$, a commutative subalgebra $\mathcal{B} \subseteq M_m(\mathbb{F})$ of length $m-2$ and of the form $\mathbb{F}E+\mathcal{N}$, where $\mathcal{N}$ is a nilpotent algebra, and if $m < n$, a commutative subalgebra $\mathcal{C} \subseteq M_{n-m}(\mathbb{F})$ generated by a nondegenerate matrix, such that the algebra $\mathcal{A}$ is conjugate to the algebra $\mathcal{B} \oplus \mathcal{C}$.*

Applying the description of some nilpotent commutative subalgebras in $M_n(\mathbb{F})$ given by D.A. Suprunenko, R.I. Tyshkevich [5, Chapter 3] and I.A. Pavlov [6], we obtain our main result:

Theorem 2. *Let $n \geq 3$ and let $\mathbb{F}$ be a field with at least $n+1$ elements. Set $A = E_{1,2} + \cdots + E_{n-2,n-1}$, where $E_{i,j}$ denotes the matrix with the unit on the position (i,j) and zeros on the other positions. Let $\mathcal{A}$ be a commutative subalgebra in $M_n(\mathbb{F})$ that contains the identity matrix I_n. Then $l(\mathcal{A}) = n-2$ if and only if the algebra $\mathcal{A}$ is conjugate in $M_n(\mathbb{F})$ to one of the following algebras:*

1. $\mathbb{F}I_2 \oplus \mathcal{C}_{n-2}$, *where* $\mathcal{C}_{n-2} \subset M_{n-2}(\mathbb{F})$ *is a subalgebra generated by a nondegenerate matrix;*

2. $\mathcal{A}_{0;n} = \langle I_n, A, A^2, \ldots, A^{n-2}\rangle$;

3. $\mathcal{A}_{1;n} = \langle E_{1,n},\ C|\ C \in \mathcal{A}_{0;n}\rangle$;

4. $\mathcal{A}_{2;n} = \langle E_{n,n-1},\ C|\ C \in \mathcal{A}_{0;n}\rangle$;

5. $\mathcal{A}_{3;4}(\alpha) = \langle E_{1,4} + \alpha E_{4,3},\ C|\ C \in \mathcal{A}_{0;4}\rangle$, $\alpha \in \mathbb{F} \setminus \{0\}$ *for* $n = 4$;

6. $\mathrm{char}\mathbb{F} = 2$, $\mathcal{A}_{4;4} = \langle E_4, E_{1,2} + E_{3,4},\ E_{1,3} + E_{2,4},\ E_{1,4}\rangle$ *for* $n = 4$ *and* $\mathrm{char}\mathbb{F} = 2$;

7. $\mathcal{A}_{5;4}(\beta) = \left\{ \begin{pmatrix} aC(\beta) + bI_2 & cC(\beta) + dI_2 \\ O & aC(\beta) + bI_2 \end{pmatrix} | a,b,c,d \in \mathbb{F} \right\}$, *where* $C(\beta)$ *is the companion matrix of an irreducible polynomial* $t^2 + \beta \in \mathbb{F}[t]$, *for* $n = 4$ *and* $\mathrm{char}\mathbb{F} = 2$;

8. $\mathcal{A}_{j;m} \oplus \mathcal{C}_{n-m}$, *where* $j = 0, 1, 2$, $3 \leq m < n$, $\mathcal{C}_{n-m} \in M_{n-m}(\mathbb{F})$ *is a subalgebra generated by a nondegenerate matrix.*

Algebras of types 2–7 are pairwise non-conjugate.

This result is a generalization of a similar classification obtained for algebras over algebraically closed fields in [7].

The author has been partially supported by grants MD-962.2014.1 and RFBR No. 15-31-20329.

References

1. Pappacena C.J. *An upper bound for the length of a finite-dimensional algebra* // J. Algebra. 1997. No. 197. P. 535–545.

2. Paz A. *An application of the Cayley–Hamilton theorem to matrix polynomials in several variables* // Linear Multilinear Algebra. 1984. V. 15. P. 161-170.

3. Guterman A.E., Markova O.V. *Commutative matrix subalgebras and length function* // Linear Algebra Appl. 2009. V. 430. P. 1790-1805.

4. Markova O.V. *Characterization of commutative matrix subalgebras of maximal length over an arbitrary field* // Vestn. Mosk. Univ. Ser. 1. 2009. No. 5. P. 53-55; English transl. in Mosc. Univ. Math. Bull. 2009. V. 64, No. 5. P. 214-215.

5. Suprunenko D.A., Tyshkevich R.I. *Commutative matrices*. 2-nd edition, URSS: Moscow, 2003.

6. Pavlov I.A. *On commutative nilpotent algebras of matrices* // Dokl. Akad. Nauk BSSR. 1967. V. 11, No. 10. P. 870-872.

7. Markova O.V. *On the lengths of matrix algebras and sets of matrices* // Proceedings of the XII International Conference "Algebra and Number Theory: Modern Problems and Applications", dedicated to 80-th anniversary of Professor V. N. Latyshev, Tula, 21-25 April 2014. P. 113–115.

ON THE REALIZABILITY OF A GRAPH AS THE GRUENBERG–KEGEL GRAPH OF A FINITE GROUP

N.V. Maslova

N.N. Krasovskii Institute of Mathematics and Mechanics of the Ural Branch of Russian Academy of Sciences,
16 S. Kovalevskaya str., 620990 Yekaterinburg, Russia,
Ural Federal University named after the first President of Russia B.N. Yeltsin,
19 Mira str., 620002 Yekaterinburg, Russia
butterson@mail.ru

In this abstract "a group" always means "a finite group" and "a graph" means "an undirected graph without loops and multiple edges".

The study of arithmetical properties of groups attracts many researchers working in finite group theory. One of problems in this field is concerned with properties of the Gruenberg–Kegel graph of a group.

Let G be a group. Denote by $\pi(G)$ the set of all prime divisors of the order of G and by $\omega(G)$ the *spectrum* of G, i.e., the set of all its element orders. The set $\omega(G)$ determines the *Gruenberg–Kegel graph* (or the *prime graph*) $\Gamma(G)$ of G; in this graph, the vertex set is $\pi(G)$ and distinct vertices p and q are adjacent if and only if $pq \in \omega(G)$.

We say that a graph Γ with $|\pi(G)|$ vertices *can be realized as the Gruenberg–Kegel graph of a group* G if there exists a labeling of the vertices of Γ by distinct primes from $\pi(G)$ such that the labeled graph is equal to $\Gamma(G)$.

The following problem arises.

Problem. *Let* Γ *be a graph. Can* Γ *be realized as the Gruenberg–Kegel graph of a group*?

Of course, in general, the problem has the negative solution. For example, the Gruenberg–Kegel theorem and the description of connected components of the Gruenberg–Kegel graphs for all simple non-abelian groups [1,2] imply that the graph consisting of five pairwise non-adajcent vertices (a 5-coclique) cannot be realized as the Gruenberg–Kegel graph of a group.

There are not many results concerning this interesting problem.

In [3] it has been shown that a graph can be realized as the Gruenberg–Kegel graph of a solvable group if and only if its complement is 3-colorable and triangle free.

I. N. ZharkovIn who was a student of V. D. Mazurov, has proved that a chain can be realized as the Gruenberg–Kegel graph of a group if and only if the length of this chain is at most 4 [4, unpublished].

In [5] it has been shown that any graph with at most five vertices, except a 5-coclique, can be realized as the Gruenberg–Kegel graph of a group.

Herer we give a solution of the problem mentioned above for all complete bipartite graphs $K_{m,n}$, where $K_{m,n}$ is the graph with $m+n$ vertices whose vertices can be divided into two disjoint subsets U and V such that $|U| = m$, $|V| = n$, and vertices are adjacent if and only if they belong to different subsets. We prove the following theorem.

Theorem. *Let Γ be a complete bipartite graph $K_{m,n}$, where $m \leq n$. Then the following statements hold*:

(1) *Γ can be realized as the Gruenberg–Kegel graph of a group if and only if $m + n \leq 6$ and $(m, n) \neq (3, 3)$;*

(2) *if $m + n \leq 6$ and $(m, n) \neq (3, 3), (1, 5)$, then there exist infinitely many sets T of primes such that Γ can be realized as the Gruenberg–Kegel graph of a group G and $T = \pi(G)$;*

(3) *if $(m, n) = (1, 5)$ and Γ can be realized as the Gruenberg–Kegel graph of a group G, then $\pi(G) = \{2, 3, 7, 13, 19, 37\}$, $O_2(G) \neq 1$ and $G/O_2(G) \cong {}^2G_2(27)$.*

References

1. Williams J. S.*Prime graph components of finite groups* // J. Algebra. 1981. V. 69, no. 2. P. 487–513.

2. Kondrat'ev A. S. *Prime graph components of finite simple groups* // Math. USSR Sb. 1990. V. 67. P. 235–247.

3. Gruber A., Keller T. M., Lewis M., Naughton K., Strasser B. *A Characterization of the prime graphs of solvable groups* // J. Algebra. In Press (Corrected Proof). arXiv:1305.2368 [math.GR].

4. Zharkov I. N. *On groups whose prime graph is a chain*, Bachelor work, Novosibirsk State University, 2008 (In Russian, unpublished).

5. Gavrilyuk A. L., Khramtsov I. V., Kondrat'ev A. S., Maslova N. V. *On realizability of a graph as the prime graph of a finite group* // Sib. Electron. Mat. Izv. 2014. V. 11. P. 246–257.

COMMUTATIVE NILPOTENT ALGEBRAS AND RESTRICTIONS OF WEIL REPRESENTATIONS

C. Pallikaros

University of Cyprus, Department of Mathematics and Statistics
1678 Nicosia, Cyprus pallikar@ucy.ac.cy

Let $\mathbb{F}$ be the field $GF(q^2)$ of q^2 elements, q odd, and let V be an $\mathbb{F}$-vector space endowed with a nonsingular Hermitian form φ. Let σ be the adjoint involutory antiautomorphism of $\mathrm{End}_{\mathbb{F}}V$ associated to the form, and let $\mathrm{U}(\varphi)$ be the corresponding unitary group. In this joint work with H. N. Ward, we investigate whether the restrictions of the Weil representation of $\mathrm{U}(\varphi)$ to certain subgroups are multiplicity-free. These subgroups consist of the members of $\mathrm{U}(\varphi)$ in subalgebras of the form $\mathbb{F}I + N$, where N is a σ-stable commutative nilpotent subalgebra of $\mathrm{End}_{\mathbb{F}}V$ with the further property that N contains its annihilator. In this setup, the extremal case of (nonreductive) self-dual pairs in the unitary group for which the self-centralizing Abelian subgroup has scalar semisimple part is being considered.

THE ZIEGLER SPECTRUM OF *A*-INFINITY PLANE SINGULARITY

Gena Puninski

Belarusian State University
av. Nezalezhnosti 4, 220030 Minsk, Belarus punins@mail.ru

Let F be an algebraically closed field of characteristic zero and let $R = F[[x, y]]/(y^2)$ be the so-called A_∞ plane singularity. We consider the theory T of x-torsion free R-modules.

The classification of indecomposable finitely generated modules in T (i.e. finitely generated indecomposable maximal Cohen–Macaulay R-modules) is well known [1]. Namely each such a module is either isomorphic to the right ideal $I_n = (x, y^n)$ of R or to the right ideal $I_\infty = xR$.

We will calculate the Ziegler spectrum, Zg, of torsion-free R-modules, i.e. a topological space (see [2]) whose points are indecomposable pure injective models of T. Because the modules I_n and I_∞ are linearly compact they are (the only) finitely generated points of Zg.

Theorem. *Each infinitely generated point of* Zg *is the following:*

1) the ring of quotients Q of R;

1) the integral closure $\widetilde{R}$ of R in Q;

3) $G = F((y))$ the ring of Laurent power series.

Furthermore one can execute the Cantor–Bendixson analysis on the Ziegler spectrum.

Proposition.

1) The modules I_n, $n < \infty$ are the only isolated points in Zg*;*

2) the modules I_∞ and $\widetilde{R}$ have Cantor–Bendixson rank 1*;*

3) Q and G have CB*-rank* 2*.*

Thus the Cantor–Bendixson rank of Zg *equals 2.*

This note is an announcement of some results from a project, joint with Ivo Herzog, where infinitely generated points of the Ziegler spectrum are used to get a better (than the Auslander–Reiten quiver) understanding of the category of finitely generated R-modules.

References

1. Yoshino Y. *Cohen–Macaulay Modules over Cohen–Macaulay Rings*. Cambridge University Press, 1990.

2. Ziegler M. *Model theory of modules* // Ann. Pure. Appl. Logic. 1984. V. 26. P. 149–213.

ON SCHUR 3-GROUPS

G.K. Ryabov

Novosibirsk State University, Department of Mechanics and Mathematics
11 Pirogova str., 630090, Novosibirsk, Russia gric2ryabov@gmail.com

Let G be a finite group. An S-ring $\mathcal{A}$ over G is a subring of the group ring $\mathbb{Z}G$ that has a linear basis associated with a special partition of G. About 40 years ago R. Pöschel suggested the problem which can be formulated as follows: for which group G every S-ring $\mathcal{A}$ over it is schurian, i.e. the partition of G corresponding to $\mathcal{A}$ consists of the orbits of the one point stabilizer of a permutation group in $Sym(G)$ that contains a regular subgroup isomorphic to G. We prove that the groups $M_{3^n} = \langle a, b \mid a^{3^{n-1}} = b^3 = e, a^b = a^{3^{n-2}+1} \rangle$, where $n \geq 3$, are not Schur and the groups $\mathbb{Z}_3 \times \mathbb{Z}_{3^n}$, where $n \geq 1$, are Schur. Modulo previously obtained results, it follows that every non-cyclic Schur p-group is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ or $\mathbb{Z}_3 \times \mathbb{Z}_{3^n}$, $n \geq 1$, whenever p is an odd prime.

References

1. Evdokimov S., Kovács I., Ponomarenko I. *On schurity of finite abelian groups* // accepted to Comm. Algebra, http://arxiv.org/abs/1309.0989 [math.GR], 2013.

2. Ponomarenko I., Vasil'ev A. *On non-abelian Schur groups* // J. Algebra Appl. 2014. Vol. 8. 1450055 (22 pages).

ON PARTIALLY ORDERED RINGS

E.E. Shirshova

Moscow, Russia

Let G be a partially ordered additive group [1]. An element $x \in G$ is said to be *very much less than* $y \in G$ *(*$x \ll y$*)* if $nx \leqslant y$ for all $n \in \mathbb{Z}$. We denote by M_a the set of all $g \in G$ such that $g \ll a$ for some $a \in G$, where $a > 0$.

Definition 1. *A ring* R *is called a partially right* $\mathcal{K}$*-ordered ring, if it satisfies the conditions: 1)* $< R, + >$ *is a partially ordered group; 2) if* $a > 0$ *in* R*, then* $ar \ll a$ *for all* $r \in R$*. If the order of the group* $< R, + >$ *is linear, we say that the ring* R *is a linear right* $\mathcal{K}$*-ordered ring.*

Theorem 2. *Let* R *be a ring,* I *being an ideal of* R *satisfying the conditions: 1) the rings* $< I, \leqslant_1 >$ *and* $< R/I, \leqslant_2 >$ *are partially right* $\mathcal{K}$*-ordered rings; 2) the conditions* $a \in I$ *and* $a >_1 0$ *imply the inequality* $ar \leqslant_1 a$ *for each* $r \in R$*. Then the ring* R *can be furnished with a partial right* $\mathcal{K}$*-order* $\leqslant$*, from which the order* $\leqslant_1$ *inherits in the ring* I*, and the order* $\leqslant_2$ *inherits in the ring* R/I*; and* I *being a convex ideal of* R *under the order* $\leqslant$*.*

Let $\mathfrak{U}$ be a system of ideals of a ring R, including $\{0\}$ and R. The system of ideals $\mathfrak{U}$ is called *complete*, if for any subsystem of $\mathfrak{U}$ the following is true: both union and intersection of ideals forming this subsystem belong to $\mathfrak{U}$. An inclusion of ideals $A \subset B$ are said *to be a step*, if the relation $A \subseteq J \subseteq B$ implies $A = J$ or $J = B$ for each ideal J of R.

Theorem 3 *If* R *is a linear right* $\mathcal{K}$*-ordered ring, then there exists a complete system of right ideals in* R*, where any step of right ideals* $I \subset J$ *in this system satisfies the conditions: 1)* $JR \subset I$*; 2)* I *is a convex ideal of* J*; 3)* $I = M_b$ *for all* $b \in J \setminus I$*, where* $b > 0$*.*

Theorem 4 *Let* R *be a ring without an identity element, and there exists a complete system of right ideals in* R *which satisfies the condition: if* $I \subset J$ *is any step of right ideals in this system, then* I *is an ideal of* J*, and the quotient group* $< J/I, + >$ *is a torsion-free group. Then* R *can be made into a linear right* $\mathcal{K}$*-ordered ring.*

References

1. Fuchs L. *Partially ordered algebraic systems.* Oxford - London - New York - Paris: Pergamon Press, 1963.

SPECTRAL DECOMPOSITION OF AN INCIDENCE STRUCTURE

Johannes Siemons

School of Mathematics, University of East Anglia, Norwich, NR4 7TJ, UK

Let X and Y be finite sets and let S be a subset of $X \times Y$. Then $\mathcal{S} = (X, Y; S)$ is an *incidence structure* on (X, Y), and we say that $x \in X$ is *incident with* $y \in Y$ if (x, y) belongs to S. Many combinatorial objects can be described efficiently in the language of incidence structures. These includes graphs, codes, designs, simplicial complexes, ranked partially ordered sets, and so on. The automorphism group $G := Aut(\mathcal{S})$ of $\mathcal{S}$ consists of all pairs $(g, h) \in \mathrm{Sym}(X) \times \mathrm{Sym}(Y)$ so

that $(x, y) \in S$ if and only if (x^g, y^h). In particular, we have two distinct actions of G, one on X and one on Y.

In this note we discuss the relationship between these two actions at the level of permutation modules for X and Y.

Let $R = \mathbb{C}$ and denote the free R-module with basis X by RX. The elements of RX thus are all formal sums $\sum_{x\in X} r_x\, x$ where $r_x \in R$. On RX we have the standard inner product $(\ ,\ )$ by setting $(x, x') = 0$ if $x \neq x' \in X$ and $(x, x) = 1$ otherwise. Evidently RX is a permutation module for G by setting $(\sum_{x\in X} r_x\, x)^g := \sum_{x\in X} r_x\, x^g$ for $g \in G$.

To the incidence structure $\mathcal{S} = (X, Y; S)$ now associate two linear *incidence maps* in a standard fashion:

$$\varepsilon\colon\ RX \to RY \quad \text{and} \quad \partial\colon\ RY \to RX,$$

defined on the respective bases by

$$\varepsilon(x) = \sum_{y\colon (x,y)\in S} y \quad \text{for } x \in X \quad \text{and} \quad \partial(y) = \sum_{x\colon (x,y)\in S} x \quad \text{for } y \in Y\,.$$

These maps are adjoints of each other and therefore the maps

$$\nu^+ = \partial\varepsilon\colon\ \ RX \to RX \quad \text{and} \quad \nu^- = \varepsilon\partial\colon\ \ RY \to RY$$

are symmetric with respect to the inner products on RX and RY. Evidently all eigenvalues are real and non-negative.

A simple argument shows that any non-zero eigenvalue of ν^+ is also an eigenvalue of ν^- and vice versa. Furthermore, for such a non-zero eigenvalue the two corresponding eigenspaces are isomorphic to each other via the restriction of ε or ∂. Therefore it make sense to speak of the *non-zero eigenvalues* of $\mathcal{S} = (X, Y; S)$.

Theorem (Spectral Decomposition) *Let $\mathcal{S} = (X, Y; S)$ be a finite incidence structure with eigenvalues $\lambda_0 > \lambda_1 > ... > \lambda_t > 0$. Denote the corresponding eigenspaces by E_0, E_1, .., $E_t \subseteq RX$ and E'_0, E'_1, .., $E'_t \subseteq RY$. Further, denote the kernel of ε and ∂ by $K_X \subseteq RX$ and $K_Y \subseteq RY$, respectively, and let G be the automorphism group of $\mathcal{S}$. Then*

$$RX \;=\; E_0 \oplus E_1 \oplus \ldots \oplus E_t \oplus K_X \quad \textit{and}$$

$$RY \;=\; E'_0 \oplus E'_1 \oplus \ldots \oplus E'_t \oplus K_Y \tag{1}$$

are G-invariant orthogonal decompositions into pairwise isomorphic G-modules $E_i \simeq E'_i$ for all $i = 0, .., t$.

We note that the actual decomposition is obtained in a standard fashion which is completely explicit. The projection $\pi_i : RX \to E_i$ is a polynomial expression in the λ_0, λ_1, ..., λ_t and ν^+. Therefore any element in f in RX is decomposed as $f = f_0 + f_1 + ... + f_t + f_X$ with $f_i = \pi_i(f) \in E_i$ and $f_X \in K_X$. Such explicit formulae are essential in many computations.

For regular graphs (take X=vertices and Y=edges of the graph) this decomposition coincides with the decomposition afforded by the usual graph spectrum. For association schemes (take $X = Y$ and define 'incidence' by 'i-association' for a suitable i) the eigenspaces are closely related (identical in most cases) to the decomposition afforded by the minimal idempotents of the scheme. Fundamental properties of association schemes, such as Delsarte's Linear Programming Bound and estimates for inner and outer distributions are immediate from the explicit decomposition

just mentioned. But we note that these properties of association schemes transfer naturally to incidence structures in general.

For a finite projective space $\mathrm{PG}(n,q)$ we may consider the incidence structure of s-versus t-dimensional subspaces of $\mathrm{PG}(n,q)$. Here the spectra are easy to compute, all spectral values turn out to be integral and all eigenspaces are irreducible $\mathrm{GL}(n,q)$-modules. The same is true for the $q=1$ analogue when $\mathcal{S}$ is the incidence structure of s-versus t-dimensional subsets of a n-set.

These comments show that spectral compositions provide a unifying principle that opens up new perspectives. In this talk I will concentrate on orbits of automorphism groups of incidence structures. This is joint work [1,2] with Ben Summer at UEA and Francesca Dalla Volta at Milan Bicocca.

References

1. Dalla Volta F., Siemons, J. *On the spectral decomposition of an incidence structure* // to appear.
2. Siemons J., Summer B. *On the face complex of the hyperoctahedron* // to appear.

ON SOME ARITHMETIC PROPERTIES OF FINITE GROUPS

A.N. Skiba

Francisk Skorina Gomel State University
104 Sovetskaya str., 246019, Gomel, Belarus
alexander.skiba49@gmail.com

We fix some partition $\sigma = \{\sigma_i | i \in I\}$ of the set of all primes $\mathbb{P}$ (that is, $\mathbb{P} = \cup_{i\in I}\sigma_i$ and $\sigma_i \cap \sigma_j = \emptyset$ for all $i \neq j$). A group G is called **σ-primary** if G is a σ_i-group for some $i = i(G)$.

We say that a finite group G is: **σ-soluble** if every chief factor of G is σ-primary; **σ-nilpotent** if $(H/K) \rtimes (G/C_G(H/K))$ is σ-primary for every chief factor H/K of G.

Based on these concepts, we develop and unify [1–5] some aspects of the theories of soluble and quasinilpotent groups, of the subgroup lattices theory and of the theory of subnormal subgroups.

References

1. Skiba A.N. *On σ-subnormal and σ-permutable subgroups of finite groups* // J. Algebra. 2015. V. 436. P. 1–16.

2. Guo W., Skiba *A.N. Finite groups with generalized Ore supplement conditions for primary subgroup* // J. Algebra. 2015. V. 432. P. 205–227.

3. Skiba A.N. *A generalization of a Hall theorem* // J. Algebra and its Application (accepted).

4. Skiba A.N. *On the generalized σ-Fitting subgroup of finite groups* // Proc. Amer. Math. Soc. (submitted).

5. Guo W., Skiba A.N. *Finite groups with permutable complete Wielandt sets of subgroups* // J. Group Theory. 2015. V. 18. No. 2. P. 191–200.

ON FINITE GROUPS ISOSPECTRAL TO SIMPLE LINEAR GROUPS

A.M. Staroletov

Sobolev Institute of Mathematics, 4 Acad. Koptyug avenue, 630090, Novosibirsk, Russia
Novosibirsk State University, 2 Pirogova Str., 630090, Novosibirsk, Russia,
staroletov@math.nsc.ru

Given a finite group G, denote by $\omega(G)$ the *spectrum* of G, i. e., the set of its element orders. We call finite groups G and H *isospectral* if $\omega(G) = \omega(H)$. Let $h(G)$ be the number of pairwise nonisomorphic groups isospectral to G. Group G is called *recognizable* (by spectrum) if $h(G) = 1$, *almost recognizable* if $h(G) < \infty$, and *non-recognizable* if $h(G) = \infty$. Since every finite group with a nontrivial normal soluble subgroup is non-recognizable (see [1, Corollary 4] and [2, Lemma 1]), of prime interest is the recognition problem for nonabelian simple groups. It turned out that many of nonabelian finite simple groups are recognizable or at least almost recognizable. Recently it was proved in [3] the following

Theorem 1. *Suppose that $L \simeq PSL_n(q)$ or $L \simeq PSU_n(q)$ and $n \geq 45$. Then a finite group isospectral to L is isomorphic to a group G with $L \leq G \leq AutL$. In particular, there are only finitely many pairwise non-isomorphic finite groups G with $\omega(G) = \omega(L)$.*

It follows from this theorem that simple linear and unitary groups of sufficiently large dimension are almost-recognizable. We continue investigation of the recognition problem for simple linear and unitary groups and prove

Theorem 2. *Suppose that $L \simeq PSL_n(q)$ or $L \simeq PSU_n(q)$ and $27 \leq n \leq 44$. Then a finite group isospectral to L is isomorphic to a group G with $L \leq G \leq AutL$. In particular, there are only finitely many pairwise non-isomorphic finite groups G with $\omega(G) = \omega(L)$.*

The work is supported by Russian Science Foundation (project 14-21-00065).

References

1. Shi W. *A characterization of the sporadic simple groups by their element orders* // Algebra Colloq. 1994. V. 1. No. 2. P. 159–166.

2. Mazurov V.D. *Recognition of finite groups by a set of orders of their elements* // Algebra and Logic. 1998. V. 37. No. 6. P. 371–379.

3. Vasil′ev A.V. *On finite groups isospectral to simple classical groups* // J. Algebra. 2015. V. 243. P. 318–374.

ON THE NORMAL STRUCTURE OF ISOTROPIC REDUCTIVE GROUPS OVER RINGS

Anastasia Stavrova[1], Alexei Stepanov[2]

Saint Petersburg State University
[1]a_stavrova@mail.ru, [2]stepanov239@gmail.com

Let K be a domain and let G be a reductive group scheme over K. We study the normal structure of the group of points $G(R)$ of G over a commutative ring R. For $G = GL_n$, it was described by J. Wilson ($n \geq 4$) and I. Golubchik ($n \geq 3$). For a Chevalley groups the standard normal structure was established by L. Vaserstein with invertible structure constants and by E. Abe in the general case.

Theorem (L. Vaserstein). *Let G be a Chevalley–Demazure group scheme with a reduced irreducible root system $\Phi \neq A_1$ and let R be a commutative ring. Given a normal subgroup $H \lhd G(R)$ there exists an ideal $\mathfrak{a}$ of R such that*

$$E(R, \mathfrak{a}) \leq H \leq C(R, \mathfrak{a}),$$

where $C(R, \mathfrak{a})$ is the preimage of the center under the reduction homomorphism $G(R) \to G(R/\mathfrak{a})$.

The ideal $\mathfrak{a}$ is called the level of H. By standard arguments using standard commutator formulas and elementary computations to describe the level, a proof reduces to extraction of unipotents. This is a difficult part of Vaserstein's and Abe's proofs.

A substantial progeress in understanding the structure theory of isotropic but nonsplit reductive algebraic groups was made by V. Petrov and A. Stavrova. In particular, they proved that the elementary subgroup $E_P(R)$ does not depend of the choice of a parabolic subgroup P of G. Recently A. Stavrova computed the level of a normal subgroup H of $G(R)$ provided that the structure constants are invertible. It turns out that the level is defined by an ideal $\mathfrak{a}$ of R, similarly to the case of Chevalley groups.

Another ingredient is a new proof of the Vaserstein theorem obtained by A. Stepanov. The main idea of this proof consists of 2 parts. First, we reformulate a way of extracting transvections in $\mathrm{GL}_n(R)$ in terms of parabolic subgroups and extract a unipotent element from the generic element of G. Second, we show that if this unipotent vanishes for all elements of H, then H lies in a subscheme, which is proper over any K-algebra. After that by standard arguments one proves that such H is central. In this way we obtain the following result.

Theorem. *Let G be a simple algebraic group scheme of constant type Φ defined over a connected commutative ring K such that the structure constants of Φ are invertible in K. Assume moreover that G contains at least two distinct parabolic subgroups $P_1 < P_2 < G$ over K.*

Let R be a K-algebra. Given a subgroup $H \leq G(R)$, normalized by the elementary subgroup $E(R)$, there exists an ideal $\mathfrak{a}$ of R such that

$$E(R, \mathfrak{a}) \leq H \leq C(R, \mathfrak{a}),$$

where $C(R, \mathfrak{a})$ is the preimage of the center under the reduction homomorphism $G(R) \to G(R/\mathfrak{a})$.

BIG COMPOSITION FACTORS IN RESTRICTIONS OF MODULAR REPRESENTATIONS OF CLASSICAL ALGEBRAIC GROUPS TO SUBSYSTEM SUBGROUPS

I.D. Suprunenko

Institute of Mathematics, National Academy of Belarus
11 Surganov str., 220072, Minsk, Belarus suprunenko@im.bas-net.by

The goal of the talk is to discuss constructing of composition factors with certain special properties in restrictions of modular irreducible representations of classical algebraic groups to subsystem subgroups with two simple components. We shall deal with factors that are in a certain sense big enough (or not too small) for both components of a subgroup under consideration. The existence of such factors yield effective tools for solving a number of questions, in particular, for finding or estimating various parameters of the images of individual elements in representations of such groups, and not only for elements of relevant subsystem subgroups. Often the analysis of restrictions to subsystem subgroups with several simple components yields a useful information that, probably, cannot be obtained if we deal with simple subsystem subgroups only. It was A.E. Zalesskii who has drawn the author's attention to investigating restrictions of representations of simple algebraic groups to non-simple subsystem subgroups. In a joint paper [1] we have proved that the restriction of a nontrivial representation of a simple algebraic group to a subsystem subgroup with two simple components almost always has a composition factor that is nontrivial for both components.

In what follows K is an algebraically closed field, $G = A_r(K)$ or $C_r(K)$, ω_i $(1 \le i \le r)$ are the fundamental weights of G, $\omega(\varphi)$ is the highest weight of an irreducible representation φ, and φ^* is the representation dual to φ. If $\omega(\varphi) = \sum_{i=1}^r a_i\omega_i$, set $s(\varphi) = \sum_{i=1}^r a_i$, put

$$\Sigma(\varphi) = a_1 + 2(a_2 + \ldots + a_{r-1}) + a_r$$

for $G = A_r(K)$ and

$$\Sigma(\varphi) = a_1 + 2(a_2 + \ldots + a_r)$$

for $G = C_r(K)$, in both cases set $t(\varphi) = \Sigma(\varphi) - s(\varphi)$. A subgroup in G is called a subsystem subgroup if it is generated by the root subgroups associated with all roots of a subsystem in the root system. We write an irreducible representation ρ of a semisimple group H with two simple components H_1 and H_2 in the form $\rho_1 \otimes \rho_2$ where ρ_i is an irreducible representation of H_i, $i = 1, 2$. Some of the results that will be discussed are stated below.

Theorem 1. *Let $2 \le l \le r-3$ for $G = A_r(K)$ and $2 \le l \le r-2$ for $G = C_r(K)$, and let φ be an irreducible representation of G. Assume that H_1 and $H_2 \subset G$ are commuting subsystem subgroups of types A_l and A_{r-l-1}, respectively, for $G = A_r(K)$ and of types C_l and C_{r-l} for $G = C_r(K)$. Set $H = H_1H_2$. If $\psi = \psi_1 \otimes \psi_2$ is a composition factor of the restriction $\varphi|H$, then $s(\psi_1) + s(\psi_2) \le \Sigma(\varphi)$. The representation $\varphi|H$ has a composition factor $\tau = \tau_1 \otimes \tau_2$ with $s(\tau_1) = s(\varphi)$ and $s(\tau_2) = t(\varphi)$.*

Theorem 2. *In the assumptions of Theorem 1 if φ is nontrivial, then $\varphi|H$ has a composition factor $\rho = \rho_1 \otimes \rho_2$ with $s(\rho_1) \ge s(\varphi) - 1$ and $s(\rho_2) > 0$.*

Now let K be a field of positive characteristic p. The parameter $s(\varphi)$ is important for describing the behavior of unipotent elements in p-restricted irreducible representations, but for arbitrary representations another parameter appears more useful. By the Steinberg tensor product theorem, an irreducible representation φ of G is equivalent to a tensor product $\bigotimes_{i=0}^j \varphi_i Fr^i$ where Fr is the Frobenius morphism determined by raising the elements of K to the pth power and φ_i are p-restricted irreducible representations of G (all coefficients of their highest weights are less than p). Set $s_1(\varphi) = \sum_{i=0}^j s(\varphi_i)$. One easily observes that $s_1(\varphi)$ is correctly determined. We call φ p-large if $s_1(\varphi) \ge p$. For $p > 2$ it is proved in [2, Theorem 1.1] that for every unipotent element $x \in G$ the degree of the minimal polynomial of $\varphi(x)$ is equal to the order of x if φ is p-large. Hence for applications in the analysis of the behavior of unipotent elements in modular representations it is worth to get an analog of Theorem 1 that for p-large representation φ would yield a factor τ with $s(\tau_1)$ and $s(\tau_2)$ close to the values from Theorem 1 and big $s_1(\tau_1)$. We have such result for $G = A_r(K)$ and a certain class of representations.

Theorem 3. *Let $G = A_r(K)$. In the assumptions of Theorem 1 let φ be a p-restricted representation with highest weight $\sum_{i=1}^r a_i\omega_i$, $s(\varphi) \ge p$, $\sum_{i=1}^m a_i \ne 0$, and $\sum_{i=m+2}^r a_i \ne 0$. Then $\varphi|H$ has a composition factor $\varphi_1 \otimes \varphi_2$, where φ_i is an irreducible representation of H_i, $i = 1, 2$; φ_1 is p-large, $s(\varphi_1) > s(\varphi) - p$; for $t(\varphi) \ge p$ the representation φ_2 is p-large and $s(\varphi_2) > t(\varphi) - p$; if $t(\varphi) < p$, the parameter $s(\varphi_2) \ge t(\varphi)$.*

We shall also discuss how the analysis of restrictions of representations of classical algebraic groups to subsystem subgroups with two simple components can be used for investigating the behavior of unipotent elements in representations. In particular, we use this approach for finding estimates for the number of certain Jordan blocks in the images of such elements in irreducible representations (the blocks of the maximal possible size or the blocks whose order is equal to the order of an element under consideration).

This research has been supported by the Belarusian Republican Foundation for Fundamental Research, project F14-043.

References

1. Suprunenko I.D., Zalesskii A.E. *On restricting representations of simple algebraic groups to semisimple subgroups with two simple components* // Trudy Instituta matematiki. 2005. V. 13. No 2. P. 109–115.

2. Suprunenko I. D. *The minimal polynomials of unipotent elements in irreducible representations of the classical groups in odd characteristic* // Memoirs of the AMS. 2009. Vol. 200. No. 939.

DIVISION ALGEBRAS OF PRIME DEGREE WITH INFINITE GENUS

S.V. Tikhonov

Belarusian State University, Faculty of Mechanics and Mathematics
Nezavisimosti Ave. 4, 220030 Minsk, Belarus tikhonovsv@bsu.by

The genus $\mathbf{gen}(D)$ of a finite-dimensional central division algebra D over a field F is defined as the collection of classes $[D'] \in Br(F)$, where D' is a central division F-algebra having the same maximal subfields as D. In [1], it is shown that there are quaternion algebras with infinite genus. Besides, it is proved that there exists a field F over which there are infinitely many nonisomorphic quaternion algebras with center F, and any two quaternion division algebras with center F have the same genus. In [2], we generalize the results from [1] to the case of division algebras of any prime degree. More precisely, for any prime p, we construct a division algebra of degree p with infinite genus. Moreover, we show that there exists a field K such that there are infinitely many nonisomorphic central division K-algebras of degree p, and any two such algebras have the same genus.

References

1. Meyer J.S. *Division algebras with infinite genus* // Bull. London Math. Soc. 2014. V. 46. No. 3. P. 463–468.

2. Tikhonov S.V. *Division algebras of prime degree with infinite genus* // Preprint `arXiv:1407.5041`.

ON STRONGLY SUPERSOLUBLE FINITE GROUPS

V.A. Vasilyev

Francisk Skorina Gomel State University, Department of Mathematics
104 Sovetskaya str., 246019 Gomel, Belarus vovichx@mail.ru

Throughout this report, all groups are finite. The notion of a normal subgroup takes a central place in the theory of groups. One of its generalizations is the notion of a modular subgroup, i.e. a modular element (in the sense of Kurosh [1, Chapter 2, p. 43]) of the lattice of all subgroups of a group. Recall that a subgroup M of a group G is called modular in G, if the following assertions hold:

1) $\langle X, M \cap Z\rangle = \langle X, M\rangle \cap Z$ for all $X \leq G, Z \leq G$ such that $X \leq Z$, and

2) $\langle M, Y \cap Z\rangle = \langle M, Y\rangle \cap Z$ for all $Y \leq G, Z \leq G$ such that $M \leq Z$.

Properties of modular subgroups were studied in the book [1]. Groups with all subgroups are modular were studied by R. Schmidt [1], [2] and I. Zimmermann [3]. By parity of reasoning with subnormal subgroup, in [3] the notion of a submodular subgroup was introduced.

Definition 1 [3]. A subgroup H of a group G is called submodular in G if there exists a chain of subgroups $H = H_0 \leq H_1 \leq \ldots \leq H_{s-1} \leq H_s = G$ such that H_{i-1} is a modular subgroup in H_i for $i = 1, \ldots, s$.

Using this notion we introduce a key notion of this report.

Definition 2. A group G we will call strongly supersoluble if G is supersoluble and every Sylow subgroup of G is submodular in G.

Denote $s\mathfrak{U}$ the class of all strongly supersoluble groups. The following results are obtained.

Theorem 1. *Let G be a group. Then the following hold:*

1) *if G is strongly supersoluble, then every subgroup of G is strongly supersoluble;*

2) *if G is strongly supersoluble and $N \trianglelefteq G$, then G/N is strongly supersoluble;*

3) *if $N_i \trianglelefteq G$ and G/N_i is strongly supersoluble for $i = 1, 2$, then $G/N_1 \cap N_2$ is strongly supersoluble;*

4) *if $H_i \trianglelefteq G$, H_i is strongly supersoluble, $i = 1, 2$ and $H_1 \cap H_2 = 1$, then $H_1 \times H_2$ is strongly supersoluble;*

5) *if $G/\Phi(G)$ is strongly supersoluble, then G is strongly supersoluble;*

6) *the class of groups $s\mathfrak{U}$ is a hereditary saturated formation.*

We denote $\mathfrak{B}$ the class of all abelian groups of exponent free from squares of primes.

Theorem 2. *The class of all strongly supersoluble groups is a local formation and has a local screen f such that $f(p) = \mathfrak{A}(p-1) \cap \mathfrak{B}$ for any prime p.*

Theorem 3. *Let the group $G = AB$ be the product of nilpotent subgroups A and B. If A and B are submodular in G, then G is strongly supersoluble.*

In Theorem 3 we can't discard the submodularity of one of subgroups.

Example. In group $G = AB$, where $A \simeq Z_{17}$ and $B \simeq Aut(Z_{17}) \simeq Z_{16}$, the subgroup A is submodular, but the subgroup B is not submodular in G. The group G is supersoluble, but not strongly supersoluble. The example also shows that $s\mathfrak{U} \neq \mathfrak{U}$.

Theorem 4. *A group G is strongly supersoluble if and only if G is metanilpotent and any Sylow subgroup of G is submodular in G.*

References

1. Schmidt R. *Subgroup Lattices of Groups*. Berlin etc: Walter de Gruyter, 1994.
2. Schmidt R. Modulare Untergruppen endlicher Gruppen. // J. Ill. Math. 1969. V. 13. P. 358–377.
3. Zimmermann I. Submodular Subgroups in Finite Groups. // Math. Z. 1989. V. 202. P. 545–557.

REDUCED WHITEHEAD GROUPS FOR OUTER FORMS OF ANISOTROPIC GROUPS OF TYPE A_n

V.I. Yanchevskiĭ

Institute of Mathematics, National Academy of Belarus
11 Surganov str., 220072, Minsk, Belarus yanch@im.bas-net.by

Let K be a field and D a central finite-dimensional division K-algebra.

We will be interested in the problem of describing of reduced Whitehead groups of anisotropic groups of type A_n. It is well known that there are two forms (inner and outer) of such groups. As for inner case the groups of K-rational points of anisotropic groups can be described as

$$SL(D) = \{d \in D^* | Nrd_D(d) = 1\},$$

where Nrd_D is the reduced norm homomorphism of D^* to K^*. The describing of normal structure of such groups is a very vast problem for the arbitrary field K, but at least the special case of algebraic number fields K we have the following fundamental Segev's result [1,2].

If one looks at the similar problem for outer forms in anisotropic situation, so there are no any complete results even in the case related to computation of reduced Whitehead groups of such forms. In our talk we will discuss the problem of description of reduced Whitehead groups for multiplicative groups of tame henselian division algebras. More precisely, let k be any field of

characteristic different from 2, and let K be a quadratic extension. Denote the non-trivial Galois automorphism of K over k by σ. Let D be a central division algebra over K (i.e. K = center of D) such that σ extends to an involution τ of D (in this case τ is an unitary involution). One can define the unitary group of D as

$$U(D,\tau) = \{d \in D^* | d^\tau d = 1\},$$

and special unitary group

$$SU(D,\tau) = U(D,\tau) \cap SL(D).$$

The latter group is the group of k-rational points of outer form of an anisotropic k-defined algebraic group of type ${}^2A_{n-1}$. The main problem in this situation is the problem of computation of so-called reduced Whitehead group of D:

$$SUK_1^{an}(D,\tau) = SU(D,\tau)/[U(D,\tau), U(D,\tau)],$$

where $[U(D,\tau), U(D,\tau)]$ is the commutator subgroup of $U(D,\tau)$.

For some time there was a widespread opinion that the above group is trivial at least in the situation of global fields k, but Sury proved in [3] that this is not the case (see also [4] for other kind of fields k). Since groups $SUK_1^{an}(D,\tau)$ are nontrivial in general, then the problem of its computation arises. In the talk among other topics [see 5–10] we will discuss some results, which deal with tame henselian division algebras D and allows us to reduce mainly the computation of $SUK_1^{an}(D,\tau)$ to processing with objects defined over residue algebra $\overline{D}$.

References

1. Segev Y. On finite homomorphic images of the multiplicative group of a division algebra // Ann. of Math. 1999. V. 149. No. 1. P. 219–251.

2. Segev Y., Seitz G.M. Anisotropic groups of type A_n and the commuting graph of finite simple groups // Pacific journal of mathematics. 2002. V. 202. No. 1. P. 125–225.

3. Sury B. On $SU(1,D)/[U(D,\tau), U(D,\tau)]$ for quaternion division algebras D // Archiv der Mathematik. 2008. V. 90. No. 6. P. 493–500.

4. Sethuraman B.A. and Sury B. On the special unitary group of a division algebra // Proc. Amer. Math. Soc. 2005. V. 134. P. 351–354.

5. Yanchevskiĭ V.I. Reduced Whitehead groups and the conjugacy problem for special unitary groups of anisotropic hermitian forms // Journal of Mathematical Sciences (New York). 2013. V. 192. No. 2. P. 250–262

6. Rehmann U., Tikhonov S.V., Yanchevskiĭ V.I. Prescribed behavior of central simple algebras after scalar extension // Journal of Algebra. 2012. V. 351. No. 1. P. 279–293.

7. Albert A.A. Involutorial simple algebras and real Riemann matrices // Annals of mathematics. 1935. V. 36. No. 4. P. 886–964.

8. Hazrat R., Wadsworth A.R. Unitary SK_1 of graded and valued division algebras // Proc. London Math. Soc. 2011. V. 103. No. 3. P. 508–534.

9. Wadsworth A.R., Yanchevskiĭ V.I. Unitary SK_1 for a graded division ring and its quotient division ring // Journal of Algebra. 2012. V. 352. P. 62–78.

10. Wadsworth A.R. Unitary SK_1 of semiramified graded and valued division algebras // Manuscripta Math. in press, preprint available at arXiv:1009.3904.

SINGER CYCLES IN COMPLEX REPRESENTATIONS OF THE GENERAL LINEAR GROUP OVER A FINITE FIELD

A.E. Zalesski

National Academy of Belarus, 11 Surganov str., 220072, Minsk, Belarus
alexandre.zalesski@mail.com

Let $G = PGL(n, q)$ be the projective general linear group of degree n over a finite field of q elements. Let $t \in G$ be a Singer cycle in G, that is, an element of order $(q^n - 1)/(q - 1)$ whose preimage in $GL(n, q)$ is irreducible. Let ϕ be an irreducible representation of G over the complex numbers. We prove that 1 is an eigenvalue of $\phi(t)$, unless, possibly, the degree of ϕ is strictly less than $|t|$, the order of t. This answers a question raised by Pablo Spiga (University of Milan in Bicocca). Irreducible representations of G of degree less than $|t|$ are well known, and the inspection yields a more precise answer. Namely, the degree is either $|t| - 1$ or 1, or 3 for the case where $(n, q) = (3, 2)$.

Apart from an intrinsic interest, the result is assumed to be used as a base of induction for studying the occurrence of eigenvalue 1 for other semisimple elements of G. The method can probably be used to prove that the minimum polynomial degree of $\phi(t)$ equals $|t|$ with the same exceptions as above. In another direction, one can try to generalize the result to other classical groups. (The case $G = PSL(n, q)$ can be easily deduce to the above result.)

The proof is somehow by induction on the number of divisors of n. If n is a prime, the result follows by applying standard results of the Deligne-Lusztig theory of characters of groups of Lie type. The main difficulties arise in performing the induction step. In this situation, that is, when n is not a prime, an essential role in the proof is played by representation theory of groups with cyclic Sylow p-subgroup, not only over the complex numbers but also over the ring of p-adic integers. The starting point is the fact that the group $T = \langle t \rangle$ contains a cyclic Sylow p-subgroup, unless $n = 2$ and $q + 1$ is a 2-power, or $(n, q) = (6, 2)$. However, the reasonuing is not straightforward as the representation theory of groups with cyclic Sylow p-subgroup is efficient for analyzing eigenvalues of p-elements whereas t is not usually a p-element. Exactly this requires realization of the representation in question over the ring of p-adic integers, and some use of the theory of projective modules over such rings.

ABELIAN BY SIMPLE FINITE MOUFANG LOOPS

Andrei V. Zavarnitsine

Sobolev Institute of Mathematics, 4, Koptyug av., 630090, Novosibirsk, Russia
zav@math.nsc.ru

Recall that a loop M is *Moufang* if the identity $xy \cdot zx = (x \cdot yz)x$ holds for all $x, y, z \in M$. Suppose there is a short exact sequence of finite Moufang loops

$$1 \to U \to E \to M \to 1,$$

where U is an abelian group. We will identify U with its image in E and say that the extension E is *minimal*, if U contains no subgroup that is a normal subloop of E. The case where M is simple is of special interest due to the classification [1].

We give explicitly two construction of minimal extensions of abelian groups by simple Moufang loops. The first one is based on the correspondence between Moufang loops and groups with

triality. Given a group G, any RG-module V gives rise to a module for the *wreathlike* triality group $G \times G \times G$ on which S_3 acts by permuting the three factors. We obtain a criterion when this module admits triality and write a multiplication formula in the corresponding Moufang loop which we call a *Moufang semidirect product* $G \leftthreetimes V$.

The second construction may be viewed as a generalization of group action on associative algebras to Moufang loop 'action' on alternative algebras. Whenever a Moufang loop M is mapped to invertible elements $A^\times$ of an alternative algebra A, one can always construct an *outer semidirect product* $M \leftthreetimes U$ which is a Moufang loop, where U is any factor group of the additive group of A invariant under the operators $L_{m,n}$ and T_m for $m, n \in M$.

Thus the known nontrivial (i. e. nonassociative and not of the form $U \times M$) minimal extensions of finite simple noncyclic Moufang loops are as follows:

- Moufang semidirect products $G \leftthreetimes V$ for a finite simple group G.
- Outer semidirect products $M \leftthreetimes U$ for a finite simple Paige–Moufang loop M and an irreducible factor space U of the corresponding Cayley algebra.
- Nonsplit central extensions $1 \to \mathbb{Z}_2 \to E \to M(q) \to 1$, where q is an odd prime power or $q = 2$, and $M(q)$ is the the simple Paige–Moufang loop over $\mathbb{F}_q$.

The extensions in the last case are isomorphic to the elements of norm 1 of the finite Cayley algebra $\mathbb{O}(q)$ if q is odd, and to the exceptional double cover of $M(2)$ of order 240 if $q = 2$. We put forward

Conjecture. *Up to isomorphism, the only nontrivial minimal extensions for finite simple noncyclic Moufang loops are those given in the list above.*

We also remark that the case where M is cyclic was treated in [2].

References

1. Liebeck M. W. The classification of finite simple Moufang loops // Math. Proc. Camb. Phil. Soc. 1987. V. 102. No. 1. P. 33–47.

2. Grishkov A. N., Zavarnitsine A. V. Abelian-by-cyclic Moufang loops // Comm. Alg. 2013. V. 41. No. 6. P. 2242–2253.

ON FREE LEFT n-DINILPOTENT DOPPELALGEBRAS

A.V. Zhuchok

Luhansk Taras Shevchenko National University
Gogol square, 1, Starobilsk 92703, Ukraine zhuchok_a@mail.ru

Recall that a doppelalgebra [1] is a nonempty set with two binary associative operations $\dashv$ and $\vdash$ satisfying the axioms $(x \dashv y) \vdash z = x \dashv (y \vdash z)$, $(x \vdash y) \dashv z = x \vdash (y \dashv z)$. As usual, $\mathbb{N}$ denotes the set of all positive integers.

Lemma. *In a doppelalgebra $(D, \dashv, \vdash)$ for any $n > 1, n \in \mathbb{N}$, and any $x_i \in D$, $1 \leq i \leq n+1$, and $*_j \in \{\dashv, \vdash\}$, $1 \leq j \leq n$, any parenthesizing of*

$$x_1 *_1 x_2 *_2 \ldots *_n x_{n+1}$$

gives the same element from D.

A doppelalgebra $(D, \dashv, \vdash)$ will be called left dinilpotent, if for some $n \in \mathbb{N}$ and any $x_1, ..., x_n$, $x \in D$ the following identities hold:

$$(x_1 *_1 ... *_{n-1} x_n) \dashv x = x_1 *_1 ... *_{n-1} x_n = (x_1 *_1 ... *_{n-1} x_n) \vdash x,$$

where $*_1, ..., *_{n-1} \in \{\dashv, \vdash\}$. The least such n we shall call the left dinilpotency index of $(D, \dashv, \vdash)$. For $k \in \mathbb{N}$ a left dinilpotent doppelalgebra of left dinilpotency index $\leq k$ is said to be left k-dinilpotent. The notion of a left dinilpotent doppelalgebra is an analog of the notion of a left nilpotent semigroup [2]. It is clear that operations of any left 1-dinilpotent doppelalgebra coincide and it is a left zero semigroup. The class of all left n-dinilpotent doppelalgebras forms a subvariety of the variety of doppelalgebras. A doppelalgebra which is free in the variety of left n-dinilpotent doppelalgebras will be called a free left n-dinilpotent doppelalgebra.

Let X be an arbitrary nonempty set and let ω be an arbitrary word in the alphabet X. The length of ω will be denoted by l_ω. Let further $F[X]$ be the free semigroup on X, T be the free monoid on the two-element set $\{a, b\}$ and $\theta \in T$ be an empty word. Fix $n \in \mathbb{N}$. If $l_w \geq n$ for $w \in F[X]$, by $\overrightarrow{w}^{n}$ denote the initial subword with the length n of w. By definition, the length l_θ of θ is equal to 0 and $\overrightarrow{u}^{0} = \theta$ for all $u \in T \backslash \{\theta\}$. Define operations $\dashv$ and $\vdash$ on

$$L_n = \{(w, u) \in F[X] \times T \mid l_w - l_u = 1,\, l_w \leq n\}$$

by

$$(w_1, u_1) \dashv (w_2, u_2) = \begin{cases} (w_1 w_2, u_1 a u_2), & l_{w_1} + l_{w_2} \leq n, \\ (\overrightarrow{w_1 w_2}^{n}, \overrightarrow{u_1 a u_2}^{n-1}), & l_{w_1} + l_{w_2} > n, \end{cases}$$

$$(w_1, u_1) \vdash (w_2, u_2) = \begin{cases} (w_1 w_2, u_1 b u_2), & l_{w_1} + l_{w_2} \leq n, \\ (\overrightarrow{w_1 w_2}^{n}, \overrightarrow{u_1 b u_2}^{n-1}), & l_{w_1} + l_{w_2} > n \end{cases}$$

for all $(w_1, u_1), (w_2, u_2) \in L_n$. The obtained algebra will be denoted by $FDDA_n^l(X)$.

Theorem. *$FDDA_n^l(X)$ is the free left n-dinilpotent doppelalgebra.*

We also consider separately free left n-dinilpotent doppelalgebras of rank 1 and characterize the least left n-dinilpotent congruence on a free doppelalgebra. In order to construct free right n-dinilpotent doppelalgebras and characterize the least right n-dinilpotent congruence on a free doppelalgebra we use the duality principle.

References

1. Pirashvili T. *Sets with two associative operations* // Cent. Eur. J. Math. 2003. No. 2. P. 169–183.

2. Schein B.M. *One-sided nilpotent semigroups* // Uspekhi Mat. Nauk. 1964. Vol. 19. No. 1. P. 187–189 (in Russian).

ON AUTOMORPHISMS OF THE ENDOMORPHISM SEMIGROUP OF A FREE ABELIAN DIMONOID

Yurii V. Zhuchok

Kyiv National Taras Shevchenko University
64 Volodymyrska str., 01601, Kyiv, Ukraine zhuchok_y@mail.ru

An algebra $(D, \dashv, \vdash)$ with two binary associative operations $\dashv$ and $\vdash$ is called a *dimonoid* [1] if for all $x, y, z \in D$ the following conditions hold:

$$(x \dashv y) \dashv z = x \dashv (y \vdash z), \quad (x \vdash y) \dashv z = x \vdash (y \dashv z), \quad (x \dashv y) \vdash z = x \vdash (y \vdash z).$$

A dimonoid $(D, \dashv, \vdash)$ will be called *abelian* (in the same as a digroup in [2]) if $x \dashv y = y \vdash x$ for all $x, y \in D$. For example, any left zero and right zero dimonoid is abelian. More general information on dimonoids and examples of different dimonoids can be found, e.g., in [1–3].

Let X be a nonempty set and $FCm(X)$ be the free commutative monoid on X with the unity ε. We put $FAd(X) = X \times FCm(X)$ and define two binary operations $\dashv$ and $\vdash$ on $FAd(X)$ by

$$(x,u) \dashv (y,v) = (x,uyv), \;\; (x,u) \vdash (y,v) = (y,xuv).$$

Theorem 1. *The algebra $\mathfrak{F}_X = (FAd(X), \dashv, \vdash)$ is the free abelian dimonoid of rank $|X|$.*

We denote by $\mathfrak{F}_n$ the free abelian dimonoid $\mathfrak{F}_X$ on an n-element set X.

Let $(S, \circ)$ be an arbitrary semigroup and $a \in S$. Define on S a new binary operation $\circ_a$ by $x \circ_a y = x \circ a \circ y$ for all $x, y \in S$. Clearly, $(S, \circ_a)$ is a semigroup, it is called a *variant* of $(S, \circ)$.

Corollary 1. *The free abelian dimonoid $\mathfrak{F}_1$ is isomorphic to the variant $(N^0, +_1)$ of the additive semigroup of all nonnegative integers.*

Proposition 1. *The endomorphism monoid $End(\mathfrak{F}_1)$ of the free abelian dimonoid $\mathfrak{F}_1$ is isomorphic to the semigroup $(N^0, \star)$, where $x \star y = x + y + x \cdot y$ for all $x, y \in N^0$.*

Denote by $\mathbb{P}$ the set of all prime numbers.

Proposition 2. *Let X be a singleton set, Y be an arbitrary set and $End(\mathfrak{F}_X) \cong End(\mathfrak{F}_Y)$. Then $|Y| = 1$ and the isomorphisms of $End(\mathfrak{F}_X)$ onto $End(\mathfrak{F}_Y)$ are in a natural one-to-one correspondence with permutations of $\mathbb{P}$.*

From here it follows that the automorphism group $Aut(End(\mathfrak{F}_1))$ of the endomorphism monoid $End(\mathfrak{F}_1)$ is isomorphic to the symmetric group $S(\mathbb{P})$ on a countably infinite set $\mathbb{P}$.

Theorem 2. *Let $(x, \varepsilon), (y, \omega) \in FAd(X)$, where $w = w_1^{\alpha_1} w_2^{\alpha_2} ... w_n^{\alpha_n} \neq \varepsilon$. Every isomorphism $End(\mathfrak{F}_X) \to End(\mathfrak{F}_Y)$ is induced by the isomorphism $\pi_\varphi : \mathfrak{F}_X \to \mathfrak{F}_Y$ such that*

$$(x,\varepsilon)\pi_\varphi = (x\varphi, \varepsilon), \;\; (y,\omega)\pi_\varphi = (y\varphi, (w_1\varphi)^{\alpha_1}(w_2\varphi)^{\alpha_2} \dots (w_n\varphi)^{\alpha_n}),$$

where $\varphi : X \to Y$ is a uniquely determined bijection.

Corollary 2. *For an arbitrary set X with $|X| \geq 2$, the automorphism group $Aut(End(\mathfrak{F}_X))$ is isomorphic to the symmetric group $S(X)$.*

We observe that the automorphism group of the endomorphism monoid of a free semigroup or a free monoid was described by Mashevitsky G. and Schein B.M. [4].

References

1. Loday J.-L. *Dialgebras* // in: *Dialgebras and related operads*. Lect. Notes Math., Springer-Verlag. 2001. V. 1763. P. 7–66.

2. Felipe R. *Generalized Loday algebras and digroups* // Comunicaciones del CIMAT. 2004. No. I-04-01/21-01-2004.

3. Zhuchok A.V. *Free dimonoids* // Ukr. Math. J. 2011. V. 63. No. 2. P. 196–208.

4. Mashevitsky G., Schein B.M. *Automorphism of the endomorphism semigroup of a free monoid or a free semigroup* // Proceedings of the AMS. 2003. V. 131. No. 6. P. 1655–1660.

ДИСКРЕТНАЯ МАТЕМАТИКА И МАТЕМАТИЧЕСКАЯ КИБЕРНЕТИКА

О ВЕРХНЕЙ ОЦЕНКЕ ЧИСЛА ДОПОЛНИТЕЛЬНЫХ ДУГ В МИНИМАЛЬНОМ РЕБЕРНОМ 1-РАСШИРЕНИИ ДИГРАФА

М.Б. Абросимов, О.В. Моденова

Саратовский государственный университет им. Н.Г.Чернышевского
Астраханская 83, 410012 Саратов, Россия {mic,oginiel}@rambler.ru

Определение 1. Граф $G^* = (V^*, \alpha^*)$ называется *реберным k-расширением* (k – натуральное) графа $G = (V, \alpha)$, если граф G вкладывается в каждый подграф графа G^*, получающийся удалением любых его k ребер.

Определение 1. Граф $G^* = (V^*, \alpha^*)$ называется *минимальным реберным k-расширением* n-вершинного графа $G = (V, \alpha)$, если выполняются следующие условия:

1) граф G^* является реберным k-расширением G;

2) граф G^* содержит n вершин, то есть $|V^*| = |V|$;

3) α^* имеет минимальную мощность среди всех графов, удовлетворяющих условиям 1) и 2).

Основные определения даются в соответствии с работами [1,2]. Построение минимального реберного k-расширения графа G можно представить как добавление к графу G минимально возможного числа новых ребер (дуг), так чтобы получившийся граф оказался реберным k-расширением. В данной работе мы будем рассматривать случай $k = 1$.

Обозначим число дополнительных ребер (дуг) в минимальном реберном 1-расширении через $ec(G)$. Число ребер (дуг) в графе G будем обозначать через $E(G)$.

Для неориентированных графов хорошей оценки числа дополнительных ребер в минимальном реберном 1-расширении неизвестно. Очевидно, что полный граф является реберным 1-расширением для любого отличного от него графа с тем же числом вершин. Это позволяет получить тривиальную оценку числа дополнительных ребер минимального реберного 1-расширения, однако она достигается только для графа, получающегося из полного удалением одного ребра. Для произвольных ориентированных графов хорошей оценки числа дополнительных ребер в минимальном реберном 1-расширении также неизвестно. Однако для направленных графов или диграфов такую оценку удалось получить, и она является достижимой.

Теорема. *Для произвольного диграфа G справедлива оценка:*

$$ec(G) \leq E(G). \tag{1}$$

Ранее в работе [2] был получен следующий результат, на котором достигается приведенная оценка.

Теорема. *Единственным с точностью до изоморфизма минимальным реберным 1-расширением n-вершинного турнира является полный n-вершинный граф без петель. При $k > 1$ n-вершинный турнир не имеет минимальных реберных k-расширений.*

Удалось найти еще семейства диграфов, для которых оценка является достижимой.

Теорема. *Гамильтонова ориентация цикла имеет единственное с точностью до изоморфизма минимальное реберное 1-расширение, которое получается добавлением для каждой дуги встречной.*

Заметим, что для произвольных графов оценка (1) не выполняется. Под *соединением* двух графов $G_1 = (V_1, \alpha_1)$ и $G_2 = (V_2, \alpha_2)$, не имеющих общих вершин, понимается граф

$$G_1 + G_2 = (V_1 \cup V_2, \alpha_1 \cup \alpha_2 \cup V_1 \times V_2 \cup V_2 \times V_1).$$

В работе [3] доказывается следующий результат относительно минимальных реберных k-расширений неориентированных графов вида $K_m + O_n$.

Теорема. *При $k \leq n/2$ граф $K_{m+2k} + O_{n-2k}$ является единственным с точностью до изоморфизма минимальным реберным k-расширением графа $K_m + O_n$. При $k > n/2$ граф $K_m + O_n$ не имеет минимальных реберных k-расширений.*

Граф $K_m + O_n$ содержит $\frac{m(m-1)}{2} + mn$ ребер. Определим число дополнительных ребер в его минимальном реберном 1-расширении: две вершины из части O_n соединяются ребром между собой и с оставшимися $n-2$ вершинами, получаем:

$$ec(K_m + O_n) = 2n - 3.$$

Можно найти значения m и n, при которых оценка (1) не будет выполняться: $m = 1$ и $n > 3$. При $m = 1$ граф $K_m + O_n$ оказывается звездой $K_{1,n} = K_1 + O_n$ и содержит n ребер. Таким образом, любая звезда $K_{1,n}$ при $n > 1$ имеет единственное с точностью до изоморфизма минимальное реберное 1-расширение, причем для него справедливо

$$ec(K_{1,n}) = 2E(K_{1,n}) - 3$$

и при $n > 3$

$$ec(K_{1,n}) > E(K_{1,n}).$$

Литература

1. Harary F., Hayes J. P. *Edge fault tolerance in graphs* // Networks. 1993. Vol. 23. P. 135–142.

2. Абросимов М. Б. *Графовые модели отказоустойчивости*. Саратов : Изд-во Сарат. ун-та, 2012.

3. Абросимов М. Б. *Минимальные реберные расширения некоторых предполных графов* // Прикладная дискретная математика. 2010. № 1. С. 105–117.

О РАСШИРЕНИЯХ СИЛЬНО РЕГУЛЯРНЫХ ГРАФОВ БЕЗ ТРЕУГОЛЬНИКОВ С СОБСТВЕННЫМ ЗНАЧЕНИЕМ 4

И.Н. Белоусов, А.А. Махнев

Институт математики им. Н.Н. Красовского УрО РАН, Ковалевской 16, 620990 Екатеринбург, Россия
i_belousov@mail.ru, makhnev@imm.uran.ru

Мы рассматриваем неориентированные графы без петель и кратных ребер. Для вершины a графа Γ через $\Gamma_i(a)$ обозначим i-окрестность вершины a, то есть, подграф, индуцированный Γ на множестве всех вершин, находящихся на расстоянии i от a. Подграф $\Gamma(a) = \Gamma_1(a)$ называется окрестностью вершины a и обозначается $[a]$, если граф Γ фиксирован.

Степенью вершины называется число вершин в ее окрестности. Граф Γ называется регулярным степени k, если степень любой вершины a из Γ равна k. Граф Γ назовем реберно регулярным с параметрами (v, k, λ), если он содержит v вершин, регулярен степени k, и каждое его ребро лежит в λ треугольниках. Граф Γ — вполне регулярный граф с параметрами (v, k, λ, μ), если он реберно регулярен с соответствующими параметрами, и $[a] \cap [b]$ содержит точно μ вершин для любых двух вершин a, b, находящихся на расстоянии 2 в Γ. Вполне регулярный граф называется сильно регулярным графом, если он имеет диаметр 2. Графом в половинном случае называется сильно регулярный граф с параметрами $(4\mu+1, 2\mu, \mu-1, \mu)$.

Если вершины u, w находятся на расстоянии i в Γ, то через $b_i(u,w)$ (через $c_i(u,w)$) обозначим число вершин в пересечении $\Gamma_{i+1}(u)$ ($\Gamma_{i-1}(u)$) с $[w]$. Граф Γ диаметра d называется дистанционно регулярным с массивом пересечений $\{b_0, b_1, \ldots, b_{d-1}; c_1, \ldots, c_d\}$, если значения $b_i(u,w)$ и $c_i(u,w)$ не зависят от выбора вершин u, w на расстоянии i в Γ для любого $i = 0, ..., d$. Графом Тэйлора называется дистанционно регулярный граф с массивом пересечений $\{k, \mu, 1; 1, \mu, k\}$.

Дж. Кулен предложил задачу изучения дистанционно регулярных графов, в которых окрестности вершин — сильно регулярные графы со вторым собственным значением, не большим t, для данного натурального числа t. В настоящее время задача Кулена полностью решена для $t = 3$.

В [1] начато решение задачи Кулена для $t = 4$. А именно получена редукция к окрестностям вершин, являющимся исключительными графами. Нетрудно доказать, что сильно регулярный граф без треугольников с неглавным собственным значением 4 имеет параметры $(352, 26, 0, 2)$, $(352, 36, 0, 4)$, $(392, 46, 0, 6)$, $(552, 76, 0, 12)$, $(667, 96, 0, 16)$ или $(784, 116, 0, 20)$.

В данной статье изучены графы, в которых окрестности вершин имеют вышеуказанные параметры, причем $v \geq 392$. Ранее, в [2] было доказано, что дистанционно регулярный граф, в котором окрестности вершин — сильно регулярные графы с параметрами $(352, 36, 0, 4)$, является сильно регулярным графом с параметрами $(9593, 352, 36, 12)$. Случай окрестностей с параметрами $(352, 26, 0, 2)$ является очень трудным (граница для диаметра имеет вид $d \leq 26$).

Теорема. *Граф, в котором окрестности вершин — сильно регулярные графы с параметрами* $(392, 46, 0, 6)$, $(552, 76, 0, 12)$, $(667, 96, 0, 16)$ *или* $(784, 116, 0, 20)$ *не является дистанционно регулярным.*

Работа выполнена при финансовой поддержке гранта РНФ (проект 14-11-00061).

Литература

1. Махнев А. А. *Сильно регулярные графы с неглавным собственным значением 4 и их расширения* // Известия Гомельского госуниверситета. 2014. Т. 84. №3. С. 84–85.

2. Махнев А. А., Нирова М. С. *О графах, в которых окрестности вершин – сильно регулярные графы с параметрами (352,36,0,4)* // Алгебра и приложения. Труды Межд. алгебр. конф. Нальчик. 2014 С. 84–85.

ПРОСТЫЕ НЕЦЕЛОЧИСЛЕННЫЕ ВЕРШИНЫ РЕЛАКСАЦИОННОГО МНОГОГРАННИКА ДЛЯ ЗАДАЧИ ЛИНЕЙНЫХ ПОРЯДКОВ И ОТСЕКАЮЩИЕ ФАСЕТЫ

Г.Г. Болоташвили

Институт кибернетики Грузинского технического университета,
ул. Сандро Еули 5, Тбилиси, Грузия
bolotashvili@yahoo.com

Построение многогранника NP-трудной задачи с помощью линейных неравенств, а потом использование их при решение задачи есть наша основная задача. Данная работа посвящена этой проблеме. Мы для нецелочисленной вершины релаксационного многогранника задачи линейных порядков находим смежные целочисленные вершины и с их помощью однозначно определяем фасеты.

Пусть имеем множества $N_n = \{1, 2, \ldots, n\}$. Если любому линейному порядку $i_1 i_2 ... i_n$ из множества элементов N_n сопоставим точку в $(n^2 - n)$-мерном пространстве следующим образом:

$$x_{i_s i_q} = \begin{cases} 1, & s < q, \\ 0, & s > q, \end{cases}$$

то задача линейных порядков как задача целочисленного линейного программирования имеет вид:

$$\sum_{i=1,i\neq j}^{n}\sum_{j=1}^{n} c_{ij}x_{ij} \to max$$

$$\dot{0} \leq x_{ij} \leq 1, x_{ij} + x_{ji} = 1, i \neq j, i, j = 1, ..., n; \quad (1)$$

$$\dot{0} \leq x_{ij} + x_{jk} - x_{ik} \leq 1, i \neq j, j \neq k, i \neq k, i, j, k = 1, ..., n; \quad (2)$$

$$x_{ij} \in \{0, 1\}, i \neq j, i, j = 1, ..., n.$$

Многогранник, соответствующий системе (1), (2) есть начальный релаксационный многогранник, который обозначим через B_n. Многогранник B_n имеет как целочисленные вершины взаимно однозначно соответствующие допустимым решениям, так и нецелочисленные вершины. Линейную выпуклую оболочку целочисленных вершин многогранника B_n, назовем многогранником линейных порядков и обозначим через P_n. Учитывая, систему равенств $x_{ij}+x_{ji} = 1, i \neq j, i, j = 1, \ldots, n$ многогранники B_n и P_n рассматриваются в $n(n-1)/2$-мерном пространстве.

Получены следующие результаты.

Теорема 1. *Точка* x^0, *имеющая следующие координаты* $x^0 = (x^0_{i_s i_q} = x^0_{j_s j_q} = 1/2, s \neq q, s, q = 1, ..., m;\ x^0_{i_s j_s} = x^0_{j_s i_s} = 1/2, s = 1, ..., m;\ x^0_{i_s j_q} = 0, x^0_{j_q i_s} = 1, s \neq q, s, q = 1, ..., m)$, *где* $I_m = \{i_1, ..., i_m\}$ *и* $J_m = \{j_1, ..., j_m\}$ — *непересекающиеся подмножества множества* $\{1, 2, \ldots, n\}$, $m \geq 3$, *является нецелочисленной вершиной многогранника* B_n.

Определение 1. Нецелочисленную вершину из теоремы 1 назовем простой нецелочисленной вершиной начального релаксационного многогранника B_n.

Теорема 2. *Простая нецелочисленная вершина* x^0 *многогранника* B_n *имеет только такие смежные целочисленные вершины, которые соответствуют следующим линейным порядкам:*

$$J^p A_p I^p,$$

где $p = 1, 2, ..., m-1$, J^p — *любой линейный порядок на множестве* $J_m - \{j_{s_1}, j_{s_2}, ..., j_{s_p}\}$;
A_p — *любой линейный порядок на множестве пар* $\{i_{s_1}j_{s_1}, i_{s_2}j_{s_2}, ..., i_{s_p}j_{s_p}\}$
I^p — *любой линейный порядок на множестве* $I_m - \{i_{s_1}, i_{s_2}, ..., i_{s_p}\}$.

Далее рассмотрим фасету многогранника линейных порядков из [1].

$$\dot{t}\sum_{s=1}^{m} x_{i_s j_s} - \sum_{s=1,s\neq q}^{m}\sum_{q=1}^{m} x_{i_s j_q} \leq t(t-1)/2, \quad (3)$$

где $\{i_1, ..., i_m\}$, $\{j_1, ..., j_m\}$ непересекающиеся подмножества множества $\{1, 2, \ldots, n\}$, $m \geq 3$, $1 \leq t \leq m-2$, сложение и вычитание индексов производится по mod m.

При $t = 1$ из неравенства (3) получаем первый класс фасет многогранника P_n, которые независимо друг от друга были получены в работах [2–4]. Их называют простыми фасетами.

Теорема 3. *Целочисленные вершины релаксационного многогранника* B_n *соответствующие линейным порядкам*

$$J^p A_p I^p,$$

где $p = t, t+1$, J^p — *любой линейный порядок на множестве* $J_m - \{j_{s_1}, j_{s_2}, ..., j_{s_p}\}$;
A_p — *любой линейный порядок на множестве пар* $\{i_{s_1}j_{s_1}, i_{s_2}j_{s_2}, ..., i_{s_p}j_{s_p}\}$
I^p — *любой линейный порядок на множестве* $I_m - \{i_{s_1}, i_{s_2}, ..., i_{s_p}\}$;
и только эти целочисленные вершины удовлетворяют неравенству (3) как равенству.

Определение 2. Если x^0 — нецелочисленная вершина многогранника B_n, имеющая смежные целочисленные вершины, которые однозначно определяют фасеты, то эти фасеты будем называть максимально отсекающими для нецелочисленной вершины x^0.

Теорема 4. *Пусть x^0 — простая нецелочисленная вершина многогранника B_n, тогда для x^0 фасеты (3) являются максимально отсекающими.*

Литература

1. Leung, J., Lee, J. *More facets from fances for linear ordering and acyclic sub graph polytopes* // Discr. Appl. Math. 1994. Vol. 50. P. 185-200.

2. Болоташвили Г. Г. *О гранях перестановочного многогранника.* // Сообщения АН Грузии. 1986. Т. 121, N 2. С. 281-284.

3. Cohen, M., Falmagne, J. C. *Random utility representation of binary choice probabilities: a new class of necessary conditions.* // J. Math. Psych. 1990. Vol. 34. P. 88-94.

4. Grotschel, M., Junger, M., Reinelt, G. *Facets of the linear ordering polytope* // Math. Program. 1985. Vol. 33. P. 43-60.

ОПТИМИЗАЦИЯ ДИНАМИЧЕСКИХ ЦЕН ГОСТИНИЦЫ

А.М. Бондоловский, М.Я. Ковалев

Объединенный институт проблем информатики НАН Беларуси, Сурганова 6, 220012 Минск, Беларусь
kovalyov_my@newman.bas-net.by, andrei.bandalouski@gmail.com

Рассматривается задача определения цен на гостиничные номера различных категорий на каждый день в заданном интервале времени в будущем с целью максимизации дохода. Предполагается, что спрос является эластичным, таким что его величина является линейно убывающей функцией от цены: $d_{\tau,c}(p_{\tau,c}) = a_{\tau,c} - b_c p_{\tau,c}$, где $d_{\tau,c}(p_{\tau,c})$ – величина спроса на номера категории c в день τ и $p_{\tau,c}$ – цена соответствующего номера.

В ОИПИ НАН Беларуси [1,2] создана экспериментальная система динамического ценообразования гостиницы. В докладе описывается оптимизационная компонента этой системы. На вход оптимизационной компоненты подаются:

t – идентификатор текущего дня;

J – количество типов номеров (1-местный, 2-местный и т.п.);

C – количество категорий номеров (категория определяется типом номера, сезоном, временем до заселения, продолжительностью проживания и т.п.);

$[t+1, t+T]$ – горизонт планирования;

$a_{\tau,c}$ – свободный коэффициент линейной функции спроса от цены для дня τ и категории c;

b_c – угловой коэффициент линейной функции спроса от цены для категории c. Предполагается, что он не зависит от дня для заданной категории номеров. Значения $a_{\tau,c}$ и b_c определяются прогнозной компонентой системы на основе исторических данных.

$L_{\tau,c}$ – нижняя граница цены $p_{\tau,c}$;

$U_{\tau,c}$ – верхняя граница цены $p_{\tau,c}$;

h_c – стоимость обслуживания номера категории c;

$R_{\tau,j}$ – количество номеров типа j, доступных в день τ;

M_j – множество категорий, включающих тип j комнаты. Предполагается, что множества M_j пронумерованы по неубыванию цен комнат.

Максимизация дохода гостиницы достигается за счет решения следующей задачи математического программирования с сепарабельной квадратичной вогнутой целевой функцией и линейными ограничениями.

$$\max \quad \sum_{c=1}^{C} \sum_{\tau=t+1}^{t+T} (a_{\tau,c} - b_c p_{\tau,c})(p_{\tau,c} - h_c) - W \sum_{c=1}^{C} \sum_{\tau=t+1}^{t+T} y_{\tau,c}, \tag{2}$$

при условиях

$$L_{\tau,c} \le p_{\tau,c},\ \tau = t+1,\dots,t+T,\ c = 1,\dots,C, \tag{3}$$

$$p_{\tau,c} \le U_{\tau,c} + y_{\tau,c},\ \tau = t+1,\dots,t+T,\ c = 1,\dots,C, \tag{4}$$

$$a_{\tau,c} \ge b_c p_{\tau,c},\ \tau = t+1,\dots,t+T,\ c = 1,\dots,C, \tag{5}$$

$$p_{\tau,c} \ge h_c,\ \tau = t+1,\dots,t+T,\ c = 1,\dots,C, \tag{6}$$

$$\sum_{c\in M_j} (a_{\tau,c} - b_c p_{\tau,c}) \le R_{\tau,j},\ \tau = t+1,\dots,t+T,\ j = 1,\dots,J, \tag{7}$$

$$p_{\tau,c_1} \le p_{\tau,c_2},\ c_1 \in M_1,\ c_2 \in M_2,\ \tau = t+1,\dots,t+T, \tag{8}$$

$$p_{\tau,c_2} \le p_{\tau,c_3},\ c_2 \in M_2,\ c_3 \in M_3,\ \tau = t+1,\dots,t+T, \tag{9}$$

$$p_{\tau,c_3} \le p_{\tau,c_4},\ c_3 \in M_3,\ c_4 \in M_4,\ \tau = t+1,\dots,t+T, \tag{10}$$

$$p_{\tau,c_4} \le p_{\tau,c_5},\ c_4 \in M_4,\ c_5 \in M_5,\ \tau = t+1,\dots,t+T, \tag{11}$$

$$p_{\tau,c} \ge 0,\ y_{\tau,c} \ge 0,\ \forall\ \tau,\ c. \tag{12}$$

Здесь

$y_{\tau,c}$ – вспомогательная переменная, позволяющая нарушить верхние границы цен в случае, когда не существует решения, допустимого относительно этих верхних границ;

W – достаточно большое число, превосходящее оптимальное значение в случае, когда верхние границы цен отсутствуют.

Целевая функция (2) представляет собой количество денег от продаж минус расходы на обслуживание номеров и минус стоимость нарушения верхних границ цен. Эти границы не будут нарушены в оптимальном решении, если существует решение, допустимое относительно верхних границ. Соотношения (3) и (4) отвечают за нижние и верхние границы цен. Значение переменной $y_{\tau,c}$ можно использовать для регулирования излишнего спроса без отказов со стороны гостиницы. Ограничения (5) гарантируют неотрицательность спроса. Соотношения (6) требуют, чтобы цена номера была больше либо равна стоимости его обслуживания. Ограничения (7) обеспечивают то, что суммарный спрос на номера одного типа в разных категориях в день τ не превосходит количества доступных номеров этого типа в этот день. Ограничения (8)–(11) обеспечивают иерархию цен на номера разных типов.

Задача (2)-(12) может быть декомпозирована на T подзадач, где каждая подзадача рассматривает один день τ, $\tau = t+1,\dots,t+T$. Оптимальное решение исходной задачи определяется оптимальными решениями подзадач.

Приведенная модель не допускает превышение вместимости гостиницы. Если спрос превышает вместимость, модель автоматически увеличит цены для снижения спроса до оптимального уровня. Зная оптимальные цены $p^*_{\tau,c}$, можно вычислить соотвествующий ожидаемый спрос $a_{\tau,c} - b_c p^*_{\tau,c}$, который можно использовать для оценки загруженности гостиницы и планирования соотвествующего обслуживания. Решение задачи (2)–(12) может быть проанализировано, одобрено или модифицировано менеджером. На основании решения можно применить следующие две политики бронирования номеров. Первая политика состоит в том, чтобы принимать все заявки по заданным ценам $p^*_{\tau,c}$, и преобразовывать цены после каждой заявки. Вторая политика состоит в том, чтобы принимать не более $a_{\tau,c} - b_c p^*_{\tau,c}$ заявок в каждой категории c. Эффективность второй политики существенно зависит от качества прогноза спроса. Независимо от политики бронирования, мы предлагаем преобразовывать цены после каждого бронирования, поскольку каждое бронирование уменьшает количество доступных номеров. Мы также предлагаем рассматривать несколько горизонтов планирования различной длины, например, 1, 7, 31, 90, 180 и 360 дней, и отыскивать решения для всех горизонтов планирования одновременно, поскольку точность прогноза уменьшается с увеличением длины горизонта планирования.

Научно-исследовательская работа выполнена при финансовой поддержке Белорусского республиканского фонда фундаментальных исследований по договору № Ф14М-005 от 23 мая 2014 года.

Литература

1. Бондоловский А. М. *Обзор моделей управления доходностью в гостиничном бизнесе* // Информатика. 2014. № 2. С. 66–83.

2. Bandalouski A., Egorova N. G., Kovalyov M. Y., Pesch E., Tarim S. A. *Multi-product dynamic pricing for hotel revenue management* // in submission.

ВЫРАЖЕНИЕ ЧИСЛА ПОМЕЧЕННЫХ СВЯЗНЫХ ГРАФОВ ЧЕРЕЗ ЧИСЛО ПОМЕЧЕННЫХ БЛОКОВ С ПОМОЩЬЮ МНОГОЧЛЕНОВ РАЗБИЕНИЙ

В.А. Воблый

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация
vitvobl@yandex.ru

Теорема. *Пусть C_n – число помеченных связных графов с n вершинами, B_n – число помеченных блоков с n вершинами, а $Y_k(x_1, ..., x_k)$ – многочлен разбиений. Тогда при $n \geq 1$ верна формула*

$$C_n = \frac{1}{n} Y_{n-1}(nB_2, ..., nB_n). \tag{1}$$

Доказательство. Введем производящую функцию: $B(z) = \sum\limits_{p=2}^{\infty} B_p \frac{z^p}{p!}$.

В работах [1] и [2] автором было получено соотношение

$$C_n = \frac{(n-1)!}{n} [z^{-1}] \exp(nB'(z)) z^{-n}, \tag{2}$$

где $[z^{-1}]$ – оператор формального вычета [3, С. 25].

Многочлены разбиений (многочлены Белла) $Y_n(x_1, ..., x_n)$ могут быть определены с помощью производящей функции [4, с. 174]

$$\exp\Big(\sum_{m=1}^{\infty} x_m \frac{t^m}{m!}\Big) = \sum_{n=0}^{\infty} Y_n(x_1, ..., x_n) \frac{t^n}{n!}\ , Y_0 = 1. \tag{3}$$

Для этих многочленов известна формула [4, с. 173]

$$Y_m(x_1, ..., x_m) = \sum_{\pi(m)} \frac{m!}{k_1! ... k_m!} \Big(\frac{x_1}{1!}\Big)^{k_1} ... \Big(\frac{x_m}{m!}\Big)^{k_m}\ ,$$

где суммирование проводится по всем разбиениям $\pi(m)$ числа m:

$k_1 + 2k_2 + ... + mk_m = m, k_i \geq 1, i = 1, ..., m$.

Подставляя в (2) выражение для $B'(z)$ с помощью (3) получим

$$C_n = \frac{(n-1)!}{n} [z^{-1}] \exp(n \sum_{p=2}^{\infty} B_p \frac{z^{p-1}}{(p-1)!}) z^{-n} = \frac{(n-1)!}{n} [z^{-1}] \exp(\sum_{m=1}^{\infty} nB_{m+1} \frac{z^m}{m!}) z^{-n} =$$

$$\frac{(n-1)!}{n} [z^{-1}] \sum_{p=0}^{\infty} Y_p(x_1, ..., x_p) \frac{z^{p-n}}{p!} = \frac{(n-1)!}{n} Y_{n-1}(x_1, ..., x_{n-1}) \frac{1}{(n-1)!} = \frac{1}{n} Y_{n-1}(nB_2, ..., nB_n).$$

Здесь $x_m = nB_{m+1}$. Доказательство закончено.

Следствие 1. *Пусть L_n – число помеченных связных графов без мостов с n вершинами, B_n – число помеченных блоков с n вершинами, а $Y_k(x_1, ..., x_k)$ – многочлен разбиений. Тогда при $n \geq 3$ верна формула*

$$L_n = \frac{1}{n} Y_{n-1}(0, nB_3, ..., nB_n).$$

Доказательство. Так как граф без мостов не имеет блоков, состоящих из одного ребра, то $B_2 = 0$ и из (1) получим утверждение следствия.

Следствие 2. *Пусть E_n – число помеченных эйлеровых графов с n вершинами, $\bar{B}_n$ – число помеченных эйлеровых блоков с n вершинами, а $Y_k(x_1, ..., x_k)$ – многочлен разбиений. Тогда при $n \geq 3$ верна формула*

$$E_n = \frac{1}{n} Y_{n-1}(0, n\bar{B}_3, ..., n\bar{B}_n).$$

Доказательство. Так как эйлеров граф является графом без мостов и, следовательно, не имеет блоков, состоящих из одного ребра, то $B_2 = 0$ и из (1) получим утверждение следствия.

Литература

1. Воблый В. А. *О перечислении помеченных связных графов по числу точек сочленения* // Дискретная математика. 2008. Т. 20. Вып. 1. С. 14–23.

2. Воблый В. А. *Об одной формуле для числа помеченных связных графов* // Дискретный анализ и исследование операций. 2012. Т. 19. №4. С. 48–59.

3. Гульден Я., Джексон Д. *Перечислительная комбинаторика.* М.: Наука, 1990.

4. Риордан Дж. *Комбинаторные тождества.* М., Наука, 1982.

О ЗАДАЧЕ ЦЕЛОЧИСЛЕННОГО ПРОГРАММИРОВАНИЯ С ОГРАНИЧЕННЫМИ МИНОРАМИ

Д.В. Грибанов[1], **С.И. Веселов**[2],

[1]Нижегородский Государственный Университет им. Лобачевского
просп. Гагарина 23, 603950 Нижний Новгород, Россия
Лаборатория ЛАТАС, Национальный Исследовательский Университет Высшая Школа Экономики
Родионова 136, 603093 Нижний Новгород, Россия dimitry.gribanov@gmail.com
[2]Нижегородский Государственный Университет им. Лобачевского
просп. Гагарина 23, 603950 Нижний Новгород, Россия veselov@vmk.unn.ru

Рассмотрим матрицу $A \in Z^{m \times n}$, пусть r её ранг. Пусть $P(A, b) = \{x \in \mathbb{R}^n : Ax \leq b\}$, где $b \in \mathbb{Z}^m$. Таким образом $P(A, b)$ есть полиэдр заданный системой с матрицей A. Обозначим за $\Delta(A)$ и $\delta(A)$ соответственно максимальное и минимальное абсолютные значения $r \times r$ миноров матрицы A. Обращаясь к работе [1], будем называть матрицу A *почти унимодулярной* если $\Delta(A) = 2$ и $\Delta_{r-1}(A) \leq 1$, где Δ_{r-1} есть максимальное абсолютное значение миноров порядка $(r-1) \times (r-1)$. В работе [2] *бимодулярными* матрицами названы такие матрицы A, у которых $\Delta(A) = 2$. Также в данной работе были получены результаты о полиэдрах заданных системами с бимодулярными матрицами ограничений. Например, задача проверки содержит ли такой полиэдр целую точку сводится к задаче определения телесности полиэдра, которая является полиномиально разрешимой.

В работе [3] даны определения *k-модулярной* и *k-регулярной* матриц, также описаны свойства данных матриц и полиэдров заданных системами с такими матрицами.

Определение 1 Матрица A называется k-модулярной, если для любой её базисной $(r \times r)$ подматрицы B верно $|det(B)| \in \{0, \pm k^i : i \in \mathbb{N}\}$.

Определение 2 Матрица A называется k-регулярной, если для любой её невырожденной квадратной подматрицы B верно, что kB^{-1} целочисленная матрица.

Шириной выпуклого тела P будем называть следующую величину:

$$w(P) = min_{c \in Z^n \setminus \{0\}} \{max_P c^\top x - min_P c^\top x\}.$$

Хинчиным [4] был установлен следующий факт: если P не содержит точек из Z^n, тогда $width(P) \leq f(n)$, где величина $f(n)$ зависит только от размерности. Существует много оценок на величину $f(n)$. Наилучшая оценка $O(n^{3/4} log^c(n))$ дана в работе [5]. Наилучшая оценка для симплексов $O(n\, log(n))$ дана в работе [6].

Результаты работы:

1) *Показано, что задача целочисленного программирования с почти унимодулярной матрицей ограничений полиномиально разрешима. К сожалению сложных примеров полиэдров заданных такими матрицами пока не было найдено.*

2) *Пусть $P = P(A, b)$ есть симплекс и $P \cap \mathbb{Z}^n = \emptyset$, тогда $w(P) < \delta(A) - 1$. Если же $w(P) \geq \delta(A) - 1$, то в P можно найти целую точку, используя полиномиальный алгоритм. Также в таком случае, для задачи целочисленной оптимизации применимы алгоритмы групповой минимизации предложенные Гомори и Ху [7,8], что приводит к временной сложности $O(n\delta(A))$. В данном результате существенно используются свойства* углового многогранника *[7,9]. Введением в изучение симплексов без целых точек могут послужить работы [10,11].*

3) *Пусть $P = P(A, b)$ есть политоп и $P \cap \mathbb{Z}^n = \emptyset$. Пусть также любой базисный минор матрицы A есть $\pm\Delta(A)$ или 0. Тогда $w(P) < (\Delta(A) - 1)(n + 1)$. В противном случае показано, что $|P \cap \mathbb{Z}^n| \geq n + 1$. Более того, данные $n + 1$ целых точек могут быть найдены за полиномиальное время. Доказательство опубликовано в сборнике [12].*

4) *Аналогичный результат получен для k-модулярной матрицы A. В данном случае, для выполнения неравенства $|P \cap \mathbb{Z}^n| \geq n + 1$ нужно, чтобы $w(P) \geq (\Delta(A) - 1)\dfrac{\Delta(A)}{\delta(A)}(n + 1)$. Похожий результат получен и для случая k-регулярной матрицы A.*

5) *Приведен пример конуса заданного* бимодулярной *матрицей ограничений и порожденного экспоненциальным числом образующих. Данный пример важен, потому что из противоположного утверждения о полиномиальности числа рёбер в любом* бимодулярном *конусе следовала бы полиномиальность задачи целочисленного программирования на политопе с бимодулярной матрицей ограничений.*

Работа выполнена при поддержке лаборатории алгоритмов и анализа сетевых структур НИУ ВШЭ, грант правительства РФ дог. 11.G34.31.0067 и при поддержке РФФИ, грант 15-01-06249.

Литература

1. Cornuéjols G., Zuluaga L.F. *On Padberg's conjecture about almost totally unimodular matrices* // Oper. Res. Lett. Vol. 2000. 27. No. 3. P. 97–99.

2. Veselov S.I., Chirkov A.J. *Integer program with bimodular matrix* // Discrete Optimization. 2009. Vol. 6. No. 2. P. 220–222.

3. Kotnyek Balázs. *A generalization of totally unimodular and network matrices.* PhD thesis. Published by ProQuest LLC, 2014.

4. Khinchine A. *A quantitative formulation of Kronecker's theory of approximation* // Izvestiya Akademii Nauk SSR Seriya Matematika. 1948. Vol. 12. P. 113–122 [in Russian].

5. Rudelson M. *Distances between non-symmetric convex bodies and the MM^*-estimate* // Positivity. 2000. Vol. 4. No. 2. P. 161–178.

6. Banaszczyk W., Litvak A.E., Pajor A., Szarek S.J. *The flatness theorem for non-symmetric convex bodies via the local theory of Banach spaces* // Mathematics of operations research. 1999. Vol. 24. No. 3. P. 728–750.

7. Gomory R.E. *On the Relation Between Integer and Non-Integer Solutions to Linear Programs* // Proc. Natl. Acad. Sci., USA. 1965. Vol. 53. No. 2. P. 260–265.

8. Hu T.C. *On the Asymptotic Integer Algorithm.* MRC Report 946, University of Wisconsin, Madison. 1968.

9. Shevchenko V.N. *Qualitative Topics in Integer Linear Programming.* Translations of Mathematical Monographs. AMS. 1996.

10. Haase C., Ziegler G. *On the Maximal Width of Empty Lattice Simplices* // Europ. J. Combinatorics. 2000. Vol. 21. P. 111–119.

11. Sebö A. *An Introduction to Empty Lattice Simplexes* // In: LNCS, eds.: Cornuéjols G., Burkard R.R., Woeginger R.E. Vol. 1610. 1999. P. 400–414.

12. Gribanov D. V. *The Flatness Theorem for Some Class of Polytopes and Searching an Integer Point* // Springer Proceedings in Mathematics & Statistics. Models, Algorithms and Technologies for Network Analysis. 2013. Vol. 104. P. 37–45.

МИНИМИЗАЦИЯ СИММЕТРИЧЕСКИХ БУЛЕВЫХ ФУНКЦИЙ В КЛАССЕ ПОЛИНОМОВ РИДА – МАЛЛЕРА

В.В. Дьяченко, В.П. Супрун

Белгосуниверситет, механико-математический факультет
пр-т Независимости 4, 220050 Минск, Беларусь
suprun@bsu.by

Под полиномом Рида-Маллера булевой функции $F = F(x_1, x_2, ..., x_n)$ понимается полином, в слагаемые которого одна часть переменных функции F входит только с отрицанием, а другая ее часть – только без отрицания. В частности, полином Жегалкина P(F) является положительно поляризованным полиномом Рида-Маллера функции F.

В общем случае булева функция $F = F(x_1, x_2, ..., x_n)$ имеет 2^n полиномов Рида-Маллера, которые отличаются друг от друга поляризацией переменных, числом слагаемых и числом вхождений переменных в слагаемые полиномов.

Если булева функция $F = F(x_1, x_2, ..., x_n)$ является симметрической, то такая функция имеет $n+1$ различных полиномов Рида-Маллера $P_0(F)$, $P_1(F)$, ... , $P_n(F)$, где полином $P_k(F)$ содержит ровно k переменных с отрицанием и $0 \leq k \leq n$. Здесь $P_0(F)$ - полином Жегалкина $P(F)$ и $P_n(F)$ - отрицательно поляризованный полином Рида-Маллера функции F, который обозначается как $Q(F)$.

Метод построения монотонно поляризованных полиномов $P(F)$ и $Q(F)$ для симметрических булевых функций $F = F(x_1, x_2, ..., x_n)$ (метод треугольника) описан в работе [1], а метод разложения симметрических булевых функций n переменных в полиномы Рида-Маллера с произвольной поляризацией переменных приводится в [2].

Под сложностью полинома $P_k(F)$ обычно понимается число $l_1(P_k)$ слагаемых (элементарных конъюнкций) или число $l_2(P_k)$ вхождений переменных x_1,x_2, ... ,x_n в слагаемые полинома $P_k(F)$.

По аналогии с теорией ДНФ под кратчайшим полиномом Рида-Маллера $P_{short}(F)$ булевой функции F будем понимать полином с минимальным значением l_1 среди всех полиномов $P_0(F)$, $P_1(F)$, ... , $P_n(F)$, а под минимальным полиномом $P_{min}(F)$ – полином с минимальным значением l_1 среди полиномов $P_0(F)$, $P_1(F)$, ... , $P_n(F)$.

Следует отметить, что до последнего времени под минимальным полиномом Рида-Маллера булевой функции F понимался кратчайший полином Рида-Маллера, что совершенно не соответствует общепринятому определению кратчайшей и минимальной ДНФ булевых функций.

Пусть $F = F(x_1, x_2, ..., x_n)$ — произвольная симметрическая булева функция n переменных и $P_0(F)$, $P_1(F)$, ... , $P_n(F)$ - всевозможные полиномы Рида-Маллера функции F. Каждый

из $n+1$ полиномов имеет сложность $l_1(P_0)$, $l_1(P_1)$, ... , $l_1(P_n)$. Тогда под сложностью $l_1(F)$ функции F понимается $l_1(F) = \min\limits_{0\le k\le n} l_1(P_k)$. Очевидно, что здесь $l_1(F)$ — число слагаемых полинома $P_{short}(F)$. Функция Шеннона $L_1(n)$ для оценки сложности (по числу слагаемых) симметрических булевых функций n переменных определяется, как $L_1(n) = \max l_1(F)$, где максимум берется по всем $2^{(n+1)}$ симметрическим булевым функциям n переменным.

В 1995 году было установлено [3], что $L_1(n) = [\frac{2^{n+1}}{3}]$. Отметим, что данная оценка функции Шеннона справедлива как для симметрических, так и для произвольных булевых функций n переменных.

Введем в рассмотрение функцию Шеннона $L_2(n)$ для оценки сложности симметрических булевых функций $F = F(x_1, x_2, ..., x_n)$ по числу вхождений переменных в слагаемые полиномов Рида-Маллера.

Пусть $F = F(x_1, x_2, ..., x_n)$ — произвольная симметрическая булева функция n переменных и $P_0(F)$, $P_1(F)$, ... , $P_n(F)$ - всевозможные полиномы Рида-Маллера функции F, каждый из которых имеет сложность (по числу вхождений переменных в слагаемые полиномов) $l_1(P_0)$, $l_1(P_1)$, ... , $l_1(P_n)$. Тогда $l_2(F) = \min\limits_{0\le k\le n} l_2(P_k)$ и $L_2(n) = \max l_2(F)$, где максимум берется по всем симметрическим булевым функциям n переменным.

Для вычисления значений $L_2(n)$ при условии, что $2 \le n \le 14$, была написана программа на языке C++ в среде разработки Borland Builder 6 для ОС семейства Windows, которая реализует приведенный в работе [2] метод построения полиномов $P_k(F)$ симметрических булевых функций $F = F(x_1, x_2, ..., x_n)$. Работа программы основана на переборе всевозможных полиномов Рида-Маллера всех $2^{(n+1)}$ симметрических булевых функций n переменных. Результаты опытной эксплуатации программы представлены посредством таблицы, в которой приведены также локальные коды $\pi(F)$ симметрических булевых функций F, на которых было достигнуто значение функции Шеннона $L_2(n)$.

n	$L_2(n)$	$\pi(F)$	k
2	2	010	0
3	7	0110	1
4	20	00100	2
5	52	010010	2
6	126	0010010	0
7	295	01001001	1
8	680	001001001	0
9	1531	0110110110	1
10	3410	00100100100	2
11	7504	010010010010	2
12	16380	0010010010010	0
13	35491	01001001001001	1
14	76454	001001001001001	0

К настоящему времени пока не удалось вывести аналитическую зависимость значения функции Шеннона $L_2(n)$ от числа переменных n симметрических булевых функций. Однако научные исследования в этом направлении продолжаются.

Литература

1. Супрун В. П. *Полиномиальное разложение симметрических булевых функций* // Известия АН СССР. Техническая кибернетика. 1985. № 4. С. 123 — 127.

2. Suprun V. P. *Fixed Polarity Reed-Muller Expressions of Symmetric Booleans Functions* // Proc. IFIP WG 10.5 Workshop on Applications of the Reed-Muller Expansion in Circuit Design (Reed-Muller'95). 27–29 August 1995. Makuhari, Chiba, Japan. P. 246 – 249.

3. Перязев Н. А. *Сложность булевых функций в классе полиномиальных поляризованных форм* // Алгебра и логика. 1995. Т. 34. № 3 С. 323 — 326.

ПОСТОПТИМАЛЬНЫЙ АНАЛИЗ ЗАДАЧИ ОТЫСКАНИЯ ПОДМНОЖЕСТВА ВЕКТОРОВ

В.А. Емеличев, К.Г. Кузьмин

Белгосуниверситет, механико-математический факультет
пр-т Независимости 4, 220030 Минск, Беларусь
vemelichev@gmail.com, kuzminkg@mail.ru

Пусть задано конечное семейство векторов $\{v_1, v_2, \ldots, v_n\}$ действительного пространства $\mathbf{R}^k$ и натуральное число $m < n$. Из этого семейства требуется выбрать m векторов, евклидова норма суммы которых максимальна. Такая задача возникает (см., например, [1,2]) при нахождении фиксированного числа участков в числовой последовательности, образованной квазипериодически повторяющимся фрагментом при заданном числе повторов. Подобная ситуация типична для ряда таких приложений как радиолокация, телекоммуникация, обработка речевых сигналов, электронная разведка и др. [3]. В силу природы этих задач исходные данные – компоненты векторов – неизбежно задаются с некоторой погрешностью. В таких условиях желательно не только уметь находить оптимальные решения, но и проводить для каждого из них постоптимальный анализ, чтобы получить необходимую информацию о предельном уровне изменений в пространстве параметров, сохраняющих оптимальность выбранного решения. Числовая характеристика, определяющая указанный предельный уровень, обычно [4] называется радиусом устойчивости решения. Для того чтобы дать строгое определение радиуса устойчивости и указать его верхнюю достижимую оценку, введем ряд обозначений.

Пусть из векторов $v_1, v_2, \ldots, v_n$ как из столбцов образована матрица $V = [v_{ij}] \in \mathbf{R}^{k\times n}$. Строки матрицы V будем обозначать V_i, $i \in N_k := \{1, 2, \ldots, k\}$. И пусть $X \subset \{0, 1\}^n$ – множество всех булевых векторов $x = (x_1, x_2, \ldots, x_n)^T$, каждый из которых содержит ровно m единиц. Тогда задача $Z(V)$ поиска подмножества векторов имеет вид:

$$\|Vx\|_2 \to \max_{x\in X},$$

где $\|\cdot\|_2$ – евклидова норма в пространстве $\mathbf{R}^k$. Множество оптимальных (максимальных) решений задачи $Z(V)$ будем обозначать через $Opt(V)$.

Возмущение компонент векторов из множества $\{v_1, v_2, \ldots, v_n\}$ будем моделировать, прибавляя к исходной матрице V возмущающую матрицу $V' = [v'_{ij}] \in \mathbf{R}^{k\times n}$. Тем самым, возмущенная задача записывается в виде $Z(V + V')$, а множество ее оптимальных решений имеет вид $Opt(V + V')$.

Пусть $x^0 \in Opt(V)$. По аналогии с [4] радиусом устойчивости решения x^0 назовем число

$$\rho(x^0, V) = \begin{cases} \sup \Xi, & \text{если } \Xi \neq \emptyset, \\ 0, & \text{если } \Xi = \emptyset, \end{cases}$$

где

$$\Xi = \{\varepsilon > 0 : \ \forall V' \in \Omega(\varepsilon)\ (x^0 \in Opt(V + V'))\},$$

$$\Omega(\varepsilon) = \{V' \in \mathbf{R}^{k\times n} : \|V'\|_1 < \varepsilon\},$$

$$\|V'\|_1 = \sum_{i\in N_k}\sum_{j\in N_n} |v'_{ij}|.$$

Теорема. *Для радиуса устойчивости $\rho(x^0, V)$ оптимального решения x^0 задачи $Z(V)$ верна следующая достижимая оценка:*

$$\rho(x^0, V) \le \min_{x\in X\setminus\{x^0\}} \left(\sqrt{\sum_{i\in N_k} (V_i x^0)^2 + \max_{i\in N_k}(V_i x)^2 - \sum_{i\in N_k} (V_i x)^2} - \max_{i\in N_k} |V_i x| \right).$$

В частности, эта оценка достижима для тех задач $Z(V)$, в которых каждый вектор $x \in X \setminus \{x^0\}$ подчинен неравенству

$$\max_{i\in N_k} |V_i x| \ge \max_{i\in N_k} |V_i x^0|.$$

Работа выполнена при финансовой поддержке БРФФИ, проект № Ф13К-078.

Литература

1. Бабурин А. Е., Гимади Э. Х., Глебов Н. И., Пяткин А. В. *Задача отыскания подмножества векторов с максимальным суммарным весом* // Дискр. анализ и исслед. операций. 2007. Сер. 2. Т. 14. № 1. С. 32–42.

2. Гимади Э. Х., Глазков Ю. В., Рыков И. А. *О двух задачах выбора подмножества векторов с целочисленными координатами с максимальной нормой суммы в евклидовом пространстве* // Дискр. анализ и исслед. операций. 2008. Т. 15. № 4. С. 30–43.

3. Гимади Э. Х., Кельманов А. В., Кельманова М. А., Хамидуллин С. А. *Апостериорное обнаружение в числовой последовательности квазипериодически повторяющегося фрагмента при заданном числе повторов* // Сиб. журн. индустриальной математики. 2006. Т. 9. № 1(25). С. 55–74.

4. Emelichev V., Podkopaev D. *Quantitative stability analysis for vector problems of* 0-1 *programming* // Discrete Optimization. 2010. V. 7. N 1-2. P. 48–63.

О РАДИУСЕ УСТОЙЧИВОСТИ МНОГОКРИТЕРИАЛЬНОЙ ИНВЕСТИЦИОННОЙ ЗАДАЧИ С НОРМАМИ ГЕЛЬДЕРА В ПРОСТРАНСТВАХ ПАРАМЕТРОВ

В.А. Емеличев, В.И. Мычков

Белгосуниверситет, механико-математический факультет
пр-т Независимости 4, 220030 Минск, Беларусь
vemelichev@gmail.com, vadim.mychkov@gmail.com

Рассматривается s-критериальная дискретная инвестиционная задача с критериями крайнего оптимизма

$$Z^s(E): \quad f_k(x, e_k) = \max_{i\in N_m} e_{ik}x = \max_{i\in N_m} \sum_{j\in N_n} e_{ijk}x_j \to \max_{x\in X}, \quad k \in N_s,$$

состоящая в поиске множества Парето $P^s(E)$, т.е. множества Парето-оптимальных портфелей.

Здесь $N_m = \{1, 2, \ldots, m\}$; e_{ik} – i-я строка k-го сечения $e_k \in \mathbf{R}^{m\times n}$ трехиндексной матрицы $E = [e_{ijk}] \in \mathbf{R}^{m\times n\times s}$; e_{ijk} – оценка экономической эффективности вида $k \in N_s$ инвестиционного проекта с номером $j \in N_n$ в случае, когда рынок находится в состоянии $i \in N_m$; $x_j = 1$, если j-й проект реализуется, и $x_j = 0$ – в противном случае; $X \subset \mathbf{E}^n$ – множество всех допустимых инвестиционных портфелей $x = (x_1, x_2, \ldots, x_n)^T$.

Для любых чисел $p, q, r \in [1, \infty]$ в пространствах состояний рынка $\mathbf{R}^m$ и проектов $\mathbf{R}^n$, а так же в критериальном пространстве эффективности $\mathbf{R}^s$ зададим соответственно нормы Гельдера l_p, l_q и l_r, т.е. под нормой матрицы $E \in \mathbf{R}^{m\times n\times s}$ будем понимать число

$$\|E\| = \|(\|e_1\|_{qp}, \|e_2\|_{qp}, \ldots, \|e_s\|_{qp})\|_r\,,$$

где

$$\|e_k\|_{qp} = \|(\|e_{1k}\|_q, \|e_{2k}\|_q, \ldots, \|e_{mk}\|_q)\|_p, \quad k \in N_s.$$

Радиусом устойчивости $\rho^s(p, q, r)$ задачи $Z^s(E)$, как обычно [1–3], назовем число

$$\rho^s(p, q, r) = \begin{cases} \sup \Xi, & \text{если } \Xi \neq \emptyset, \\ 0, & \text{если } \Xi = \emptyset, \end{cases}$$

где

$$\Xi = \{\varepsilon > 0 : \forall E' \in \Omega(\varepsilon)\ (P^s(E + E') \subseteq P^s(E))\},$$
$$\Omega(\varepsilon) = \{E' \in \mathbf{R}^{m\times n\times s} : \|E'\| < \varepsilon\}.$$

Теорема. *При $X \neq P^s(E)$ и любых $p, q, r \in [1, \infty]$ справедливы следующие оценки радиуса устойчивости $\rho^s(p, q, r)$ задачи $Z^s(E)$:*

$$\varphi \leq \rho^s(p, q, r) \leq m^{1/p} n^{1/q} s^{1/r} \psi,$$

где

$$\varphi = \min_{x\notin P^s(E)} \max_{x'\in P(x,E)} \frac{\gamma(x', x)}{\|(\|x'\|_{q'}, \|x\|_{q'})\|_u},$$

$$\psi = \min_{x\notin P^s(E)} \max_{x'\in P(x,E)} \frac{\gamma(x', x)}{\|x' - x\|_1},$$

$$\gamma(x', x) = \min\{f_k(x', e_k) - f_k(x, e_k) :\ k \in N_s\},$$

$$P(x, E) = \{x' \in P^s(E) : f(x', E) \geq f(x, E)\ \ \&\ \ f(x', E) \neq f(x, E)\},$$

$$f(x, E) = (f_1(x, e_1), f_2(x, e_2), \ldots, f_s(x, e_s)),$$

$$u = \min\{p', q'\},\ 1/p + 1/p' = 1,\ 1/q + 1/q' = 1.$$

Следствие 1 [1]. *При любом $p \in [1, \infty]$ верны неравенства*

$$\min_{x\notin P^s(E)} \max_{x'\in P(x,E)} \frac{\gamma(x', x)}{\|x'\|_{p'} + \|x\|_{p'}} \leq \rho^s(\infty, p, p) \leq (ns)^{1/p} \min_{x\notin P^s(E)} \max_{x'\in P(x,E)} \frac{\gamma(x', x)}{\|x' - x\|_1}.$$

Следствие 2 [2]. *При любом $p \in [1, \infty]$ верны неравенства*

$$\min_{x\notin P^s(E)} \max_{x'\in P(x,E)} \frac{\gamma(x', x)}{\|x' + x\|_1} \leq \rho^s(p, \infty, p) \leq (ms)^{1/p} \min_{x\notin P^s(E)} \max_{x'\in P(x,E)} \frac{\gamma(x', x)}{\|x' - x\|_1}.$$

Следствие 3 [3]. *При любом $p \in [1, \infty]$ верны неравенства*

$$\min_{x\notin P^s(E)} \max_{x'\in P(x,E)} \frac{\gamma(x', x)}{\|x'\|_{p'} + \|x\|_{p'}} \leq \rho^s(\infty, p, \infty) \leq n^{1/p} \min_{x\notin P^s(E)} \max_{x'\in P(x,E)} \frac{\gamma(x', x)}{\|x' - x\|_1}.$$

Работа выполнена при частичной финансовой поддержке БРФФИ, проект № Ф13К-078.

Литература

1. Бухтояров С. Е., Емеличев В. А. *О мере устойчивости решений векторного варианта одной инвестиционной задачи* // Дискр. анализ и исслед. операций. 2015. Т. 22. № 2. С. 5–16.

2. Емеличев В. А., Устилко Е. В. *Постоптимальный анализ инвестиционной задачи с критериями крайнего оптимизма* // Прикладная дискретная математика. 2014. № 3. С. 117–123.

3. Бухтояров С. Е., Емеличев В. А. *Устойчивость инвестиционной задачи Марковица с критериями крайнего оптимизма* // Весці НАН Беларусі. Сер. фіз.-мат. навук. 2014. № 3. С. 44–48.

ОПТИМИЗАЦИОННЫЕ ЗАДАЧИ НА МНОЖЕСТВЕ РАЗМЕЩЕНИЙ

О.А. Емец[1], **Т.Н. Барболина**[2]

[1]Полтавский университет экономики и торговли, Коваля 3, 36014 Полтава, Украина
yemetsli@ukr.net
[2]Полтавский национальный педуниверситет, Остроградского 2, 36003, Полтава, Украина
tm-b@ukr.net

При решении проблем в различных отраслях науки и техники важную роль играют оптимизационные задачи комбинаторного типа и методы их решения. Актуальным направлением исследований в области комбинаторной оптимизации являются методы и алгоритмы евклидовой комбинаторной оптимизации. Задачи в этой области классифицируют как по виду целевой функции и дополнительных ограничений, так и в соответствии с евклидовым комбинаторным множеством, которое определяет комбинаторное ограничение. Таким образом выделяют оптимизационные задачи на перестановках, сочетаниях, полиперестановках и т.д. В данном докладе рассматривается решение оптимизационных задач на общем множестве размещений.

Пусть $G = \{g_1, \dots, g_\eta\}$ – некоторое мультимножество, то есь совокупность элементов, среди которых могут быть и одинаковые, $E^k_\eta(G)$ – общее множество k-размещений (т.е. множество всех упорядоченных k-выборок) из мультимножества G. Если $k = \eta$, $E^k_\eta(G)$ является общим множеством перестановок (обозначается $E_k(G)$). Обозначим также $J_n = \{1, 2, \dots n\}$ — множество n первых натуральных чисел.

В работах [1–3] изучены свойства допустимой области оптимизационных задач на размещениях, особенности решения безусловных задач комбинаторной оптимизации на размещениях. В частности, установлено, достаточное условие того, что точка является решением линейной безусловной задачи минимизации на размещениях, т.е. задачи поиска пары $< L(x^*), x^* >$ такой, что

$$L(x^*) = \min_{x \in E^k_\eta(G)} \sum_{j=1}^{k} c_j x_j,\ x^* = arg \min_{x \in E^k_\eta(G)} \sum_{j=1}^{k} c_j x_j. \tag{1}$$

Исследование свойств безусловных задач на размещених было продолжено в [4], где было установлено также достаточное условие решения.

Теорема 1. *Пусть элементы мультимножества в задаче (1) удовлетворяют условию*

$$0 \le g_1 \le \dots \le g_\eta, \tag{2}$$

а коэффициенты целевой функции — условию

$$c_{q_1} = \dots = c_{q_2 - 1} > c_{q_2} = \dots = c_{q_3 - 1} > \dots > c_{q_s} = \dots = c_k,$$

причем r – наибольший индекс такой, что $c_{q_r} > 0$, а t – наименьший индекс такой, что $c_{q_t} < 0$. Точка x^* является минималью в задаче (1) тогда и только тогда, когда она удовлетворяет условиям

$\left(x^*_{q_w}, ..., x^*_{q_{w+1}-1}\right) \in E_{m_w}(G^w)\ \forall w \in J_r, G^w = \left\{g_{q_w}, ..., g_{q_{w+1}-1}\right\},\ m_w = |G^w|$

$\left(x^*_{q_w}, ..., x^*_{q_{w+1}-1}\right) \in E_{\bar{m}_w}(\bar{G}^w)\ \forall w \in J_k \setminus J_{t-1},\ \bar{G}^w = \left\{g_{\eta-k+q_w}, ..., g_{\eta-k+q_{w+1}-1}\right\},\ \bar{m}_w = |G^w|.$

В работах [5–8] исследовалось решение линейных условных задач оптимизации на размещених. Предложены методы на разных идейных основаниях. Методы отсечения [5–7] используют идейную близость задач комбинаторной и дискретной оптимизации. Другой подход состоит в использовании разбиения многогранника на классы эквивалентности с последующим направленным перебором полученных классов [8]. Этот подход был распространен также на решение оптимизационных задач с дробно-линейной целевой функцией [9].

Актуальным направлением исследованием в области оптимизации является рассмотрение задач с различными видами неопределенности, в том числе стохастической. Один из возможных подходов к постановкам оптимизационных задач на размещениях с вероятностной неопределенностью предложены в [10], [11]. Этот подход основывается на введении отношения линейного порядка на множестве случайных величин или на фактор-множестве по некоторому отношению эквивалентности.

В рамках такого подхода к постановкам оптимизационных задач исследуются свойства линейных безусловных задач на размещениях, возможность применения метода ветвей и границ для решения линейных задач с дополнительными ограничениями.

Рассмотрение оптимизационных задач в условиях неполной информации позволит осуществлять построение адекватных моделей для большего числа практически значимых задач.

Литература

1. Стоян Ю.Г., Ємець О.О. *Теорія і методи евклідової комбінаторної оптимізації.* Київ: Інститут системних досліджень освіти, 1993.

2. Emets' O.O., Roskladka O.V., Nedobachii S.I. *Irreducible System of Constraints for a General Polyhedron of Arrangements* // Ukrainian Mathematical Journal. 2003. Vol. 55. Iss. 1. P. 1–12.

3. Ємець О.О., Черненко О.О. *Оптимізація дробово-лінійної функції на розміщеннях: властивості допустимої області* // Наукові вісті НТУУ "КПІ". 2006. № 5. С. 22–29.

4. Барболіна Т.М. *Властивості лінійних безумовних задач оптимізації на розміщеннях* // Збірник наукових праць викладачів, аспірантів, магістрантів і студентів фізико-математичного факультету. Полтава: Астрая, 2015.

5. Емец О.А., Барболина Т.Н. *Комбинаторная оптимизация на размещениях.* К.: Наук. думка, 2008.

6. Емец О.А., Барболина Т.Н. *Решение линейных задач оптимизации на размещениях методом отсечения* // Кибернетика и системный анализ. 2003. № 6. С. 131–141.

7. Барболина Т.Н., Емец О.А. *Полностью целочисленный метод отсечения для решения линейных условных задач оптимизации на размещениях* // Журнал вычислительной математики и математической физики. 2005. Т. 45. № 2. С. 254–261.

8. Емец О.А., Барболина Т.Н. *Решение задач евклидовой комбинаторной оптимизации методом построения лексикографической эквивалентности* // Кибернетика и системный анализ. 2004. № 5. С. 115–125.

9. Емец О. А., Барболина Т.Н., Черненко О.А. *Решение задач оптимизации с дробно-линейными целевыми функциями и дополнительными ограничениями на размещениях* // Кибернетика и системный анализ. 2006. № 5. С. 79–85.

10. Емец О.А., Барболина Т.Н. *Об оптимизационных задачах с вероятностной неопределенностью* // Доповіді Національної академії наук України. 2014. № 11. С. 40–45.

11. Емец О.А., Барболина Т.Н. *Линейные порядке на множестве дискретных случайных величин: использование в комбинаторной оптимизации* // Дискретные модели в теории управляющих систем : IX Международная конференция, Москва и Подмосковье, 20-22 мая 2015 г. : труды – М.: МАКС Пресс, 2015. С. 76–79.

РАЗРЕШАЮЩИЕ МНОЖЕСТВА 2-ПОРОГОВЫХ ФУНКЦИЙ

Е.М. Замараева

Нижегородский Государственный Университет им. Н.И.Лобачевского
пр. Гагарина, 23, 603950, г. Нижний Новгород, Россия elena.zamaraeva@gmail.com

Пусть $E_n^d = \{0, 1, \ldots, n-1\}^d$, $n \geq 2$ и $d \geq 1$. Функция $f : E_n^d \to \{0, 1\}$ называется *k-пороговой* для натурального k, если существуют действительные числа $a_{10}, a_{11}, \ldots, a_{kd}$ такие, что

$$M_1(f) = \left\{ x \in E_n^d : \sum_{j=1}^{d} a_{ij} x_j \leq a_{i0}, \text{ для } i = 1, \ldots, k \right\},$$

где $M_\nu(f) = \{x \in E_n^d : f(x) = \nu\}$. Неравенства $\sum\limits_{j=1}^{d} a_{ij} x_j \leq a_{i0}$ для $i = 1, \ldots, k$ называются *пороговыми* или *определяющими* k-пороговую функцию f.

Обозначим через $\mathfrak{T}(d, n, k)$ класс k-пороговых функций над E_n^d.

Для любой k-пороговой функции f существуют пороговые функции $f_1, \ldots, f_k$ такие, что

$$f(x) = f_1(x) \& \ldots \& f_k(x).$$

Будем говорить, что f *определяется* функциями $f_1, \ldots, f_k$ и $\{f_1, \ldots, f_k\}$ – *определяющее множество* f.

Выпуклую оболочку множества точек $X \subseteq \mathbb{R}^d$ обозначим через $\mathrm{Conv}(X)$. Для функции $f : E_n^d \to \{0, 1\}$ обозначим $P(f) = \mathrm{Conv}(M_1(f))$. Обозначим через $\mathcal{S}(P)$ и $\mathrm{Diam}(P)$ площадь и диаметр выпуклого многоугольника P соответственно.

Пусть $\mathcal{C}$ – класс $\{0, 1\}$-значных функций над E_n^d и $f \in \mathcal{C}$. *Разрешающим множеством* функции f относительно класса $\mathcal{C}$ называется множество $T \subseteq E_n^d$ такое, что никакая другая функция из $\mathcal{C}$ не совпадает с f на всем T. Разрешающее множество T называется *тупиковым*, если никакое его собственное подмножество не является разрешающим для f. Обозначим через $\sigma(f, \mathcal{C})$ минимальную мощность разрешающего множества f относительно $\mathcal{C}$.

Обозначим также

$$B(E_n^2) = \{x \in E_n^2 : x_1 = 0 \vee x_2 = 0 \vee x_1 = n-1 \vee x_2 = n-1\}.$$

Пусть $\mathfrak{A}_i(f)$ для $i = 1, 2$ – множество всех множеств из i пороговых неравенств, определяющих f и таких, что прямые, соответствующие коэффициентам пороговых неравенств, пересекаются внутри E_n^2, если $i = 2$. Рассмотрим многоугольник, образованный пересечением $\mathrm{Conv}(E_n^2)$ с полупространствами, заданными неравенствами из некоторого множества $A \in \mathfrak{A}_i$. Через $a_1(A)$ обозначим лексикографически наименьшую вершину многоугольника, смежную с первой пороговой прямой и границей E_n^2, а через $a_2(A)$ – лексикографически наибольшую вершину многоугольника, смежную со второй пороговой прямой и границей E_n^2. Через $o(A)$ обозначим точку пересечения прямых, соответствующих пороговым неравенствам, если $A \in \mathfrak{A}_2$. Введем обозначение:

$$p_{max}(f) = \sup_{A \in \mathfrak{A}_2} \angle a_1(A) o(A) a_2(A).$$

Пусть $f \in \mathfrak{T}(2, n, 2) \setminus \mathfrak{T}(2, n)$, $B(E_n^2) \cap M_1(f) \neq \emptyset$ и $\mathfrak{A}_2(f) \neq \emptyset$. Если $p_{max}(f) < \pi$, то назовем *опорной* такую функцию $f' \in \mathfrak{T}(2, n, 2)$, для которой найдутся пороговые неравенства $A' \in \mathfrak{A}_2(f')$, удовлетворяющие условиям:

1) $f(x) = f'(x)$ для всех $x \in E_n^2 \setminus (o'a_1' \cup o'a_2')$;

2) Для $i = 1, 2$ существует $x \in o'a'_i$ такой, что $o'x \cap E_n^2 \subset M_1(f)$ и $xa'_i \cap E_n^2 \subset M_0(f)$, причем $o'x \cap E_n^2 \neq \emptyset, xa'_i \cap E_n^2 \neq \emptyset$.

3) $\angle a'_1 o' a'_2 = p_{max}(f)$.

Пороговые неравенства A' назовем *опорными* для f.

Теорема. *Класс $\mathfrak{T}(2, n, 2)$ разбивается на 9 подмножеств по оценке на мощность тупикового разрешающего множества, а именно:*

1) если $f \equiv 1$, то $\sigma(f, \mathfrak{T}(2, n, 2)) = 4$;

2) иначе, если $|M_1(f)| \leq 1$, то $\sigma(f, \mathfrak{T}(2, n, 2)) = \Omega(n^2)$;

3) иначе, если $f \in \mathfrak{T}(2, n)$, то $\sigma(f, \mathfrak{T}(2, n, 2)) = O\left(\min\limits_{A \in \mathfrak{A}_1(f)} l(a_1(A)a_2(A))\right)$;

4) иначе, если $\mathcal{S}(P(f)) = 0$, то $\sigma(f, \mathfrak{T}(2, n, 2)) = O(\sqrt{2}n - \mathrm{Diam}(P(f)))$;

5) иначе, если $M_1(f) \cap B(E_n^2) = \emptyset$, то

$$\sigma(f, \mathfrak{T}(2, n, 2)) = O(\min(\sqrt{2}n - \mathrm{Diam}(P(f)), \mathrm{Diam}(P(f))^2));$$

6) иначе, если существует единственная определяющая пара пороговых функций, то $\sigma(f, \mathfrak{T}(2, n, 2)) \leq 9$;

7) иначе, если $M_1(f) \subset B(E_n^2)$, то $\sigma(f, \mathfrak{T}(2, n, 2)) = n + 4$;

8) иначе, если $p_{max}(f) < \pi$, то

$$\sigma(f, \mathfrak{T}(2, n, 2)) = O\left(\min\left(n, \frac{1}{\pi - p_{max}(f)} + \frac{1}{\max(p_{max}(f) - \arcsin\frac{1}{l_1} - \arcsin\frac{1}{l_2}, 4(l_1 + l_2)^2)}\right)\right),$$

где $l_i = l(oa_i)$, $o = o(A), a_1 = a_1(A), a_2 = a_2(A)$ и A – пара опорных неравенств для f;

9) иначе $\sigma(f, \mathfrak{T}(2, n, 2)) = O(n)$.

Литература

1. Zamaraeva E. *On teaching sets of k-threshold functions* // http://arxiv.org/abs/1502.04340.

ИГРЫ В РАСКРАСКУ ГРАФА

Ю.А. Зуев

Московский государственный университет технологий и управления,
Земляной вал 73, 109044 Москва, yuri_zuev@mailfrom.ru

В последнее десятилетие XX века в теории графов возникло и получило развитие новое направление — *игры в раскраску графа.* Наиболее известной и исследованной игрой является следующая. Задан простой графа $G(V, E)$. Алиса и Боб поочерёдно выбирают одну из ещё не окрашенных вершин и окрашивают её в один из m заданных цветов. При этом никакие две смежные вершины не должны быть окрашены одним цветом. Алиса делает первый ход и, если игра завершается правильной раскраской графа, то она выигрывает. Если же на некотором этапе игры правильная раскраска становится невозможной (имеется неокрашенная вершина, в окружении которой использованы все краски), то выигрывает Боб.

Наименьшее число цветов m, при котором игра является выигрышной для Алисы, называется *игровым хроматическим числом* (*game chromatic number*) графа G и обозначается $\chi_g(G)$. Справедливо очевидное неравенство $\chi(G) \leq \chi_g(G) \leq \Delta(G) + 1$, где $\chi(G)$ — хроматическое число графа G, $\Delta(G)$ — его максимальная степень. Значительное число исследований было посвящено оценкам максимальных значений $\chi_g(G)$ в различных классах графов. Так в классе лесов этот максимум равен четырём.

Другую интересную игру в раскраску графа G можно получить, слегка изменив правила. Пусть число цветов $m = 2$, ходы делаются по очереди, первый ход делает Алиса, а проигрывает тот, кто при наличии неокрашенных вершин не может сделать очередного хода. Если же граф оказывается полностью раскрашенным, что возможно лишь в случае двудольного графа G, то результатом игры считается ничья. Следующая теорема описывает результаты этой игры в простейших случаях.

Теорема 1. *Если в качестве G взят простой цикл C_n, то Алиса проигрывает. Если в качестве G взята простая цепь P_n, то результатом игры является ничья. Если в качестве G взят n-мерный куб B^n, то Алиса проигрывает. В классе деревьев возможны все три результата игры.*

Доказательство теоремы проводится описанием выигрышной стратегии, когда результатом игры является выигрыш одной из сторон, и описанием ничейной стратегии для каждой стороны в случае ничьей.

Рассмотрим теперь существенно иную игру в раскраску графа, ранее в научной литературе, по-видимому, не встречавшуюся. Её постановка подсказана задачей, предлагавшейся на Московской математической олимпиаде в 2005 году [1, 66]. Алиса раскрашивает своим первым ходом в m цветов все рёбра графа $G(V, E)$, после чего Боб пытается раскрасить в те же m цветов вершины графа G так, чтобы ни для какого ребра обе его вершины не были окрашены в цвет ребра. Если ему это удаётся, то он выиграл, если нет — победила Алиса. Результат этой игры изучался автором для полного n-вершинного графа K_n. Ясно, что этот результат зависит от соотношения m и n.

Для полного n-вершинного графа K_n и m красок определим предикат $P(m, n)$

$$P(m,n) = \begin{cases} 0, & \text{если для любой раскраски рёбер графа } K_n \text{ существует} \\ & \text{раскраска его вершин, дающая правильную раскраску графа } K_n, \\ 1, & \text{если существует такая раскраска рёбер графа } K_n, \text{ что никакая} \\ & \text{раскраска его вершин не приводит к правильной раскраске} \\ & \text{графа } K_n. \end{cases}$$

Следующая теорема описывает поведение предиката $P(m, n)$ в зависимости от m и n.

Теорема 2 [2]. *Для каждого натурального m существует такое натуральное $\upsilon(m)$, что $P(m, n) = 1$ при $n \geq \upsilon(m)$ и $P(m, n) = 0$ при $n < \upsilon(m)$.*

Функция $\upsilon(m)$ строго монотонно возрастает по m и имеет квадратичный порядок роста $\upsilon(m) = \Theta\left(m^2\right)$.

Если q — степень простого числа такая, что $m \leq q - 1$, то $\upsilon(m)$ удовлетворяет двойному неравенству

$$m^2/2e + 2 \leq \upsilon(m) \leq q^2,$$

где $e = 2,71\ldots$ — основание натурального логарифма.

Доказательство монотонности предиката $P(m, n)$ по m и по n проводится стандартными для теории графов методами и не составляет труда.

Нижняя оценка теоремы доказывается вероятностным методом с использованием локальной леммы Ловаса (см. [3, 85]). Для произвольной фиксированной окраски рёбер графа K_n окрашиваем каждую его вершину независимо и равновероятно в один из m цветов. Для каждого ребра $e = \{v_i, v_j\} \in E(K_n)$ определим событие A_e: «ребро e и вершины v_i, v_j окрашены в один цвет». Тогда событие $\bigcap_{e \in E(K_n)} \bar{A}_e$ соответствует правильной вершинной раскраске.

Для каждого A_e имеем $\mathsf{P}(A_e) = 1/m^2$. Событие A_e может зависеть лишь от событий $A_{e'}$ для смежных с e рёбер e', а их $2(n-2)$. При $2em^{-2}(n-2) \leq 1$ условия локальной леммы Ловаса выполнены, а значит правильная вершинная раскраска существует. Отсюда получаем $\upsilon(m) > m^2/2e + 2$.

Идея получения верхней оценки содержится в [1, 381]. Пусть число вершин $n = q^2$, число цветов $m = q - 1$, где q — степень простого числа. Вершины графа K_{q^2} отождествляются с точками конечной аффинной плоскости порядка q. Множество из $q^2 + q$ прямых плоскости разбивается на $q + 1$ подмножеств — направлений, каждое из которых содержит q прямых. Прямые каждого направления не пересекаются и покрывают все q^2 точек. Из $q + 1$ направлений Алиса произвольно выбирает $q - 1$ и окрашивает рёбра каждого из них в отдельный цвет. Рёбра двух оставшихся направлений окрашиваются произвольно. Теперь при любой раскраске q^2 вершин в $q - 1$ цветов найдётся ребро, две вершины которого окрашены в цвет ребра. В самом деле, при раскраске q^2 точек в $q - 1$ цветов найдётся цвет, используемый более q раз. Поэтому среди q прямых направления этого цвета найдётся прямая с двумя точками этого цвета, т.е. обе вершины соответствующего ребра будут окрашены в цвет ребра. Отсюда $P\left(q-1, q^2\right) = 1$. Для произвольного числа цветов m, положив $q = 2^{\lceil \log_2(m+1) \rceil}$, имеем $m \leq q - 1$ и $q^2 < 4(m+1)^2$. Это даёт $P\left(m, 4(m+1)^2\right) = 1$. Откуда $\upsilon(m) \leq 4(m+1)^2$, что и устанавливает порядок роста $\upsilon(m)$.

В качестве непосредственного следствия из теоремы получаем следующие оценки для числа красок m в зависимости от числа вершин n графа K_n.

Следствие. *Если* $m > \sqrt{2e(n-2)}$, *то* $P(m,n) = 0$. *Если* $m < q$, *где* q — *любая степень простого числа такая, что* $q^2 \leq n$, *то* $P(m,n) = 1$.

Литература

1. Фёдоров Р. М., Каннель-Белов А. Я., Ковальджи А. К., Ященко И. В. *Московские математические олимпиады 1993-2005 г.* М.: МЦНМО. 2008.

2. Зуев Ю. А. *Одна задача о раскраске графа* // Мат. заметки. 2015. Т. 97. Вып. 6. С. 942–944.

3. Алон Н., Спенсер Дж., *Вероятностный метод.* М.: «БИНОМ, Лаборатория знаний», 2007.

ЦИКЛИЧЕСКИЙ ГРАФ ГАМИЛЬТОНОВА МАТРОИДА

А.Н. Исаченко[1], **Я.А. Исаченко**[2]

[1]Белгосуниверситет, факультет прикладной математики и информатики, Независимости 4, 220050, Минск, Беларусь isachen@bsu.by

[2]ООО "Аксенчер", Павелецкая пл., 2, 115054 Москва, Россия yarais@mail.ru

Теория матроидов тесно связана с теорией графов. Многие понятия теории матроидов появились как обобщения соответствующих графовых понятий и привели к возникновению отдельных направлений в исследовании матроидов. В свою очередь, характеризация матроидов зачастую даётся в терминах свойств графов. Приведенный ниже результат является примером такой характеризации.

Матроид [1,2] M на конечном множестве S можно определить как пару (S, C), где C семейство подмножеств из 2^S, удовлетворяющее двум аксиомам:

C1) если $X \neq Y \in C$, то $X \not\subset Y$;

C2) если $C_1, C_2 \in C$ и $z \in C_1 \cap C_2$, то существует $C_3 \in C$, такое что $C_3 \subseteq (C_1 \cup C_2) \backslash z$.

Подмножества из C называются циклами матроида. Цикл из одного элемента называют петлёй. Матроид называют связным, если для любых элементов множества S существует содержащий их цикл. Ранг $\rho(X)$ множества $X \subseteq S$ это мощность максимального подмножества X не содержащего цикла. Ранг матроида M равен $\rho(S)$.

Двойственный к M матроид $M^* = (S, C^*)$ определяется семейством C^*, состоящим из минимальных непустых подмножеств X множества S таких, что $|X \cap Y| \neq 1$ для каждого цикла $Y \in C$. Циклы двойственного матроида называются коциклами исходного матроида.

Для произвольного неориентированного графа $G = (V, E)$ пара (E, C), где C множество циклов графа образует матроид $M(G)$, который называют циклическим матроидом графа G. В свою очередь по циклам матроида можно определить так называемый циклический граф.

Пусть $M = (S, C)$ матроид на множестве S, определённый семейством циклов C. Циклический граф $G(M) = (V, E)$ матроида M это граф с множеством вершин $V = C$ и множеством рёбер E, состоящим из пар (C_1, C_2) таких, что:

1) $C_1 \cup C_2$ связное подмножество матроида M;

2) $\rho(C_1 \cup C_2) = |C_1 \cup C_2| - 2$.

В работе [3] было введено понятие гамильтонова матроида. Гамильтонов матроид – матроид, имеющий цикл с числом элементов на единицу большим ранга матроида.

Одно из свойств гамильтонова матроида дает следующее утверждение.

Теорема. *Циклический граф гамильтонова матроида является связным.*

Справедливость данного утверждения вытекает из двух фактов:

– матроид M без копетли является связным тогда и только тогда, когда его циклический граф $G(M)$ связный;

– как показано в [4] гамильтонов матроид является связным.

Литература

1. Welsh, D. J. A. *Matroid theory*. London: Acad. Press, 1976.

2. Айгнер М. *Комбинаторная теория* . М.: Мир, 1982.

3. Исаченко А. Н. *Периметр матроида и задача коммивояжера на матроиде* // XI Белорусская математическая конференция: Тез. докл. Междунар. науч. конф. Минск, 5–10 ноября 2012 г. – Часть 4. – Мн.: Институт математики НАН Беларуси, 2012. – С. 87-88.

4. Исаченко А. Н., Исаченко Я. А. *Свойства гамильтоновых матроидов* // Международный конгресс по информатике: информационные системы и технологии. Материалы меджунар. науч. конгресса, Республика Беларусь, Минск, 4–7 нояб. 2013 г. – Минск: БГУ. 2013. – С. 538–541.

К ГИПОТЕЗЕ ХАРТСФИЛДА-РИНГЕЛЯ ОБ АНТИМАГИЧНОСТИ СВЯЗНЫХ ГРАФОВ

В.Н. Калачев

Белорусский Государственный Университет, Механико-математический факультет
Независимости 4, 220050, Минск, Беларусь
vitkalachev@gmail.com

В 1990 г. Хартсфилд и Рингель ввели в своей книге [1] понятие *антимагической нумерации ребер графа*:

Определение 1. Пусть $G = (V, E)$ — (n, m)-граф, а $\varphi : E \to \{1, 2, \ldots, m\}$ — некоторая инъективная функция. Определим на V функцию f, положив для $\forall v \in V f(v) = \Sigma_e \varphi(e)$, где e пробегает множество ребер, инцидентных v. Если такая f также оказывается инъективной, то функция $\varphi(e)$ называется *антимагической нумерацией*.

Графы, для которых такая нумерация возможна, были названы *антимагическими*. Также в [1] высказано предположение, что все связные графы с $n \geqslant 3$ являются антимагическими. Таким образом, если эта гипотеза верна, получаем еще одно тривиальное свойство для связных графов (кроме K_2).

В общем случае гипотеза до сих пор не доказана и не опровергнута, хотя существует много работ, ей посвященных. Все имеющиеся на сегодня результаты получены путем сужения задачи на некоторый класс графов.

Теория алгебраической декомпозиции графов (АДГ) была разработана в Минске Р.И. Тышкевич и её учениками и зарекомендовала себя как эффективный способ решения различных задач на графах. Хотя АДГ изначально создавалась для решения алгоритмических задач и подсчета некоторых характеристик графов, последние результаты позволяют утверждать, что эта теория также применима и для исследования гипотез (например, сильной гипотезы Бержа или гипотезы Келли-Улама о реконструируемости).

Так, в частности, в 2008 г. М. Баррус в работе [2] доказал, что расщепляемые графы и 1-разложимые графы являются антимагическими. В 2014 году этот результат был обобщен автором и перенесен на более широкие классы графов, а именно на $(1,2)$-*полярные* и $(1,2)$-*разложимые* графы [3]. Также в 2014 году автором было показано, что *связные унографы являются антимагическими* [4] (на основе полного описания структуры унографов, полученного Р. И. Тышкевич в [5]).

В настоящем докладе представлены результаты дальнейших исследований в области применимости АДГ к доказательству гипотезы Харстфилда-Рингеля. Основное достижение — доказательство свойства антимагичности $(1,Q)$-*полярных* и $(1,Q)$-*разложимых* графов для произвольного $Q \geqslant 3$ при выполнении некоторых ограничений на степени вершин этих графов. А именно: $\deg b \leqslant \deg a$ и $\deg b \leqslant \deg c$ для $\forall a \in A, b \in B, c \in C$, где $V = A \sqcup B \sqcup C$, $G(A)$ — верхняя доля $(1,Q)$-полярного или $(1,Q)$-разложимого графа, $G(B)$ - его нижняя доля, $G(C)$ - произвольный граф (если он есть).

Литература

1. N. Hartsfield and G.Ringel. *Pearls in Graph Theory.* Boston: Academic Press, Inc., 1990.

2. M.D. Barrus. *Antimagic labeling and canonical decomposition of graphs.* Information Processing Letters Journal. 2010. Vol. 110. Issue 7. P.261–263.

3. Калачев В.Н. *К гипотезе Хартсфилда-Рингеля:* $(1,2)$*-полярные и* $(1,2)$*-разложимые графы.* Вестник БГУ. 2014. № 3. С. 81–83.

4. Калачев В.Н. *К гипотезе Хартсфилда-Рингеля: связные униграфы.* Труды института математики. 2014. Т. 22. № 2.

5. Tyshkevich R.I. *Decomposition of graphical sequences and unigraphs* // Discrete Mathematics. 2000. V. 220. P. 201–238.

3-РАСКРАШИВАЕМОСТЬ ЧИСТЫХ ДЕТСКИХ РИСУНКОВ СНАРКОВ И ЗАДАЧА “ОХОТА НА СНАРКА”

Т.Э. Кренкель

Московский технический университет связи и информатики,
кафедра теории вероятностей и прикладной математики
Авиамоторная 8а, 11024 Москва, Российская Федерация krenkel2001@mail.ru

Теория снарков — раздел теории топологических графов и комбинаторной топологии, в котором рассматривается задача полиэдрального вложения нетривиальных кубических (тривалентных) графов в компактные римановы поверхности рода g.

Снарк является кубическим графом, не допускающим раскраску по Тейту. Граф Петерсена (1898) является минимальным и единственным снарком с 10 вершинами и 15 ребрами. В 1946 году Татт после появления двух кубических графов Блануши доказал, что любой нетривиальный кубический граф может быть сведен к графу Петерсена с помощью двух операций - слияния вершин и вычеркивания ребер.

Исследования в теории снарков мотивированы гипотезой Грюнбаума (1969).

Гипотеза Грюнбаума. *Если кубический граф допускает полиэдральное вложение в ориентированную поверхность, то он 3 — раскрашиваем.*

Сам термин “снарк” был введен Гарднером в 1976 году к 100-летию публикации поэмы Льюиса Кэрролла “*The hunting of the snark*”, посвященной погоне за загадочным существом, именуемым “снарк”.

Теорема Шеннона. *Ребра любого графа могут быть окрашены так, что любые два ребра с общим концом будут иметь различные цвета при использовании самое большее* $\lfloor \frac{3}{2}m \rfloor$ *цветов, где* m *— максимальное число ребер, исходящих из одной вершины.*

Снарки — это тривалентные графы $m = 3$ и поэтому хроматическое число снарка по теореме Шеннона равно 4, т.е. он нераскрашиваем по Тейту.

Чтобы получить 3-раскрашиваемость снарка выскажем следующую гипотезу:

Гипотеза о 3-раскрашиваемости снарков. *Снарк раскрашиваем по Тейту при переходе от снарков в категорию чистых детских рисунков Гротендика Dessin.*

Переход от снарка к чистому детскому рисунку снарка осуществляется добавлением белой вершины посередине каждого ребра снарка, т.е. построением двукрашенного графа с полуребрами.

Лемма Гротендика. *Существует биекция между парами Белого* $(\sum_{g,3}, \beta)$ *и детскими рисунками Гротендика Dessin, где* $\sum_{g,3}$ *компактная риманова поверхность рода* g *с тремя отмеченными точками, а* β *мероморфная функция Белого с тремя критическими значениями.*

Сформулируем задачу:

Задача "Охота на Снарка". *Найти пару Белого* $(\sum_{g,3}, \beta)$ *для чистого детского рисунка Снарка.*

Снарк с большой буквы — это граф Петерсена.

ЗАДАЧА О ВЗВЕШЕННОЙ НЕЗАВИСИМОЙ $\{K_1, K_2\}$-УПАКОВКЕ ГРАФА

В.В. Лепин

Институт математики НАН Беларуси, Сурганова 11, 220072 Минск, Беларусь
lepin@im.bas-net.by

Рассматривается задача о взвешенной независимой $\{K_1, K_2\}$-упаковке графа, имеющего веса на вершинах и ребрах. Частными случаями этой задачи являются задачи об индуцированном паросочетании и о диссоциирующем множестве в графе. Задача о взвешенной независимой $\{K_1, K_2\}$-упаковке графа возникает при применении метода модулярной декомпозиции для решения указанных задач [1].

Пусть $\mathcal{H}$ — фиксированное множество связных графов. *$\mathcal{H}$-упаковкой* графа G называется множество $\mathcal{S} = \{G_1, G_2, \ldots, G_m\}$ попарно не пересекающихся по вершинам подграфов графа G, каждый из которых изоморфен графу из $\mathcal{H}$. Говорят, что *вершина графа G покрывается $\mathcal{H}$-упаковкой,* если она принадлежит подграфу этой упаковки. *Независимой $\mathcal{H}$-упаковкой* графа G называется $\mathcal{H}$-упаковка S, в которой никакие два подграфа упаковки не соединены ребром графа G. Если дан граф G с весовыми функциями $\omega_V : V(G) \to \mathbb{N}$ и $\omega_E : E(G) \to \mathbb{N}$ на вершинах и ребрах, и независимая $\{K_1, K_2\}$-упаковка S графа G, то *весом упаковки S* называется $\sum_{v \in U} \omega_V(v) + \sum_{e \in F} \omega_E(e)$, где $U = \bigcup_{G_i \in \mathcal{S},\ G_i \cong K_1} V(G_i)$ и $F = \bigcup_{G_i \in \mathcal{S}} E(G_i)$. Рассматривается задача о взвешенной независимой $\{K_1, K_2\}$-упаковке графа, в которой требуется найти независимую $\{K_1, K_2\}$-упаковку наибольшего веса.

Если множество подграфов $\mathcal{S}$ является независимой $\{K_1, K_2\}$-упаковкой графа G, то его можно однозначно задать парой множеств (U, F), где $U = \bigcup_{G_i \in \mathcal{S}_1} V(G_i)$ и $F = \bigcup_{G_i \in \mathcal{S}_2} E(G_i)$.

Будем предполагать, что для каждого ребра $vu \in E$ выполняется

$$\max\{w_V(v), w_V(u), w_E(vu)\} > 0.$$

Подмножество вершин $U \subseteq V(G)$ называется *диссоциирующим множеством* графа G, если максимальная степень вершин в подграфе $G[U]$ не превосходит 1. Задача о диссоциирующем множестве наибольшего размера является NP-трудной для двудольных графов, для C_4-свободных двудольных графов с максимальной вершинной степенью 3. Решается эта задача за полиномиальное время в нескольких классах графов.

Подмножество ребер графа G называется *паросочетанием,* если ни какие два ребра из этого множества не имеют общей концевой вершины. *Индуцированным паросочетанием* называется паросочетание $F \neq \emptyset$, в котором ни какие два ребра не соединены ребром графа G, т.е. максимальная степень вершин в подграфе $G[F]$ равна 1. Задача об индуцированном паросочетании наибольшего размера является NP-трудной для двудольных графов, планарных графов. Она эффективно решается в нескольких классах графов.

Устанавливая определенные веса вершинам и ребрам графа G, мы можем формулировать известные задачи в виде взвешенной задачи о независимой $\{K_1, K_2\}$-упаковке графа G.

Пусть G — граф. Если $\omega_V(u) = 1$ для каждой вершины $u \in V(G)$, а $\omega_E(e) = 0$ для каждого ребра $e \in E(G)$ и (U^*, F^*) — наибольшего веса независимая $\{K_1, K_2\}$-упаковка графа G, то U^* является наибольшим независимым множеством в графе G.

Если $\omega_V(u) = 0$ для каждой вершины $u \in V(G)$, а $\omega_E(e) = 1$ для каждого ребра $e \in E(G)$ и (U^*, F^*) — наибольшего веса независимая $\{K_1, K_2\}$-упаковка графа G, то F^* является наибольшим индуцированным паросочетанием в графе G.

Если $\omega_V(u) = 1$ для каждой вершины $u \in V(G)$, а $\omega_E(e) = 2$ для каждого ребра $e \in E(G)$, и (U^*, F^*) — наибольшего веса независимая $\{K_1, K_2\}$-упаковка графа G, то $U^* \cup V(F^*)$ является наибольшим диссоциирующим множеством в графе G.

Теорема 1. *Существует алгоритмы, которые решают взвешенную задачу о независимой $\{K_1, K_2\}$-упаковке для деревьев за время $O(n)$, для унициклических графов за время $O(n^2)$, для кографов и расщепляемых графов за время $O(n+m)$, для co-gem-свободных графов за время $O(m(m+n))$, где n — число вершин и m — число ребер графа.*

Теорема 2. *Существует алгоритм, такой, что если на его вход дан взвешенный граф $G = (V, E)$ и его древесная декомпозиция ширины k, то он решает взвешенную задачу о независимой $\{K_1, K_2\}$-упаковке за время $O(2^k mk)$, где $m = |V(T)|$ — число узлов в дереве декомпозиции.*

Параметризованная сложность. В теории параметризованной сложности вход задачи состоит из двух частей (I, k), где I — это главная часть, а k (часто натуральное число) — параметр. Выделяют следующие три категории фиксированно-параметрической сложности NP-полных задач:

1. Задачи, которые для каждого фиксированного k могут быть решены за полиномиальное время, где степень полинома не зависит от k;

2. Задачи, которые для каждого фиксированного k могут быть решены за полиномиальное время, но степень полинома зависит от k;

3. Для некоторого фиксированного k задача является NP-трудной;

Задачи распознавания, которые принадлежат первой категории, называются фиксированно-параметрически разрешимыми (англ. fixed-parameter tractable) и образуют класс FPT. Другими словами, если задача (I, k) может быть решена алгоритмом с трудоемкостью $O(f(k)+n^c)$ или $O(f(k)n^c)$, где f — это некоторая вычислимая функция, а c — некоторая константа не зависящая от k, то она принадлежит классу FPT.

Известно, что для доказательства того, что некоторая параметризованная задача является фиксированно-параметрически разрешимой, достаточно найти алгоритм преобразования каждой ее индивидуальной задачи к ядру, т.е., для каждой индивидуальной задачи (I, k) задачи P, построить индивидуальную задачу (I', k') такую, что выполняются следующие условия:

1. $k' \leq k$ и $|I'| \leq g(k)$, где g — некоторая вычислимая функция;

2. преобразование задачи (I, k) к (I', k') осуществляется за полиномиальное время;

3. индивидуальная задача (I, k) имеет ответ "да"тогда и только тогда, когда задача (I', k') имеет ответ "да".

Рассмотрим следующую параметризованную задачу:

ВЗВЕШЕННАЯ ЗАДАЧА О НЕЗАВИСИМОЙ $\{K_1, K_2\}$-УПАКОВКЕ

Вход: граф $G = (V, E)$, весовые функции $\omega_V : V(G) \to \mathbb{N}$ и $\omega_E : E(G) \to \mathbb{N}$, положительное целое k.

Вопрос: Существует ли независимая $\{K_1, K_2\}$-упаковка, имеющая вес не менее k.

Параметр: k.

Частным вариантом ВЗВЕШЕННОЙ ЗАДАЧИ О НЕЗАВИСИМОЙ $\{K_1, K_2\}$-УПАКОВКЕ графа является ЗАДАЧА ОБ ИНДУЦИРОВАННОМ ПАРОСОЧЕТАНИИ:

Вход: граф $G = (V, E)$, положительное целое k.

Вопрос: Существует ли индуцированное паросочетание с не менее чем k ребрами.

Параметр: k.

Известно, что эта ЗАДАЧА ОБ ИНДУЦИРОВАННОМ ПАРОСОЧЕТАНИИ является W[1]-трудной, поэтому ВЗВЕШЕННАЯ ЗАДАЧА О НЕЗАВИСИМОЙ $\{K_1, K_2\}$-УПАКОВКЕ также является W[1]-трудной. Следовательно, мало вероятно, что обе задачи принадлежат классу FPT. Поэтому представляет научный интерес выяснение параметризованной сложности этих задач в классах графов, в которых они остаются NP-полными.

Теорема 3. *ВЗВЕШЕННАЯ ЗАДАЧА О НЕЗАВИСИМОЙ $\{K_1, K_2\}$-УПАКОВКЕ в классе графов, степени вершин которых ограничены числом d имеет ядро, состоящее из $O(d^2k)$ вершин (т.е. размер ядра является линейным, если d — константа). Для любого графа ядро может быть построено за время $O(n + m)$, где $n = |V|$ и $m = |E|$.*

В [3] доказано, что ЗАДАЧА ОБ ИНДУЦИРОВАННОМ ПАРОСОЧЕТАНИИ является NP-полной в классе C_4-свободных двудольных графов. Поскольку класс C_4-свободных двудольных графов содержится в классе графов с обхватом не меньшим шести, то ВЗВЕШЕННАЯ ЗАДАЧА О НЕЗАВИСИМОЙ $\{K_1, K_2\}$-УПАКОВКЕ является NP-полной в последнем классе графов.

Теорема 4. *ВЗВЕШЕННАЯ ЗАДАЧА О НЕЗАВИСИМОЙ $\{K_1, K_2\}$-УПАКОВКЕ в классе графов с обхватом не меньшим шести имеет ядро с $O(k^3)$ вершинами. Для любого графа ядро может быть построено за время $O(n + m)$, где $n = |V|$ и $m = |E|$.*

Работа выполнена при поддержке Белорусского республиканского фонда фундаментальных исследований (проект Ф14РА–004).

Литература

1. Лепин В.В. *Алгоритмы для нахождения независимой $\{K_1, K_2\}$-упаковки наибольшего веса в графе* // Труды Института математики. 2014. Т. 22, № 1. С. 78–97.

2. Лепин, В.В. *Решение задачи о взвешенной независимой $\{K_1, K_2\}$-упаковке на графах с ограниченной древесной шириной* // Труды Института математики. 2015. Т. 23, № 1. С. 98–114.

3. Lozin V.V. *On maximum induced matchings in bipartite graphs* // Information Processing Letters. 2002. V. 81, № 1. P. 7–11.

ПОСТРОЕНИЕ *AOE*-ЦЕПИ В ПЛОСКОМ ГРАФЕ

Т.А. Макаровских[1], **Е.А. Савицкий**[2]

Южно-Уральский государственный университет, пр. Ленина, д. 76, 454080 Челябинск, Россия
[1]kwark@mail.ru, [2]egor88@inbox.ru

Пусть $G = (V, E)$ – граф, а $T = v_0, k_1, v_1, \ldots, k_n, v_n,\ v_n = v_0$ – эйлеров цикл в нем. Предположим, что в каждой вершине $v \in V$ задан циклический порядок $O^{\pm}(v)$, определяющий систему переходов $A_G(v) \subset O^{\pm}(v)$ в этой вершине. В случае, когда $\forall v \in V(G)\ A_G(v) = O^{\pm}(v)$, систему переходов $A_G(v)$ будем называть **полной системой переходов**.

Определение 1. *Маршрут T удем называть **A-цепью** тогда и только тогда, когда он является A_G-совместимой цепью. Таким образом, последовательные ребра в цепи T (инцидентные вершине v) являются соседями в циклическом порядке $O^{\pm}(v)$.*

Определение 2. *Будем говорить, что **цепь** $C = v_1e_1v_2e_2\ldots v_k$ в графе G имеет **упорядоченное охватывание** (является OE-цепью), если для любой ее начальной части $C_i = v_1e_1v_2e_2\ldots e_i$, $l \leq (|E(G)| + |H(G)|)$ выполнено условие*

$$\mathrm{Int}(C_i) \cap (E(G) \cup H(G)) = \emptyset.$$

Определение 3. *Будем говорить, что цепь является AOE-цепью, если она одновременно является OE-цепью и A-цепью.*

Данный вид цепей подробно описан в монографии Г. Фляйшнера [1]. В общем случае задача поиска такой цепи в графе относится к классу $\mathcal{NP}$-трудных задач, однако для некоторых частных случаев существуют эффективные алгоритмы ее решения. В работах данного автора приводятся также полиномиальный алгоритм для внешнеплоских графов [2] и для 4-регулярных графов [1] (т.е. графов, степень каждой вершины которых равна 4). В [1, Следствие VI.6] приводится доказательство существования A-цепи для любого связного 4-регулярного графа на любой поверхности. Для доказательства данного факта автор использует Лемму о расщеплении [1, Лемма III.26]. Также доказано, что существует полиномиальный алгоритм для распознавания A-цепи в 4-регулярном графе.

В общем случае наличие в графе A-цепи вовсе не означает выполнение для нее условия упорядоченного охватывания. Однако, маршрут, для которого не выполнено условие упорядоченного охватывания, всегда будет содержать переход через охватывающий цикл. Этот переход несовместим с системой переходов A-цепи. Таким образом справедлива теорема [3].

Теорема 1. *Если в плоском графе G графе существует A-цепь, то существует и AOE-цепь.*

Очевидно, что т.к. для всех $v \in V(G)$, имеем $\deg(v) = 4$, то 4-регулярный граф является эйлеровым. Рассмотрим следствие из теоремы 1.

Следствие 1. *В связном плоском 4-регулярном графе существует AOE-цепь.*

В [3] приведен алгоритм `AOE-TRAIL` построения AOE-цепи.

Теорема 2. *Вычислительная сложность алгоритма `AOE-TRAIL` является линейной величиной $O(|E|)$.*

Рассмотрим произвольный плоский граф G. В [4] показано, что в G всегда существует эйлерово OE-покрытие. Если G является плоским эйлеровым графом, то в нем существует OE-цикл. Плоский эйлеров граф имеет OE-цикл (цепь), однако он может и не являться AOE-цепью.

Определение 4. *Эйлеровым AOE-покрытием называется минимальная по мощности упорядоченная последовательность A-цепей, являющихся OE-покрытием. Если убрать требование минимальность, то покрытие будем называть AOE-покрытием* [3].

Следовательно, OE-цепь можно считать последовательностью нескольких A-цепей. Но если граф является суграфом некоторого 4-регулярного графа, всегда возможно построить

эйлерово AOE-покрытие. Рассмотренный выше алгоритм для 4-регулярного графа позволит построить такое покрытие после дополнения графа G до 4-регулярного графа G' добавлением N ребер, где $2N$ – число вершин нечетной степени графа G [5].

Разработана программа [6], которая обеспечивает определение AOE-цепи в плоском 4-регулярном графе. Программа является реализацией представленного алгоритма и может быть использована для демонстрации разработанных алгоритмов поиска решения указанной задачи. Каждое ребро графа представляется списком инцидентных ему вершин и левых и правых соседних ребер, инцдентных каждой из вершин и значением ранга каждого ребра.

Для представления графа в памяти компьютера используются следующие классы:

```
struct GraphEdge{
   int v1,v2; //Инцидентные вершины
   int l1,l2; //Соседние ребра при вращении против часовой стрелки
   int r1,r2; //Соседние ребра при вращении по часовой стрелке
   bool f0; //Флаг смежности ребра внешней грани
   int rank; //ранг ребра
   void REPLACE(); //Перестановка индексов ребра
   GraphEdge(){ //Конструктор по умолчанию
      };
};

class Graph{
public:
   GraphEdge *E; //Набор ребер графа
   int EdgeNum; //Число ребер графа
   Graph(int N){ //Конструктор графа из N ребер
      EdgeNum=N+1;
      E=new GraphEdge[N+1];
   };
   Graph(){}; //Конструктор по умолчанию
   void WriteData(int *ATrail); //Запись ответа
   int *FindATrail(int v0); //Поиск A-цепи
   int Deg(int vertex);//Определение степени вершины
};
```

Литература

1. Фляйшнер Г. *Эйлеровы графы и смежные вопросы.* М.: Мир, 2002.

2. Andersen L. D., Fleischner H., Regner S. *Algorithms and outerplanar conditions for A-trails in plane Eulerian graphs* // Discrete Applied Mathematics. 1998. No. 85. P. 99–112.

3. Макаровских Т. А. *Покрытие графа для прямоугольного раскройного плана AOE-цепями* // Информационные технологии и системы: тр. Четвертой междунар. науч. конф., Банное, Россия, 25 февр. – 1 марта 2015 г. (ИТиС–2015) : науч. электр. изд. / отв. ред.: Ю. С. Попков, А. В. Мельников. Челябинск : Изд-во Челяб. гос. ун-та, 2015. С. 17–18.

4. Панюкова Т. А. *Оптимальные эйлеровы покрытия с упорядоченным охватыванием для плоских графов.* Дискретный анализ и исследование операций. 2011. Том 18, № 2. С. 64–74.

5. Макаровских Т. А. *О построении эйлерова AOE-покрытия в плоском графе* // Информационный бюллютень №13, XV Всероссийская конф. «Математическое программирование и приложения». 2015. С. 96–97.

6. Макаровских Т. А. *Программа построения A-цепи с упорядоченным охватыванием в плоском 4-регулярном в графе* // Программы для ЭВМ. Базы данных. Топологии интегральных микросхем. – Официальный бюллетень Российского агентства по патентам и товарным знакам. 2015 г. М.: ФИПС. – 2015. – Рег. № 2014663188.

ВЕРИФИКАЦИЯ МОДУЛЯРНОГО РАЗДЕЛЕНИЯ СЕКРЕТА

Г.В. Матвеев[1], **Т.В. Галибус**[2]

[1]Белгосуниверситет, факультет прикладной математики и информатики
Независимости 4, 220050 Минск, Беларусь matveev@bsu.by
[2]Белгосуниверситет, факультет прикладной математики и информатики
Независимости 4, 220050 Минск, Беларусь tan2tan@gmail.com

Схемы разделения секрета (СРС) лежат в основе многих криптографических протоколов. В частности, разделение секрета применяется для совместных конфиденциальных вычислений [1], шифрования на основе атрибутов [2] и электронного защищенного голосования [3]. Важной задачей в разделении секрета является построение таких схем, где пользователи могут проверить корректность секрета и тем самым не допустить обман со стороны остальных участников и дилера. В схемах верифицируемого разделения секрета (СВРС) дилер распределяет информацию о секретном значении среди участников таким образом, что для честных пользователей гарантируется получение ими значения секрета, а для нечестных - невозможность восстановить секрет.

СВРС позволяет "честным" пользователям т.е. тем, которые следуют протоколу восстановления секрета, проверить корректность частичных секретов при их распределении и восстановлении исходного секрета. Верификация разделения секрета лежит также в основе криптографического протокола совместных конфиденциальных вычислений (СКВ) [1] .

В основе верификации схем разделения секрета лежит подход Фельдмана [4], который основывается на свойстве гомоморфности функции дискретного логарифма. Позже Беналоу [2] предложил еще один подход. Оба этих метода применяются лишь для верификации параметров пороговой схемы Шамира.

В последние годы получили развитие методы верификации для модулярного разделения секрета, что обусловлено быстродействием модулярного алгоритма восстановления [5], адаптивными свойствами таких схем [6] и возможностью включить верификацию для произвольных структур доступа [7]. Изучением данного вопроса занимались Ифтене [8], Кьонг и др.[9], Кайя и Сельджук [10]. В их работах предложены алгоритмы верификации для модулярных пороговых схем Миньотта [11] и Асмуса-Блюма [5] в кольце целых чисел. Общим недостатком данных методов является их применимость лишь в кольце целых чисел, что, в силу отсутствия совершенной схемы в этом кольце [12] делает их неприменимыми на практике. Преимуществом предложенных нами полиномиальных схем модулярного разделения секрета является их теоретико-информационная стойкость: полиномиальная модулярная схема является, в общем случае, совершенной, а в пороговом - идеальной [7].

Поэтому верификация полиномиальной модулярной схемы является актуальной задачей. Нами предлагается верификация всех параметров разделения секрета, т.е. дилер публикует секретные параметры, включая основной секрет, зашифрованные односторонней функцией верификации.

Пороговая полиномиальная модулярная СРС была предложена в работах [6], [7] и уже принята в качестве стандарта в РБ (СТБ 34.101.60). Данная схема позволяет разделить секретное значение $s(x) \in F_p[x]$. Промежуточный секрет $S(x)$ (t,k)-пороговой модулярной полиномиальной схемы выбирается так, чтобы $degS(x) < tn$, где t — порог, а n — общая степень модулей участников.

Для разделения секрета случайным образом выбирается промежуточное значение секрета $S(x) \in F_p[x]$ с условием $degS(x) < tn$. Случайным образом выбираются попарно различные неприводимые $m_i(x), i = 1,..,k$ и $p(x)$ с ограничением $degm_i(x) = degp(x) = n$. В работе [7] указан способ выбора параметров t, k, n, p. Дилером публикуются $m_i(x), p(x)$, а $s(x) = S(x) \bmod p(x)$ назначается в качестве секрета схемы. Дилером по секретным каналам участников отправляются их частичные секреты: $s_i(x) = S(x) \bmod m_i(x)$.

Для восстановления участники из подмножества A обмениваются своими частичными секретами $s_i(x), i \in A$ и находят значение секрета $s(x)$ применяя алгоритм CRT.

Пусть заданы параметры (t, k)-пороговой модулярной схемы:

$$m_1(x), m_2(x), \ldots, m_k(x), p(x), S(x), s(x) \in F_p[x].$$

При этом, $s(x) = S(x) \bmod p(x)$ или $S(x) = p(x)q(x) + s(x)$. Обобщая известный метод верификации Фельдмана [4], предлагается поступить следующим образом. Пользователю, т.е. обладателю полинома $s_i(x), i = 1, 2, \ldots, k$ фактически необходимо проверить условие: $S(x) = m_i(x)q(x) + s_i(x)$ или $s_i(x) = S(x) \bmod m_i(x)$, при том, что полином S(x) остается скрытым.

С этой целью условие $S(x) = m_i(x)q(x) + s_i(x)$ перепишем в виде: $S(\alpha_j) = s_i(\alpha_j), j = 1, 2, ..., n$, где $\alpha_1, \alpha_2, ..., \alpha_n$ - корни многочлена $m_i(x)$. Это позволяет полиномиальную схему Асмута-Блюма интерпретировать как схему Шамира, а значит, применима верификация по Фельдману [4].

Литература

1. Cramer R., Damgard I., Nielsen J. *Multiparty Computation from Threshold Homomorphic Encryption* // LNCS. 2001. Vol. 2045. P. 280–300.

2. Bethencourt J., Sahai A., Waters B. *Ciphertext-policy attribute-based encryption* // Proceedings of IEEE Symposium on Security and Privacy. 2007. P. 321–334.

3. Benaloh J. *Secret sharing homomorphisms: keeping shares of a secret secret* // LNCS. 1987. Vol. 263. P. 251–260.

4. Feldman P. *A practical scheme for non-interactive verifiable secret sharing* // IEEE Symposium on Foundations of Computer Science. 1987. P. 427–437.

5. Asmuth C. A. , Bloom J. *A modular approach to key safeguarding* // IEEE Transactions on Information Theory. - 1983. - Vol. 29. - P. 156-169.

6. Galibus T. Matveev G. Shenets N. *Some structural and security properties of the modular secret sharing* // Proc. of SYNASC'08, IEEE Comp. soc. press, Los Alamitos, 2009. P. 197-200.

7. Galibus T. Matveev G. *Generalized Mignotte Sequences in Polynomial Rings* // ENTCS. 2007. Vol. 186. P. 39–43.

8. Iftene S. *Secret sharing schemes with applications in security protocols*. Technical Report TR 07-01 // University Alexandru Ioan Cuza of Iasi, Faculty of Computer Science. 2007.

9. Qiong L., Zhifang W., Xiamu N., Shenghe S. *A non-interactive modular verifiable secret sharing scheme* // Proc. of ICCCAS'05, 2005. Vol.1. P. 84–87.

10. Kaya K., Selcuk A. *A Verifiable Secret Sharing Scheme Based on the Chinese Remainder Theorem.* // LNCS. 2008. Vol.5365. P. 288–305.

11. Mignotte M. *How to share a secret* // Advances in cryptology - Eurocrypt'82, LNCS. 1982. P. 371–375.

12. Quisquater M., Preneel B., Vandewalle J. *On the security of the threshold scheme based on the Chinese remainder theorem* // LNCS. 2002. Vol. 2274. P. 199–210.

ДИСТАНЦИОННО РЕГУЛЯРНЫЕ ГРАФЫ, В КОТОРЫХ ОКРЕСТНОСТИ ВЕРШИН СИЛЬНО РЕГУЛЯРНЫ СО ВТОРЫМ СОБСТВЕННЫМ ЗНАЧЕНИЕМ, НЕ БОЛЬШИМ t

А.А. Махнев

Институт математики им. Н.Н. Красовского УрО РАН, Ковалевской 16, 620990 Екатеринбург, Россия
makhnev@imm.uran.ru

Мы рассматриваем неориентированные графы без петель и кратных ребер. Для вершины a графа Γ через $\Gamma_i(a)$ обозначим i-окрестность вершины a, то есть, подграф, индуцированный

Γ на множестве всех вершин, находящихся на расстоянии i от a. Подграф $\Gamma(a) = \Gamma_1(a)$ называется окрестностью вершины a и обозначается $[a]$, если граф Γ фиксирован.

Степенью вершины называется число вершин в ее окрестности. Граф Γ называется регулярным степени k, если степень любой вершины a из Γ равна k. Граф Γ назовем реберно регулярным с параметрами (v, k, λ), если он содержит v вершин, регулярен степени k, и каждое его ребро лежит в λ треугольниках. Граф Γ — вполне регулярный граф с параметрами (v, k, λ, μ), если он реберно регулярен с соответствующими параметрами, и $[a] \cap [b]$ содержит точно μ вершин для любых двух вершин a, b, находящихся на расстоянии 2 в Γ. Вполне регулярный граф называется сильно регулярным графом, если он имеет диаметр 2. Графом в половинном случае называется сильно регулярный граф с параметрами $(4\mu+1, 2\mu, \mu-1, \mu)$.

Если вершины u, w находятся на расстоянии i в Γ, то через $b_i(u, w)$ (через $c_i(u, w)$) обозначим число вершин в пересечении $\Gamma_{i+1}(u)$ ($\Gamma_{i-1}(u)$) с $[w]$. Граф Γ диаметра d называется дистанционно регулярным с массивом пересечений $\{b_0, b_1, \ldots, b_{d-1}; c_1, \ldots, c_d\}$, если значения $b_i(u, w)$ и $c_i(u, w)$ не зависят от выбора вершин u, w на расстоянии i в Γ для любого $i = 0, ..., d$. Графом Тэйлора называется дистанционно регулярный граф с массивом пересечений $\{k, \mu, 1; 1, \mu, k\}$.

Система инцидентности с множеством точек P и множеством прямых $\mathcal{L}$ называется α-частичной геометрией порядка (s, t), если каждая прямая содержит ровно $s+1$ точку, каждая точка лежит ровно на $t+1$ прямой, любые две точки лежат не более чем на одной прямой, и для любого антифлага $(a, l) \in (P, \mathcal{L})$ найдется точно α прямых, проходящих через a и пересекающих l (обозначение $pG_\alpha(s, t)$). В случае $\alpha = 1$ геометрия называется обобщенным четырехугольником и обозначается $GQ(s, t)$. Точечный граф геометрии определяется на множестве точек P и две точки смежны, если они лежат на прямой. Точечный граф геометрии $pG_\alpha(s, t)$ сильно регулярен с $v = (s+1)(1+st/\alpha)$, $k = s(t+1)$, $\lambda = s-1+t(\alpha-1)$, $\mu = \alpha(t+1)$. Сильно регулярный граф с такими параметрами для некоторых натуральных чисел α, s, t называется псевдогеометрическим графом для $pG_\alpha(s, t)$.

Дж. Кулен предложил задачу изучения дистанционно регулярных графов, в которых окрестности вершин — сильно регулярные графы со вторым собственным значением, не большим t, для данного натурального числа t. Заметим, что сильно регулярный граф с нецелым собственным значением является графом в половинном случае, а вполне регулярный граф, в котором окрестности вершин — сильно регулярные графы в половинном случае, либо имеет диаметр 2, либо является графом Тэйлора. Таким образом, задача Кулена может быть решена пошагово для $t = 1, 2, ...$

В настоящее время задача Кулена полностью решена для $t = 3$. Близится к завершению перечисление массивов пересечений дистанционно регулярных графов, в которых окрестности вершин — сильно регулярные графы с собственным значением t для $3 < t \leq 4$ [1-2].

В данной статье начата разработка программы изучения дистанционно регулярных графов, в которых окрестности вершин — сильно регулярные графы с неглавным собственным значением t, $4 < t \leq 5$.

Сильно регулярный граф Γ с неглавным собственным значением $m-1$ назовем исключительным, если он не принадлежит следующему списку:

(1) объединение изолированных m-клик;

(2) псевдогеометрический граф для $pG_t(t+m-1, t)$;

(3) дополнение псевдогеометрического графа для $pG_m(s, m-1)$;

(4) граф в половинном случае с параметрами $(4\mu+1, 2\mu, \mu-1, \mu)$, $(-1+\sqrt{4\mu+1})/2 = m-1$.

А. Ноймайер [3] показал, что сильно регулярный граф Γ с неглавным собственным значением $m-1$ принадлежит либо вышеуказанному списку, либо конечному множеству исключительных графов.

Теорема. *Пусть Γ — дистанционно регулярный граф, в котором окрестности вершин — сильно регулярные графы с неглавным собственным значением t, $4 < t \leq 5$, u — вершина*

графа Γ *. Тогда* $[u]$ *— исключительный сильно регулярный граф с неглавным собственным значением* 5*, или верно одно из утверждений:*

(1) $[u]$ *— объединение изолированных* 6*-клик;*

(2) $[u]$ *— псевдогеометрический граф для* $pG_{s-5}(s, s-5)$ *и либо*

(i) Γ *— сильно регулярный граф с параметрами* $(176, 49, 12, 14)$*,* $(209, 100, 45, 50)$*,* $(806, 625, 480, 500)$*,* $(1464, 1225, 1020, 1050)$*, и* $s = 6, 9, 24, 34$ *соответственно, либо*

(ii) $s = 6$ *и* Γ *— граф Джонсона* $J(14, 7)$*, его стандартное частное или граф с массивом пересечений* $\{49, 36, 1; 1, 12, 49\}$*, либо*

(iii) $s = 7$ *и* Γ*имеет массив пересечений* $\{64, 42, 1; 1, 21, 64\}$*, либо*

(iv) $s = 10$ *и* Γ *— граф Тэйлора;*

(3) $[u]$ *— дополнение псевдогеометрического графа для* $pG_6(s, 5)$*,* Γ *— сильно регулярный граф с параметрами* $(259, 42, 5, 7)$*,* $(356, 85, 30, 17)$*, и* $s = 8, 6$ *соответственно или* $s = 12$ *и* Γ *— граф Тэйлора;*

(4) $[u]$ *— граф в половинном случае с параметрами* $(4l+1, 2l, l-1, l)$*,* $l \in \{21, 22, 24, 25, 27, 28, 29, 30\}$ *и* Γ *— граф Тэйлора.*

Работа выполнена при финансовой поддержке гранта РНФ (проект 15-11-10025).

Литература

1. Махнев А. А. *Сильно регулярные графы с неглавным собственным значением 4 и их расширения* // Известия Гомельского госуниверситета. 2014. Т. 84. № 3. С. 84–85.

2. Махнев А. А., Падучих Д. В. *Сильно регулярные графы с неглавным собственным значением 4 и их расширения* // Межд. конференция "Мальцевские чтения". Тез. докл. Новосибирск. 2014. С. 69.

3. Neumaier A. *Strongly regular graphs with smallest eigenvalue* $-m$ // Arch. Math. 1979. V. 33. С. 392–400.

ОБ АВТОМОРФИЗМАХ СИЛЬНО РЕГУЛЯРНЫХ ГРАФОВ С ПАРАМЕТРАМИ (204,28,2,4) И (595,144,18,40)

А.А. Махнев, Д.В. Падучих

Институт математики им. Н.Н. Красовского УрО РАН, Ковалевской 16, 620990 Екатеринбург, Россия
makhnev@imm.uran.ru, dpaduchikh@gmail.com

Мы рассматриваем неориентированные графы без петель и кратных ребер. Для вершины a графа Γ через $\Gamma_i(a)$ обозначим i-окрестность вершины a, то есть, подграф, индуцированный Γ на множестве всех вершин, находящихся на расстоянии i от a. Положим $[a] = \Gamma_1(a)$.

Если вершины u, w находятся на расстоянии i в Γ, то через $b_i(u, w)$ (через $c_i(u, w)$) обозначим число вершин в пересечении $\Gamma_{i+1}(u)$ ($\Gamma_{i-1}(u)$) с $[w]$. Граф Γ диаметра d называется *дистанционно регулярным с массивом пересечений* $\{b_0, b_1, \ldots, b_{d-1}; c_1, \ldots, c_d\}$, если значения $b_i(u, w)$ и $c_i(u, w)$ не зависят от выбора вершин u, w на расстоянии i в Γ для любого $i = 0, ..., d$.

Дистанционно регулярный граф Γ с массивом пересечений $\{204, 175, 48, 1; 1, 12, 175, 204\}$ является $AT4(4, 6, 5)$-графом (см. [1]). Антиподальное частное $\bar{\Gamma}$ имеет параметры $(800, 204, 28, 60)$ и неглавные собственные значения $4, -36$, первая и вторая окрестности вершины в $\bar{\Gamma}$ сильно регулярны с параметрами $(204, 28, 2, 4)$ и $(595, 144, 18, 40)$, вторая окрестность вершины в Γ является дистанционно регулярным графом с массивом пересечений $\{144, 125, 32, 1; 1, 8, 125, 144\}$. В работе исследуются автоморфизмы сильно регулярных графов с параметрами $(204, 28, 2, 4)$ и $(595, 144, 18, 40)$.

Теорема 1. *Пусть* Γ *является сильно регулярным графом с параметрами* $(204, 28, 2, 4)$*,* $G = \mathrm{Aut}(\Gamma)$*,* g *— элемент из* G *простого порядка* p *и* $\Omega = \mathrm{Fix}(g)$*. Тогда* $\pi(G) \subseteq \{2, 3, 5, 7, 17\}$ *и выполняется одно из следующих утверждений:*

(1) Ω — *пустой граф,* $p = 2, 3, 17$*;*
(2) Ω *является* n*-кликой, либо* $n = 1$*,* $p = 7$*, либо* $n = 4$*,* $p = 5$*;*
(3) Ω *является* l*-кокликой,* $p = 2$ *и* $l = 8, 10, ...34$*;*
(4) Ω *содержит геодезический* 2*-путь и либо*
(i) $p = 3$*,* Ω *– октаэдр, либо*
(ii) $p = 2$*, степени вершин в* Ω *равны* $2, 4, ..., 26$ *и* $|\Omega| = 4, 6, ..., 34$.

Следствие. *Сильно регулярный граф с с параметрами* $(204, 28, 2, 4)$ *не является вершинно симметричным.*

Теорема 2. *Пусть* Γ *является сильно регулярным графом с параметрами* $(595, 144, 18, 40)$*,* $G = \mathrm{Aut}(\Gamma)$*,* g *— элемент из* G *простого порядка* p *и* $\Omega = \mathrm{Fix}(g)$*. Тогда* $\pi(G) \subseteq \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}$ *и выполняется одно из следующих утверждений:*
(1) Ω *— пустой граф,* $p = 5, 7, 17$*;*
(2) Ω *является* n*-кликой, либо* $n = 1$*,* $p = 3$ *или* $p = 2$*, либо* $n = 5$*,* $p = 5$*;*
(3) Ω *является* l*-кокликой,* $p = 2$ *и* $l = 5, 7, ..., 91$*;*
(4) Ω *является объединением* m *изолированных* 5*-клик,* $p = 5$*,* $\alpha_1(g) = 20t - 6l + 4$ *и* $l = 8, 10, ...34$*;*
(5) Ω *содержит геодезический* 2*-путь и* $p \leq 29$.

Работа выполнена при финансовой поддержке гранта РНФ (проект 14-11-00061).

Литература

1. Махнев А. А., Падучих Д. В. *О сильно регулярных графах с собственным значением* μ *и их расширениях* // Труды Института математики и механики. 2013. Т. 19. № 3. С. 207–214.

ПЕРЕЧИСЛЕНИЕ ПОМЕЧЕННЫХ ГЕОДЕЗИЧЕСКИХ ЭЙЛЕРОВЫХ КАКТУСОВ

А.К. Мелешко

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация
akmeleshko@gmail.com

Геодезический граф – это связный граф, у которого любая пара вершин связана единственной кратчайшей цепью (геодезической) [1]. Кактусом называется связный граф, в котором нет ребер, лежащих более чем на одном простом цикле [2, С. 93]. Все блоки кактуса – ребра или простые циклы. Эйлеров граф – это связный граф, все вершины которого имеют четную степень [2, С. 22]. Эйлеровы графы являются графами без мостов [3]. Планарный граф – это граф, который можно уложить на плоскости без пересечения ребер. Два графа называются гомеоморфными, если их можно получить из одного графа с помощью последовательности подразбиений ребер.

Помеченные эйлеровы кактусы перечислены в [3]. В работе [4] перечислены помеченные геодезические кактусы.

Лемма. *Все помеченные геодезические эйлеровы кактусы – графы с нечетным числом вершин.*

Доказательство. Используем индукцию по числу блоков. Пусть геодезический эйлеров кактус состоит из одного блока. Стемпл и Уотсон [1] доказали, что граф является геодезическим планарным только тогда, когда каждый его блок – ребро, нечетный цикл или граф, гомеоморфный полному графу K_4. Так как кактусы являются планарными графами, а эйлеровы графы – графы без мостов, то блоки геодезического эйлерова кактуса – нечетные циклы. Следовательно, для геодезического эйлерова кактуса, состоящего из одного блока, лемма верна.

Допустим, что лемма верна для графа, состоящего из k блоков, $k \geq 1$, и докажем, что она верна для графа, состоящего из $k+1$ блоков. Пусть геодезический эйлеров кактус, состоящий из k блоков, имеет нечетное число вершин n. Тогда к любой вершине кактуса присоединим блок с нечетным числом вершин m и получим граф, состоящий из $k+1$ блоков. Вершина кактуса, к которой присоединили блок, будет точкой сочленения. Следовательно, геодезический эйлеров кактус, состоящий из $k+1$ блоков, имеет нечетное число вершин: $m+n-1$. Лемма доказана.

Теорема. *Пусть GE_n – число помеченных геодезических эйлеровых кактусов с n вершинами, тогда при $p \geq 1$ верна формула*

$$GE_{2p+1} = (2p)! \sum_{k=1}^{p} \frac{(2p+1)^{k-1}}{2^k k!} \binom{p-1}{k-1}. \tag{1}$$

Доказательство. Пусть C_n – число помеченных связных графов с n вершинами, а B_n – число помеченных блоков с n вершинами. Введем производящую функцию: $B(z) = \sum\limits_{n=3}^{\infty} B_n \frac{z^n}{n!}$.

В работе [5] автором было получено соотношение

$$C_n = \frac{(n-1)!}{n} [z^{-1}] \exp(nB'(z)) z^{-n},$$

где $[z^{-1}]$ – оператор формального вычета [6, С. 25].

Обозначая через $\bar{B}(z)$ экспоненциальную производящую функцию для числа блоков помеченных геодезических эйлеровых кактусов, получим

$$GE_n = \frac{(n-1)!}{n} [z^{-1}] \exp(n\bar{B}'(z)) z^{-n}.$$

Так как, согласно лемме у геодезических эйлеровых кактусов не может быть блоков с четным числом вершин, то

$$\bar{B}(z) = \sum_{n=1}^{\infty} \frac{1}{2} (2n)! \frac{z^{2n+1}}{(2n+1)!}, \bar{B}'(z) = \sum_{n=1}^{\infty} \frac{1}{2} z^{2n} = \frac{z^2}{2(1-z^2)}$$

Следовательно,

$$GE_n = \frac{(n-1)!}{n} [z^{-1}] \exp\Big(\frac{nz^2}{2(1-z)}\Big) z^{-n}.$$

Разлагая экспоненту в степенной ряд, найдем

$$GE_n = (n-1)! [z^{-1}] \sum_{k=0}^{\infty} \frac{n^{k-1} z^{2k-n}}{2^k (1-z^2)^k k!}.$$

Используя известный ряд [7, С.141]

$$(1-z)^{-r} = \sum_{m=0}^{\infty} \binom{m+k-1}{k-1} z^m,$$

получим

$$GE_n = (n-1)! [z^{-1}] \sum_{k=0}^{\infty} \sum_{m=0}^{\infty} \frac{n^{k-1} z^{2k-n+2m}}{2^k k!} \binom{m+k-1}{k-1}.$$

Найдем решение уравнения $2k+2m-n=-1$ в целых числах. Так как не существует геодезических эйлеровых кактусов с четным числом вершин, то $n=2p+1$. Тогда $2k+2m-(2p+1)=-1$ и $m=p-k$.

Вычислив вычет функции, найдем

$$GE_{2p+1} = (2p)! \sum_{k=0}^{\infty} \frac{(2p+1)^{k-1}}{2^k k!} \binom{p-1}{k-1}.$$

Учитывая, что биномиальный коэффициент обращается в нуль при $p-1 < k-1$, получим утверждение теоремы.

Автор благодарит В.А. Воблого за ценные замечания.

Литература

1. Stemple J. G., Watkins M. E. *On planar geodetic graphs* // J. Combin. Theory. 1968. Vol. 4. P. 101–117.

2. Харари Ф., Палмер Э. *Перечисление графов.* М.: Мир, 1977.

3. Воблый В. А. *Перечисление помеченных эйлеровых кактусов* // Материалы XI Международного семинара "Дискретная математика и ее приложения". М.: МГУ, 2012. С. 275–277.

4. Воблый В. А. *Перечисление помеченных геодезических планарных графов* // Математические заметки. 2015. Т. 97. № 3. С. 336–341.

5. Воблый В. А. *Об одной формуле для числа помеченных связных графов* // Дискретный анализ и исследование операций. 2012. Т. 19. №4. С. 48–59.

6. Гульден Я., Джексон Д. *Перечислительная комбинаторика.* М.: Наука, 1990.

7. Риордан Дж. *Комбинаторные тождества.* М.: Наука, 1982.

АЛГОРИТМ РАСПОЗНАВАНИЯ A_4-СТРУКТУРЫ ОДНОГО РАСШИРЕНИЯ ПОРОГОВЫХ ГРАФОВ

Ю.М. Метельский, В.А. Тимофеева

Белгосуниверситет, механико-математический факультет
Независимости 4, 220050 Минск, Беларусь
metelsky@bsu.by, varvara.timofeeva@gmail.com

В работе рассматриваются конечные неориентированные графы без петель и кратных ребер.

Определение 1. A_4-структурой графа G называется гиперграф, вершинами которого являются вершины графа G, а ребрами – все 4-элементные подмножества вершин, порождающие в G какой-либо из графов $2K_2$, C_4 или P_4.

Понятие A_4-структуры ввели Баррус и Вест [1]. Оно подсказано широко известным в теории совершенных графов понятием P_4-структуры, введенным В. Хваталом.

Исследование A_4-структур интересно в силу целого ряда соображений.

Во-первых, известно, что для ряда трудно вычислимых в общем случае параметров графа (таких как плотность, число независимости, хроматическое число и др.) в классе совершенных графов существуют полиномиальные алгоритмы их нахождения. Известно, что два графа с одинаковыми A_4-структурами либо оба совершенны, либо оба не совершенны. Тем самым, в любом классе графов, A_4-изоморфных графам из некоторого подкласса P совершенных графов, упомянутые выше параметры вычисляются за полиномиальное время. Особо стоит отметить, что класс графов, A_4-изоморфных графам из P, является расширением класса P.

Во-вторых, каждое ребро A_4-структуры графа порождает в этом графе подграф, допускающий операцию переключения. В результате применения этой операции степенная последовательность графа не меняется, хотя результат операции, вообще говоря, уже не изоморфен исходному графу. Один из центральных результатов теории степенных последовательностей утверждает, что графы с одинаковыми степенными последовательностями могут получены

один из другого с помощью некоторой цепочки переключений. Таким образом, при исследовании A_4-структур могут быть установлены новые связи между A_4-структурой и степенной последовательностью графа.

Определение 2. Граф называется пороговым, если он не содержит порожденных подграфов, изоморфных $2K_2$, C_4 или P_4.

Известно, что граф является пороговым тогда и только тогда, когда он может быть получен из одновершинного графа последовательными добавлениями доминирующих и изолированных вершин.

Поскольку A_4-структура порогового графа не содержит ребер, представляется интересным изучение A_4-структуры ближайших расширений пороговых графов. Так, в [1] исследована A_4-структура расщепляемых графов.

В данной работе в качестве расширения пороговых графов рассмотрен класс $(1,\infty)$–простых графов.

Определение 3. Граф назовем $(1,\infty)$-простым, если его можно получить из одновершинного графа с помощью последовательных операций соединения с одновершинным графом и дизъюнктного объединения с полным графом.

Авторами разработан полиномиальный алгоритм распознования A_4-структуры $(1,\infty)$–простых графов.

Литература

1. Barrus M. D., West D. B. *The A_4-structure of a graph* // J. Graph Theory. 2012. V. 71. No. 2. P. 159–175.

О СЛОЖНОСТИ РАСПОЗНАВАНИЯ ГРАФОВ ПЕРЕСЕЧЕНИЙ РЕБЕР 3-УНИФОРМНЫХ ГИПЕРГРАФОВ КРАТНОСТИ НЕ ВЫШЕ 2

Ю.М. Метельский, Р.П. Шацов

Белгосуниверситет, механико-математический факультет
Независимости 4, 220030 Минск, Беларусь
metelsky@bsu.by, roshats@gmail.com

В работе рассматриваются конечные неориентированные графы без петель и кратных ребер. *Граф пересечений ребер* $L(H)$ гиперграфа H определяется условиями:

1) вершины графа $L(H)$ биективно соответствуют ребрам гиперграфа H;

2) две вершины смежны в $L(H)$ тогда и только тогда, когда соответствующие ребра гиперграфа H пересекаются.

Гиперграф называется *k-униформным*, если каждое его ребро содержит в точности k вершин. *Кратность* гиперграфа – максимальное число его ребер, содержащих пару вершин. Класс графов пересечений ребер k-униформных гиперграфов кратности не выше m обозначим через L_k^m.

Семейство $Q = (Q_1, Q_2, \ldots, Q_p)$ клик графа G называется *покрытием* этого графа, если каждая вершина и каждое ребро содержится в некоторой клике из Q; при этом клики Q_i называются *кластерами* покрытия. Покрытие Q графа G называется *(k,m)-покрытием*, если выполняются следующие условия:

1) каждая вершина графа G входит не более чем в k кластеров покрытия Q;

2) любые два кластера из Q имеют не более чем m общих вершин.

Теорема 1 [1]. *Граф G принадлежит классу L_k^m тогда и только тогда, когда существует (k,m)-покрытие этого графа.*

Рассмотрим следующую задачу. Пусть S – множество участников некоторого мероприятия (конференции, симпозиума, съезда и т.д.), в рамках которого преполагается организовать

ряд заседаний групп его участников. При этом заданы такие и только такие пары людей из S, каждая из которых обязана участвовать хотя бы в одном заседании. А всякое $(m+1)$-элементное подмножество из S может участвовать не более чем в одном заседании. Возможно ли так организовать заседания, чтобы каждый участник заседал не более чем k раз? Обозначим через G граф, вершинами которого являются элементы из S, и две вершины смежны тогда и только тогда, когда соответствующие люди должны участвовать в совместном заседании. Очевидно, что всякое (k,m)-покрытие графа G задает способ требуемой организации мероприятия.

Известно, что задача распознавания "$G \in L_2^m$" полиномиально разрешима для каждого фиксированного $1 \le m \le \infty$ ([2 – 4]). P.Hliněný и J.Kratochvíl ([5]) доказали, что при фиксированном $k \ge 3$ задача распознавания "$G \in L_k^1$" является NP-полной. В [1] доказано, что для фиксированного $m \ge 1$ задача распознавания "$G \in L_k^m$" (k – часть входа) является NP-полной.

Нами получен следующий результат:

Теорема 2. *Задача распознавания "$G \in L_3^2$" является NP-полной.*

Идея доказательства теоремы 2 позаимствована из [5]. В частности, использована следующая версия распознавательной задачи 3-ВЫПОЛНИМОСТЬ:

Задача А. *Вход*: Множество булевых переменных $X = \{x_1, x_2, \ldots, x_n\}$ и такой набор $D = \{d_1, d_2, \ldots, d_m\}$ элементарных дизъюнкций над X, что каждая дизъюнкция d_j содержит не более трех литералов и каждая переменная x_i входит не больше, чем в три дизъюнкции из D.

Вопрос: Существует ли такая функция $t : X \to \{0,1\}$, что в точке $(t(x_1), t(x_2), \ldots, t(x_n))$ каждая элементарная дизъюнкция d_j истинна?

Известно, что задача А является NP-полной [6]. Легко видеть, что задача распознавания "$G \in L_3^2$" принадлежит классу NP. В доказательстве теоремы 2 построено полиномиальное сведение задачи А к задаче распознавания "$G \in L_3^2$". А именно, по произвольному входу задачи А построен граф F, для которого существует $(3,2)$-покрытие тогда и только тогда, когда существует требуемая функция t для соответствующего входа задачи А. Добавив к каждой вершине графа F по $k-3$ концевых ребра из теоремы 1 непосредственно получаем

Следствие. *Задача распознавания "$G \in L_k^2$" является NP-полной для фиксированного $k \ge 3$.*

Работа выполнена при финансовой поддержке Белорусского республиканского фонда фундаментальных исследований (проект №Ф15МЛД-022).

Литература

1. Glebova O., Metelsky Y., Skums P. *Krausz dimension and its generalizations in special graph classes* // Discrete Mathematics and Theoretical Computer Science. 2013. V. 15. P. 107–120.

2. Beineke L. W. *Derived graphs and digraphs* // Beitrage zur Graphentheorie. Leipzig, 1968. P. 17–33.

3. Bermond J. C., Meyer J. C. *Graphs representatif des arêtes d'un multigraphe* // J. Math. Pures et Appl. 1973. V. 52. P. 299–308.

4. Ташкинов В. А. *Характеризация реберных графов р-графов* // Тезисы докладов 5-й Всесоюзной конференции по проблемам теоретической кибернетики. Новосибирск, 1980. С. 135–137.

5. Hliněný P., Kratochvíl J. *Computational complexity of the Krausz dimension of graphs* // Lecture Notes in Computer Science. 1997. V. 1335. P. 214–228.

6. Fellows M., Kratochvíl J., Middendorf M., Pfeiffer F. *The complexity of induced minors and related problems* // Algorithmica. 1995. V. 13. P. 266–282.

О РАВЕНСТВЕ ЧИСЕЛ P_4-УПАКОВКИ И P_4-ПОКРЫТИЯ В ГРАФАХ

Д. Б. Мокеев

НИУ Высшая Школа Экономики в Нижнем Новгороде, Лаборатория Алгоритмов и Технологий Анализа Сетевых Структур, ул. Родионова, 136, 603093 Нижний Новгород, Россия;

Нижегородский Государственный Университет им. Н.И.Лобачевского, Институт Информационных Технологий, Математики и Механики, пр. Гагарина, 23, 603950 Нижний Новгород, Россия.

MokeevDB@gmail.com

Пусть $\mathcal{F}$ – множество графов. Максимальное число попарно непересекающихся порожденных подграфов графа G, принадлежащих $\mathcal{F}$, называется числом $\mathcal{F}$-упаковки графа G. Минимальное число вершин графа G, покрывающее все порожденные подграфы из $\mathcal{F}$ называется его числом $\mathcal{F}$-покрытия.

Определение 1. Кёниговым графом относительно $\mathcal{F}$ называется граф, каждый порожденный подграф которого обладает свойством: число $\mathcal{F}$-упаковки равно числу $\mathcal{F}$-покрытия. Класс всех кёниговых графов относительно множества $\mathcal{F}$ обозначаем через $\mathcal{K}(\mathcal{F})$. Если $\mathcal{F}$ состоит из единственного графа H, то будем говорить о классе Кёниговых графов относительно H и обозначать его $\mathcal{K}(H)$.

Задаче об упаковке графа посвящено немало работ, особенно её алгоритмическим аспектам (см., например, [1, 2]). Известно, что задача поиска числа H-упаковки NP-полна для любого графа H, имеющего компоненту связности с тремя или более вершинами. Будучи сформулированы как задачи ЦЛП, задачи об $\mathcal{F}$-упаковке и $\mathcal{F}$-покрытии образуют пару двойственных задач. Кёниговы графы, таким образом, суть графы, у которых для любого порождённого подграфа отсутствует разрыв двойственности, что способствует эффективному решению этих задач для таких графов.

Класс $\mathcal{K}(\mathcal{F})$ при любом $\mathcal{F}$ является наследственным и, следовательно, может быть описан множеством запрещенных графов (минимальных по отношению «быть порожденным подграфом» графов, не принадлежащих $\mathcal{F}$). Для P_2 такую характеризацию даёт теорема Кёнига вместе с известным критерием двудольности. Кроме этой классической теоремы автору известны следующие результаты такого рода для обыкновенных графов: в [3] эта задача решена для класса $\mathcal{K}(P_3)$; в [4] – для класса $\mathcal{K}(\mathcal{C})$, где $\mathcal{C}$ – множество всех простых циклов.

Цель настоящей работы – охарактеризовать класс графов $\mathcal{K}(P_4)$. Применяется два подхода к описанию этого класса. Один из них – конструктивный: показано, как можно построить графы данного класса с помощью процедуры расширенного подразбиения. Второй подход – стандартное описание наследственного класса запрещёнными подграфами.

Определение 2. Будем называть связный граф G P_4-связным, если его дополнение связно и через каждую его вершину проходит хотя бы один порождённый 4-путь.

Лемма 1. *Граф является кёниговым тогда и только тогда, когда каждый его максимальный по включению P_4-связный подграф кёнигов.*

Операция замены кографом вершины x состоит в следующем: эта вершина удаляется из графа; к графу добавляются несколько новых вершин, и каждая из них соединяется ребром с каждой вершиной, смежной x в исходном графе; новые вершины соединены между собой так, что образуют кограф.

Определение 3. Назовём путь графа висячим, если степень одной из его вершин 1, а остальных – не более 2. Контактной вершиной висячего пути назовём вершину графа, смежную одной из вершин пути, но ему не принадлежащую (если такая имеется, то она единственная).

Операция замены кографом висячего пути из 3 вершин состоит в следующем: вершины этого пути удаляются из графа; к графу добавляется несколько новых вершин, соединённых

между собой так, что образуют кограф; новые вершины соединены с контактной вершиной так, чтобы максимальный путь, содержащий контактную и добавленные вершины имел длину 3.

Операция замены кографом висячего пути из 2 вершин состоит в следующем: вершины этого пути удаляются из графа; к графу добавляются вершины $k_1, k_2, \ldots, k_p$, которые соединены попарно между собой и соединены с контактной вершиной; к графу добавляются вершины $l_1, l_2, \ldots, l_{p-1}$ и, быть может, l_p, причём $N(l_i) = \{k_1, k_2, \ldots, k_i\}$; каждую добавленную вершину, а так же контактную вершину, если её степень в исходной графе равна 2, можно заменить кографом произвольной структуры.

Пусть H – двудольный граф. Каждое ребро этого графа, принадлежащее какому-нибудь циклу, подразобьём одной вершиной. Заменим произвольными кографами некоторые вершины степени 1 и 2, при этом если в цикле графа H есть вершина v, смежная с 3 и более вершинами степени больше 1, то вершины 4-класса, содержащего v, не могут быть заменены кографами, а так же если в цикле графа H есть вершина v степени 3 и более, то вершина 4-класса, содержащего v и вершина 4-класса, содержащего вершину, отстоящую на расстоянии 2 от v, не могут быть заменены кографами одновременно. Последним шагом заменим кографами некоторые висячие пути из 2 и 3 вершин. Будем говорить, что результирующий граф получен DQ-преобразованием двудольного графа H.

Обозначим $\mathcal{A}$ множество графов и дополнений графов, полученных из цикла длины кратной 4 добавлением двух вершин, не смежных между собой, каждая из которых соединяется ребром с одной вершиной цикла, причём расстояние между добавленными вершинами нечётно.

Обозначим $\mathcal{B}$ множество графов и дополнений графов, полученных из цикла длины кратной 4 добавлением висячего пути длины 2, смежного с вершиной с номером 0 и заменой кографом из двух вершин вершины цикла с номером $4k, k \in \mathbb{N}$, а так же полученных из цикла длины кратной 4 добавлением вершины, смежной с вершиной с номером 0 и заменой кографами из двух вершин вершин цикла с номерами $4k, k \in \mathbb{N}$ и $4l + 2, l \in \mathbb{N} \cup \{0\}$.

Обозначим $\mathcal{C}$ множество циклов и их дополнений с числом вершин не менее 5 и не кратным 4.

Обозначим $\mathcal{D}$ множество графов и дополнений графов, полученных из цикла длины $k_1 + k_2 + k_3 + k_4$ заменой кографами из двух вершин вершин с номерами $0, k_1, k_1 + k_2, k_1 + k_2 + k_3$, причём $k_1 \equiv k_2 \equiv k_3 \equiv k_4 \equiv 1 \pmod 4, k_i \geq 5, i = 2, 3, 4$ или $k_1 \equiv 1 \pmod 4, k_1 \geq 5, k_2 \equiv k_4 \equiv 2 \pmod 4, k_3 \equiv 3 \pmod 4$.

Обозначим $\mathcal{E}$ множество минимальных запрещённых графов из 6 и 7 вершин, не входящих в $\mathcal{A} \cup \mathcal{C}$. Таких графов ровно 64.

Теорема 1. *P_4-связный граф является кёниговым тогда и только тогда, когда может быть получен DQ-преобразованием двудольного графа и не содержит порождённых подграфов из множества $\mathcal{D}$.*

Теорема 2. *Графы множества $\mathcal{A} \cup \mathcal{B} \cup \mathcal{C} \cup \mathcal{D} \cup \mathcal{E}$ составляют множество минимальных запрещённых графов для класса $\mathcal{K}(P_4)$.*

Работа выполнена при финансовой поддержке лаборатории ЛАТАС, НИУ ВШЭ (грант правительства ag. 11.G34.31.0057; РФФИ, проект № 14-01-00515-а).

Литература

1. Hell P. *Graph packing* // Electronic Notes in Discrete Mathematics. 2000. V. 5. P. 170–173.

2. Yuster R. *Combinatorial and computational aspects of graph packing and graph decomposition* // Computer Science Review. 2007. V. 1. P. 12–26.

3. Алексеев В. Е., Мокеев Д. Б. *Кёниговы графы относительно 3-пути* // Дискретный анализ и исследование операций. 2012. № 19 (4). С. 3–14.

4. Ding G., Xu Z., Zang W. *Packing cycles in graphs, II* // J. Comb. Theory. B,. 2003. V. 87. P. 244–253.

ИСПОЛЬЗОВАНИЕ ТЕОРИИ МНОЖЕСТВ ПРИ ФОРМАЛЬНОМ ОПИСАНИИ КЛАССОВ ПРЕДМЕТНОЙ ОБЛАСТЕЙ В ПОНЯТИЯХ МЕТАМОДЕЛИ ОБЪЕКТНОЙ СИСТЕМЫ

П.П. Олейник

к.т.н, системный архитектор программного обеспечения, ОАО «Астон»
доцент, Шахтинский институт (филиал) Южно-Российского государственного политехнического университета им. М.И. Платова, Россия, Ростов-на-Дону
xsl@list.ru

В настоящее время доминирующей методологией, используемой при разработке приложений, является объектно-ориентированный подход. В данной статье представлен формальный математический аппарат, основанный на теории множеств и позволяющий описать объектную модель любой предметной области. Основой для разрабатываемого подхода является метамодель, используемая в унифицированной среде быстрой разработки корпоративных информационных систем SharpArchitect RAD Studio [1]. В работах [2-8] была представлена полная диаграмма классов метамодели и подробно описано назначение классов, а также её эволюция и расширение. На рис. 1 представлен фрагмент метамодели с отображением ключевых ассоциаций, важных для дальнейшего обсуждения.

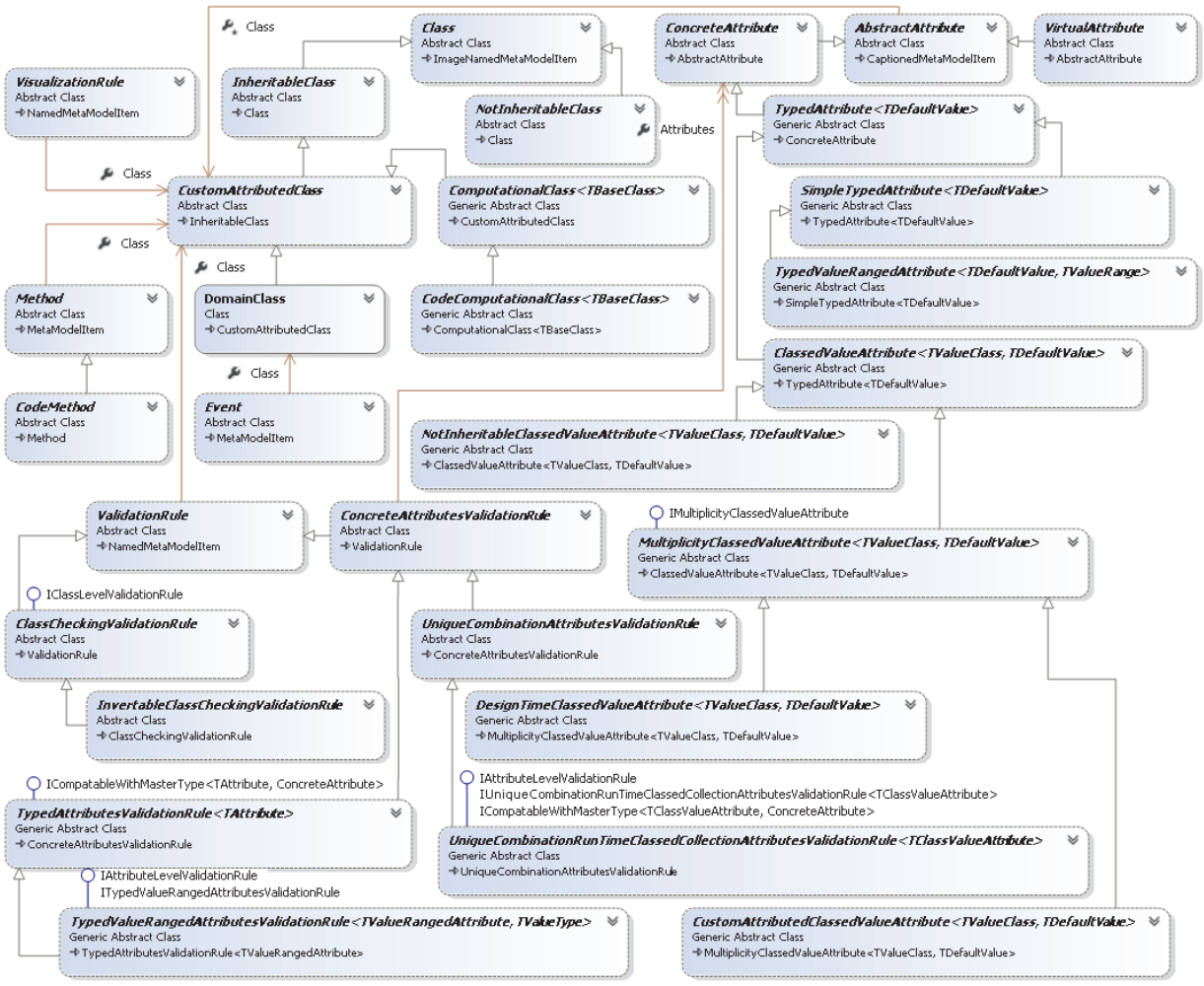


Рис. 1. Фрагмент унифицированной метамодели объектной системы

Опыт показал, что при проектировании ИС больше всего выделяют сохраняемых сущностей, которые в нашем случае описываются метаклассом DomainClass, представляющем классы предметной области (КПО). В общем случае для описания всех классов предметной области (DC) используется множество, элементами которых является вектора и описываемое как (2):

$$DC = < ATT, BCdc, M, E, VLR, VSR, BHC, R > \quad (1)$$

где элементы вектора каждого КПО заданы следующим образом:
ATT (Attribute) – множество атрибутов класса предметной области;
BCdc (BaseClass)– множество базовых классов предметной области, от которого унаследован данный;
M (Method) – множество методов класса, позволяющих реализовать поведение экземпляров классов, т.е. динамическую составляющую;
E (Event) – множество обработчиков событий, возникающих в жизненном цикле объекта класса предметной области;
VLR (ValidationRule) – множество предикатов, представляющих валидационные правила, которым должен отвечать каждый объект;
VSR (VisualizationRule) – множество визуализационных правил, которые управляют видимостью, доступность, цветом отдельных атрибутов;
BHC (BehaviorController) – множество контроллеров поведения, позволяющих управлять как поведением объектов, так и пользовательским интерфейсом приложения;
R (Report) – множество отчетов системы, позволяющие выводить экземпляры класса (объекта) в удобном для пользователя виде с возможностью распечатки данных.

Представленный подход использовался автором многократно при формальном описании различных прикладных областей, которые подробно описаны в работах [5, 8].

Литература

1. Олейник П.П., программа для ЭВМ «*Унифицированная среда быстрой разработки корпоративных информационных систем SharpArchitect RAD Studio*», свидетельство о государственной регистрации № 2013618212 от 04 сентября 2013 г.

2. Олейник П.П. *Иерархия классов метамодели объектной системы* // Объектные системы – 2012: материалы VI Международной научно-практической конференции (Ростов-на-Дону, 10-12 мая 2012 г.) / Под общ. ред. П.П. Олейника. – Ростов-на-Дону: ШИ ЮРГТУ (НПИ), 2012. – С. 37-40.

3. Олейник П.П. *Иерархия классов представления валидационных правил объектной системы* // Объектные системы – 2013: материалы VII Международной научно-практической конференции (Ростов-на-Дону, 10-12 мая 2013 г.) / Под общ. ред. П.П. Олейника. – Ростов-на-Дону: ШИ (ф) ЮРГТУ (НПИ), 2013. – С. 14-17.

4. Oleynik P.P. *Domain-driven design the database structure in terms of metamodel of object system.* Proceedings of 11th IEEE East-West Design & Test Symposium (EWDTS'2013), Institute of Electrical and Electronics Engineers (IEEE), Rostov-on-Don, Russia, September 27 – 30, 2013, pp. 469-472.

5. Олейник П.П. *Элементы среды разработки программных комплексов на основе организации метамодели объектной системы* // Бизнес-информатика. 2013. №4(26). – С. 69-76.

6. Олейник П.П. *Предметно-ориентированное проектирование структуры базы данных в понятиях метамодели объектной системы* // Объектные системы – 2014: материалы VIII Международной научно-практической конференции (Ростов-на-Дону, 10-12 мая 2014 г.) / Под общ. ред. П.П. Олейника. – Ростов-на-Дону: ШИ (ф) ЮРГПУ (НПИ) им. М.И. Платова, 2014. - С. 41-46.

7. Oleynik P.P. *Using metamodel of object system for domain-driven design the database structure.* Proceedings of 12th IEEE East-West Design & Test Symposium (EWDTS'2014), Kiev, Ukraine, September 26 – 29, 2014, DOI: 10.1109/EWDTS.2014.7027052

8. Олейник П.П., Кураков Ю.И. *Концепция создания обслуживающей корпоративной информационной системы экономического производственно-энергетического кластера* // Прикладная информатика. 2014. №6. - С. 5-23.

КОЛИЧЕСТВО СОВЕРШЕННЫХ ПАРОСОЧЕТАНИЙ НА ТРЕУГОЛЬНЫХ РЕШЕТКАХ ФИКСИРОВАННОЙ ШИРИНЫ

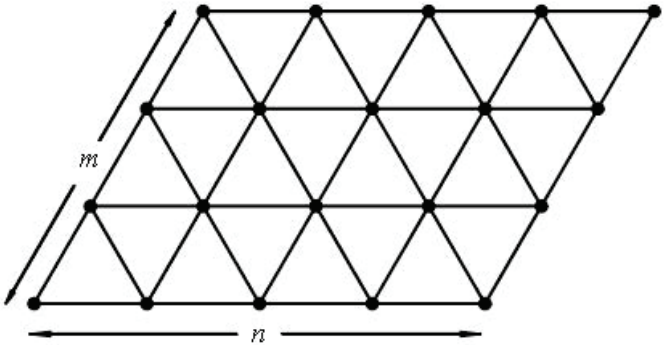
С.Н. Перепечко

Петрозаводский государственный университет
Ленина 33, 185910 Петрозаводск, Россия persn@newmail.ru

Проблема подсчёта совершенных паросочетаний (в дальнейшем просто паросочетаний) в некотором семействе графов тесно связана с одной из классических решёточных моделей статистической механики — так называемой *задачей о димерах*. При равенстве активностей всех димеров производящая функция для числа паросочетаний становится идентичной производящей функции в модели димеров.

В силу исторически сложившихся обстоятельств в физических приложениях наибольший интерес вызывают двухпараметрические семейства планарных решёточных графов. Формально для таких графов задача подсчёта сводится к вычислению пфаффиана. Однако его вычисление в символьном виде наталкивается на серьёзные трудности, и немногочисленные разрешимые случаи приводят к громоздким выражениям в виде двойных произведений, анализ которых оказывается чрезвычайно сложным. С вычислительной точки зрения эффективность подобного рода формул также оставляет желать лучшего. Выполнять расчёты за разумное время можно только в графах небольшого или умеренного порядка. В сложившейся ситуации представляет интерес изучение альтернативных методов подсчёта, позволяющих проводить как точные, так и приближённые вычисления в больших графах.

Данное сообщение посвящено обсуждению подхода, основанного на сведении двухпараметрической задачи к набору однопараметрических задач. В качестве графов рассматриваются, как показано на рисунке, фрагменты треугольной решётки в форме параллелограмма. Будем обозначать графы указанного семейства символом $\mathbf{T}_{m,n}$. Неослабевающий интерес к этому семейству обусловлен, прежде всего, тем, что способ построения пфаффовой ориентации в $\mathbf{T}_{m,n}$ известен уже более полувека [1], однако предпринимавшиеся ранее попытки получить выражения, пригодные для проведения расчётов, к успеху не приводили. Сравнительно недавно был достигнут существенный прогресс в исследовании родственной модели, соответствующей укладке треугольной решётки на поверхность тора [2, 3]. В то же время для числа паросочетаний в $\mathbf{T}_{m,n}$, возникающих в задаче со свободными граничными условиями, известен лишь незначительный набор числовых данных при небольших значениях m и n.



В ходе решения перечислительной задачи параметр m, называемый шириной решётки, фиксировался, и вычислялось количество паросочетаний в $\mathbf{T}_{m,n}$ при различных n. Поскольку в графах нечётного порядка отсутствуют совершенные паросочетания, то можно обозначить одним и тем же символом $K_{m,n}$ число паросочетаний в $\mathbf{T}_{m,n}$ при чётных значениях m и в графах $\mathbf{T}_{m,2n}$ при нечётных m. По общепринятому соглашению $K_{m,0} = 1$.

При фиксированном m последовательность $\{K_{m,n}\} = K_{m,0}, K_{m,1}, K_{m,2}, \ldots$ является монотонно возрастающей и удовлетворяет линейному рекуррентному соотношению с постоянными коэффициентами. Поскольку для треугольной решётки можно построить матрицу переноса, применив аналогичную [4] схему кодирования состояний, то существование такого соотношения вытекает из теоремы Кэли-Гамильтона. В терминах производящих функций

$G_m(z) = \sum_{n=0}^{\infty} K_{m,n} z^n$ данное обстоятельство соответствует тому, что $G_m(z) = P_m(z)/Q_m(z)$ рациональны. При выводе $G_m(z)$ использовалось условие нормировки $Q_m(0) = 1$.

Для $2 \leqslant m \leqslant 11$ были вычислены достаточно длинные начальные отрезки последовательностей $\{K_{m,n}\}$, из которых удалось восстановить как сами рекуррентные соотношения, так и ассоциированные с ними $G_m(z)$. Несколько простейших примеров приведены ниже:

$$G_3(z) = \frac{1 - 4z + z^2}{(1 - z)(1 - 6z + z^2)},$$
$$G_4(z) = \frac{(1 - z)(1 + z)(1 - z - 5z^2 - z^3 + z^4)}{(1 + z - 3z^2 - 3z^3 + z^4)(1 - 3z - 3z^2 + z^3 + z^4)}.$$

Порядки рекуррентных соотношений в рассматриваемой модели существенно зависят от чётности ширины решётки и во всех изученных случаях оказались равными 2^{m-1} при чётных значениях m и $3^{\lfloor m/2 \rfloor}$ при нечётных.

Свойства $P_m(z)$ и $Q_m(z)$ близки, либо совпадают со свойствами аналогичных полиномов в семействе прямоугольных решёток вида $P_m \times P_n$ [5]. В частности, $q_m - p_m = 1$ при нечётных m и равно 2 при чётных, где $q_m = \deg Q_m(z)$, $p_m = \deg P_m(z)$. Симметрия коэффициентов рекуррентного соотношения приводит к равенствам $Q_m(z) = -z^{q_m} Q_m(1/z)$, $P_m(z) = z^{p_m} P_m(1/z)$, которые имеют место при нечётных m. В то же время при выполнении условия $m \bmod 4 = 0$ знаменатели $Q_m(z)$ удовлетворяют несколько иному соотношению: $Q_m(z) = z^{q_m} Q_m(1/z)$. Все найденные в ходе выполнения работы $Q_m(z)$ оказались приводимы в $\mathbb{Z}[z]$. Для решёток $P_m \times P_n$ подобная ситуация наблюдается только в исключительных случаях.

Для вывода рекуррентного соотношения длина начального известного отрезка последовательности $\{K_{m,n}\}$ должна, по крайней мере, в 2 раза превышать порядок соотношения. По причине экспоненциального роста порядка подсчёт паросочетаний оказывается весьма трудоёмким. Так, например, при $m = 12$ необходимо найти паросочетания во всех графах вплоть до $\mathbf{T}_{12,4096}$. Поскольку расчёты выполнялись в системе компьютерной алгебры Maple, то при $12 \leqslant m \leqslant 25$ вычислялись элементы $K_{m,n}$ для $n \leqslant n^*$. При чётных m в качестве n^* выбиралось значение 300. В нечётном случае можно было положить $n^* = 200$. Полученных данных оказалось достаточно, чтобы с высокой точностью оценить асимптотику $K_{m,n}$ при $n \to \infty$, которая имеет следующий вид: $K_{m,n} \sim C(m)\lambda(m)^n$.

В результате применения экстраполяционных методов ускорения сходимости к набору $\lambda(m)$ удалось вычислить «молекулярную свободу» — один из важнейших параметров решёточной модели. С погрешностью, не превышающей единицу последнего удержанного разряда, полученное значение оказалось равным 2,356 527 3. Использованный в работе подход является первым систематическим методом оценки данного параметра в моделях со свободными граничными условиями. Ранее известные методы существенно опирались на свойство регулярности исследуемых графов.

Литература

1. Montroll E. W. *Lattice statistics* // Applied Combinatorial Mathematics, ed.: E. F. Beckenbach. John Wiley ans Sons, 1964. P. 96–143.

2. Fendley P., Moessner R., Sondhi S. L. *Classical dimers on the triangular lattice* // Physical Review B. 2002. V. 66. Art. 214513.

3. Izmailian N. Sh., Oganesyan K. B., Wu M-C., Hu C-K. *Finite-size corrections and scaling for the triangular lattice dimer model with periodic boundary conditions* // Physical Review E. 2006. V. 73. Art. 016128.

4. Караваев А. М., Перепечко С. Н. *Подсчёт гамильтоновых циклов на треугольных решётках* // Материалы IV международной конференции “Моделирование-2012”, Киев. 2012. С. 383–386.

5. Караваев А. М., Перепечко С. Н. *Производящие функции в задаче о димерах на прямоугольных сеточных графах* // Информационные процессы. 2013. Т. 13. №4. С. 374–400.

О ПРИЛОЖЕНИИ ТЕОРИИ ФУНКЦИОНАЛЬНЫХ СИСТЕМ К НЕКОТОРЫМ ПРОБЛЕМАМ ТЕОРИИ КОЛЛЕКТИВНОГО ВЫБОРА

Н.Л. Поляков

Финансовый Университет при Правительстве РФ
Щербаковская 38, 105187 Москва, РФ gelvella@mail.ru

Введение. *Теория коллективного выбора* (social choice theory) изучает различные методы агрегирования коллективных предпочтений по профилям индивидуальных предпочтений. Классическим результатом теории коллективного выбора является известная *теорема Эрроу о невозможности*, см. [1-2]. Эта теорема утверждает, что не существует процедуры агрегирования рациональных предпочтений, обладающей некоторыми естественными свойствами. В работе [3] С. Шелах установил, что принцип невозможности Эрроу может быть распространен на нерациональные предпочтения при некоторых дополнительных условиях. Доказательство основной теоремы работы [3] использует понятия теории функциональных систем; в т.н. простом случае оно может быть проинтерпретировано как описание фрагмента *соответствия Галуа для классов дискретных функций* (о соответствии Галуа (inv, pol) для классов дискретных функций см. [4]). Подход С. Шелаха оказывается весьма плодотворным и может претендовать на роль одного из универсальных методов абстрактной теории коллективного выбора. С помощью модификации этого подхода была установлена полная классификация симметричных классов r-функций выбора, обладающих *свойством Эрроу*, см. [5]. Одновременно этот подход позволяет легко получить некоторые позитивные результаты (*теоремы о возможности*) в случае т.н. ограниченных областей (restricted domains). В настоящей работе мы приводим полное описание множества клонов простых правил агрегирования, которые сохраняют какое-либо симметричное множество *решающих правил*. Заметим, что для каждого клона $\mathcal{F}$ из этого множества можно дать несложное описание множества $\operatorname{inv}\mathcal{F}$, что позволяет еще шире распространить принцип Эрроу, а также обнаружить некоторые "патологические" случаи его нарушения.

Базовые понятия. Пусть даны конечные множества Q (условий), A (решений) и $\mathbb{C} \subseteq A^Q$ (решающих правил). В типичной ситуации множество Q есть множество всех непустых подмножеств множества A (или множество $[A]^2$ неупорядоченных пар элементов множества A), а $\mathbb{C}$ есть множество всех функций выбора (или, соответственно, их ограничений на $[A]^2$). В более общей ситуации в качестве $\mathbb{C}$ можно рассматривать множество функций выбора на мультимножествах или на подмножествах множества A, обогащенных некоторой дополнительной структурой.

Множество $\mathbb{C}$ называется *симметричным*, если для каждой перестановки σ множества A существует такая перестановка σ^* множества Q, что вместе с каждой функцией h множество $\mathbb{C}$ содержит функцию h_σ, определенную равенствами

$$h_\sigma(q) = \sigma^{-1}h(\sigma^* q)$$

для всех $q \in Q$ (свойство симметричности играет роль замкнутости относительно изоморфизмов).

Пусть дано натуральное число n (участников голосования или критериев). (Простое) *правило агрегирования* это любая функция $f\colon A^n \to A$, удовлетворяющая условию *консервативности* (иначе, *квазитривиальности*)

$$(\forall x_1, x_2, \ldots, x_n \in A) \bigvee_{1\le i\le n} f(x_1, x_2, \ldots x_n) = x_i$$

(о правилах агрегирования более общего вида см. [3,5]).

Правило агрегирования f *сохраняет множество* $\mathbb{C}$, если для каждого $(h_1, h_2, \dots, h_n) \in \mathbb{C}^n$ множество $\mathbb{C}$ содержит функцию $f(h_1, h_2, \dots, h_n)$.

Легко проверить, что отношение сохранения функцией f (произвольной арности) на множестве A множества $\mathbb{C} \subseteq A^Q$ в естественном смысле порождает соответствие Галуа между булевыми решетками $\mathcal{P}(\bigcup\limits_{n<\omega} A^{A^n})$ и $\mathcal{P}(\mathcal{P}(A^Q))$. Это соответствие можно рассматривать как фрагмент соответствия $(\mathrm{inv}, \mathrm{pol})$ (см. [4]), если каждое множество $\mathbb{C} \subseteq A^Q$ отождествить с предикатом $\{(h(q_1), h(q_2), \dots, h(q_m))\colon h \in \mathbb{C}\}$, где $m = |Q|$ и $(q_i)_{i\le m}$ есть фиксированная нумерация множества Q. Из этого, в частности, вытекает, что множество правил агрегирования, которые сохраняют некоторое множество $\mathbb{C}$, замкнуто относительно композиции и содержит все проекции, т.е. есть *клон*. Клон всех (простых) правил агрегирования, которые сохраняют множество $\mathbb{C}$, обозначим символом $\mathrm{Av}\,\mathbb{C}$. Следующая теорема дает эффективное описание множества $\{\mathrm{Av}\,\mathbb{C}\colon \mathbb{C}$ симметрично$\}$.

Основная теорема. Вначале мы определим некоторые специальные клоны правил агрегирования. Множество всех правил агрегирования обозначим символом Av. Для каждого натурального числа r символом $A^{<\omega}_{<r}$ обозначим множество $\{\mathbf{a} \in A^{<\omega}\colon |\operatorname{ran}\mathbf{a}| < r\}$.

Клоны E_r**.** Для каждого натурального числа $r \ge 2$ символом E_r обозначим множество всех функций $f \in \mathrm{Av}$, которые совпадают с некоторой проекцией на множестве $A^{<\omega}_{<r}$.

Клоны M_m**.** Для каждого натурального числа $m \ge 2$ символом M_m обозначим множество всех функций $f \in \mathrm{Av}$, которые удовлетворяют условию

$$(f(\mathbf{a}) = a \wedge \{i \in \operatorname{dom}\mathbf{a}\colon a_i = a\} \subseteq \{i \in \operatorname{dom}\mathbf{b}\colon b_i = b\}) \to f(\mathbf{b}) = b$$

для всех $\mathbf{a} \in A^{<\omega}_{<3}$, $\mathbf{b} \in A^{<\omega}_{<m}$ $(\operatorname{dom}\mathbf{a} = \operatorname{dom}\mathbf{b})$, $a \in \operatorname{ran}\mathbf{a}$, $b \in \operatorname{ran}\mathbf{b}$.

Клоны F_R**.** Бинарное отношение R на множестве $A^{<\omega}$ называется *устойчивым*, если

1. $\mathbf{a}\,R\,\mathbf{b} \to \mathbf{a} = \sigma\mathbf{b}$ для некоторой перестановки σ множества A;
2. $\mathbf{a}\,R\,\mathbf{b} \to \sigma\mathbf{a}\pi = \sigma\mathbf{b}\pi$ для любой перестановки σ множества A, натурального числа k и функции $\pi\colon \{1, 2, \dots, k\} \to \operatorname{dom}\mathbf{a}$.

Для каждого устойчивого отношения отношения эквивалентности R на множестве $A^{<\omega}$ символом F_R обозначим множество всех функций $f \in \mathrm{Av}$, которые совпадают с некоторой проекцией на каждом классе эквивалентности отношения R.

Клоны P_Π**.** Пусть Π есть один из Постовских классов, который состоит из функций, сохраняющих $\mathbf{0}$ и $\mathbf{1}$, и замкнут относительно двойственности. Для каждого двухэлементного множества B обозначим символом Π_B клон с носителем B, эквивалентный Постовскому классу Π. Символом P_Π обозначим множество всех функций $f \in \mathrm{Av}$, удовлетворяющих условию $f \restriction B^{<\omega} \in \Pi_B$ для всех $B \in [A]^2$.

Теорема 1. *Пусть дано симметричное множество* $\mathbb{C} \subseteq A^Q$ *(решающих правил). Тогда существуют такие натуральные числа* $m, r \ge 2$*, устойчивое отношение эквивалентности* R *на множестве* $A^{<\omega}$ *и замкнутый относительно двойственности Постовский класс* $\Pi \subseteq T_{01}$*, что*

$$\mathrm{Av}\,\mathbb{C} = \mathrm{E}_r \cap \mathrm{M}_m \cap \mathrm{F}_R \cap \mathrm{P}_\Pi.$$

Литература

1. Arrow K. *Social Choice and Individual Values.* 2 edition. Yale University Press: 1963.

2. Geanakoplos J. *Three Brief Proofs of Arrow's Impossibility Theorem* // Economic Theory. 2005. V. 26. №. 1. P. 211–215.

3. Shelah S. *On the Arrow property* // Advances in Applied Mathematics. 2005. V. 34. P. 217–251.

4. Боднарчук В. Г., Калужнин Л. А., Котов В. Н., Ромов Б. А. *Теория Галуа для алгебр Поста* // Кибернетика. 1969. Т 3. С. 1-10. Т.5. С. 1–9.

5. Поляков Н. Л., Шамолин М. В. *Об одном обобщении теоремы Эрроу* // Докл. РАН. 2014. Т. 456. № 2. С. 143–145.

ПОИСК РАЗРЕЗА ГРАФА, ИСПОЛЬЗУЕМЫЙ В РЕШЕНИИ НЕКОТОРЫХ ЗАДАЧ ЛОГИЧЕСКОГО ПРОЕКТИРОВАНИЯ

Ю.В. Поттосин[1], **С.А. Поттосина**[2]

[1]Объединенный институт проблем информатики НАН Беларуси,
Сурганова 6, 220012 Минск, Беларусь pott@newman.bas-net.by
[2]Белорусский государственный университет информатики и радиоэлектроники,
П.Бровки 6, 220013 Минск, Беларусь s.pottosina@gmail.com

Согласно [1], для графа $G = (V, E)$ с множеством вершин V и множеством ребер E и некоторых непересекающихся подмножеств A и B множества V разрезом называется множество ребер, одни концы которых лежат в A, другие — в B. Рассматривается задача нахождения максимального разреза в графе, ребра которого взвешены действительными числами, т. е. такого разреза, у которого сумма весов ребер максимальна.

Одной из важных задач логического проектирования является задача декомпозиции булевых функций. Рассмотрим эту задачу в следующей постановке [2]. Для системы полностью определенных булевых функций $\mathbf{y} = f(\mathbf{x})$, где $\mathbf{y} = (y_1, y_2, ..., y_m)$, $\mathbf{x} = (x_1, x_2, ..., x_l)$, $f(\mathbf{x}) = (f_1(\mathbf{x}), f_2(\mathbf{x}), ..., f_m(\mathbf{x}))$, требуется найти суперпозицию $\mathbf{y} = \phi(\mathbf{w}, \mathbf{z_2})$, $\mathbf{w} = \mathbf{g}(\mathbf{z_1})$, где $\mathbf{z_1}$ и $\mathbf{z_2}$ — векторные переменные, компонентами которых служат соответственно переменные из подмножеств Z_1 и Z_2, образующих разбиение множества $X = \{x_1, x_2, ..., x_l\}$. При этом число компонент векторной переменной $\mathbf{w}$ должно быть меньше, чем у переменной $\mathbf{z_1}$. К этому требованию добавим еще то, чтобы функции $\phi(\mathbf{w}, \mathbf{z_2})$ и $\mathbf{g}(\mathbf{z_1})$ были как можно более простыми.

Табличный метод декомпозиции [3] предусматривает представление исходной системы булевых функций в виде двумерной таблицы M, столбцам которой соответствуют множества значений переменной $\mathbf{z_1}$, а строкам — множества значений переменной $\mathbf{z_2}$. Приписав различным столбцам таблицы M различные булевы векторы, получим функцию $\mathbf{w} = \mathbf{g}(\mathbf{z_1})$, значениями которой являются указанные векторы. Сложность функций $\phi(\mathbf{w}, \mathbf{z_2})$ и $\mathbf{g}(\mathbf{z_1})$ сильно зависит от варианта такого кодирования.

В работе [4] предлагается метод кодирования столбцов таблицы M, целью которого является упрощение функций $\phi(\mathbf{w}, \mathbf{z_2})$ и $\mathbf{g}(\mathbf{z_1})$. Метод представляет собой многошаговый процесс, на каждом i-м шаге которого вводится переменная w_i, являющаяся компонентой вектора $\mathbf{w}$, и определяются ее значения. Для этого строится полный граф $G = (V, E)$ и на парах различных столбцов таблицы M задается целочисленная функция h, значения которой определяются следующим образом. Если каждый столбец таблицы M рассматривать как булев вектор размерности sm, где s — число строк таблицы M, то расстояние по Хэммингу между i-м и j-м столбцами является значением функции h на данной паре столбцов. Вершинам графа G соответствуют столбцы таблицы M, а ребрам приписываются веса в виде соответствующих значений функции h.

На i-м шаге упомянутого процесса находится максимальный разрез графа G, представляемый парой подмножеств A, B множества V, и переменная w_i, получает значение 0 (или 1) для столбцов, соответствующих вершинам из A, и значение 1 (или 0) для столбцов, соответствующих вершинам из множества B. Для поиска разреза используется „жадный“ алгоритм из статьи [5]. Затем удаляются ребра, соединяющие вершины из A с вершинами из B, и выполняется следующий, $(j + 1)$-й шаг. Процесс заканчивается, когда граф G становится пустым. Использование функции h указанного вида способствует увеличению возможности склеивания элементарных конъюнкций в дизъюнктивных нормальных формах функций $\phi(\mathbf{w}, \mathbf{z_2})$ и $\mathbf{g}(\mathbf{z_1})$.

Другой задачей, где может быть использован поиск максимального разреза, является задача кодирования состояний дискретного автомата. Одной из моделей поведения дискретного устройства является конечный автомат, который состоит из множества входных сигналов

A, множества выходных сигналов B, множества состояний Q и двух функций — функции выходов $\Phi(a,q)=b$ и функции переходов $\Psi(a,q)=q^+$, где $a\in A,\ \ b\in B,\quad q,q^+\in Q$ и q^+ является состоянием, в которое автомат переходит из состояния q при входном сигнале a.

В процессе синтеза логической схемы функции Φ и Ψ преобразуются в систему булевых функций посредством замены абстрактных символов a, b и q булевыми векторами. В функциональном описании синтезируемой схемы часто входы и выходы уже представлены в виде булевых векторов. Задача заключается в том, чтобы приписать абстрактным символам состояний q булевы векторы $\mathbf{z}=(z_1,z_2,...,z_k)$ в соответствии с некоторым критерием оптимизации. В этом случае любое состояние автомата будет представлено в схеме набором состояний двоичных элементов памяти (триггеров), где состояние i-го триггера представляет собой значение внутренней переменной z_i. Булев вектор $\mathbf{z}$, приписанный состоянию автомата, называется кодом состояния.

В случае синхронной реализации автомата при кодировании состояний обычно преследуется следующие цели: получение как можно более простой системы булевых функций, описывающей комбинационную часть проектируемого устройства [2], или уменьшение интенсивности переключений элементов памяти [6]. Последнее ведет к уменьшению потребляемой энергии проектируемой схемой. Предлагается следующий метод энергосберегающего кодирования состояний автомата, использующий поиск максимального разреза в графе.

Рассматриваются вероятности переходов между состояниями, и чем больше вероятность перехода для какой-то пары состояний, тем меньше должно быть по возможности компонент в кодах этих состояний, которые имеют различные значения, не важно, в каком направлении происходит переход. Значения внутренних переменных $z_1,z_2,...,z_k$ определяются следующим образом.

Реализуется такой же многошаговый процесс, как в предыдущей задаче. Текущая ситуация в этом процессе характеризуется частичными кодами состояний $(z_1,z_2,...,z_j)$, $j<k$, и взвешенным графом $G=(V,E)$, вершины которого соответствуют состояниям автомата. Две вершины этого графа связаны ребром, если и только если соответствующие состояния имеют один и тот же частичный код. Каждое ребро $\nu_s\nu_t\in E$ имеет вес $h_{st}=1-p^*_{st}$, где p^*_{st} — вероятность перехода между состояниями q_s и q_t, соответствующими вершинам ν_s и ν_t, независимо от направления перехода, т. е. $p^*_{st}=p_{st}+p_{ts}$, где p_{st} — вероятность перехода из состояния q_s в состояние q_t. На каждом шаге находится максимальный разрез, определяются значения очередной переменной z_i и удаляются ребра, принадлежащие разрезу. Процесс заканчивается, когда граф G оказывается пустым. Очевидно, для снижения переключательной активности элементов памяти, если вероятность p^*_{st} высока, то расстояние по Хэммингу между кодами состояний q_s и q_t должно быть сделано коротким. На последнем шаге ребрами связаны те вершины, соответствующие которым пары состояний связаны переходами с наибольшей вероятностью. Расстояния между их кодами равно единице.

Литература

1. Кристофидес Н. *Теория графов. Алгоритмический подход.* М.: Мир, 1978.

2. Закревский А. Д., Поттосин Ю. В., Черемисинова Л. Д. *Логические основы проектирования дискретных устройств.* М.: Физматлит, 2007.

3. Поттосин Ю. В., Шестаков Е. А. *Табличные методы декомпозиции систем полностью определенных булевых функций.* Минск: Белорус. наука, 2006.

4. Taghavi Afshord S., Pottosin Yu. V. *A new suboptimal decomposition algorithm based on the tabular method* // Танаевские чтения: доклады Шестой Международной научной конференции (27-28 марта 2014 г., Минск). Минск: ОИПИ НАН Беларуси, 2014. С. 161–165.

5. Закревский А. Д. *Раскраска графов при декомпозиции булевых функций.* Минск: ИТК НАН Беларуси, 2000. Вып. 5. С. 83–97.

6. Закревский А. Д. *Алгоритмы энергосберегающего кодирования состояний автомата* // Информатика. 2011. № 1(29). С. 68–78.

АНАЛИЗ НЕ УСТОЙЧИВОСТИ ГРАДИЕНТНОГО АЛГОРИТМА В ОДНОЙ СПЕЦИАЛЬНОЙ ЗАДАЧЕ ДИСКРЕТНОЙ ОПТИМИЗАЦИИ

А.Б. Рамазанов

Бакинский Государственный Университет, Баку, Азербайджан
rab-unibak@rambler.ru, ram-bsu@mail.ru

В данной работе анализируется не устойчивость градиентного алгоритма в одной специальной задаче дискретной оптимизации.

Пусть Z_+^n (R_+^n)- множество n-мерных неотрицательных целочисленных (действительных) векторов, $P \subseteq Z_+^n$ - порядково-выпуклое множество [1]. Рассмотрим задачу

$$\dot{f}(x) = \sum_{i=1}^{n} c_i x_i - \sum_{i=1}^{n} \alpha_i x_i^2 \to \max, \tag{1}$$

где $x = (x_1, ..., x_n) \in P, c = (c_1, ..., c_n),\ \alpha = (\alpha_1, ..., \alpha_n) \in R_+^n$.

Пусть x^g (x^*) - градиентное (оптимальное) решение задачи (1). Под гарантированный оценкой точности градиентного алгоритма решения задачи (1), как обычно, понимаем такое число $\varepsilon \geq 0$, что $(f(x^*) - f(x^g))/(f(x^*) - f(0)) \leq \varepsilon$. Задачу, полученную из задачи (1) путем возмущения вектора $c = (c_1, ..., c_n) \in R_+^n$ в пределах $(0, \delta)$, обозначим через $A(\delta)$. Пусть ε и $\varepsilon(\delta)$ - гарантированные оценки для задачи (1) и $A(\delta)$ соответственно. Градиентный алгоритм будем называть не устойчивым для задачи (1), если $\varepsilon(\delta) > \varepsilon$ (см., напр., [2]).

Теорема. *При малых возмущениях (колебаниях) вектора $c = (c_1, ..., c_n)$ в задаче (1) градиентный алгоритм не устойчив.*

Литература

1. Ковалев М. М.*Матроиды в дискретной оптимизации.* Минск: 1987, 222 с.

2. Рамазанов А. Б. *Анализ устойчивости градиентного алгоритма в задаче обслуживание сети со штрафом* // Вестник Бакинского Университета. 2014. №3. С. 38–44.

О ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ ПОИСКА ОСОБЫХ ТОЧЕК

А.В. Селиверстов

Институт проблем передачи информации им. А.А. Харкевича РАН
Большой Каретный 19, 1, 127051 Москва, Россия slvstv@iitp.ru

Многие важные задачи комбинаторной оптимизации остаются вычислительно трудными после длительного поиска эффективных методов решения [1]. Распознавание особой точки на комплексной гиперповерхности служит примером вычислительно трудной задачи, связанной с комбинаторной оптимизацией [2]. Проективная гиперповерхность, заданная формой f над полем характеристики нуль, особая, если совокупность частных производных первого порядка $\frac{\partial f}{\partial x_k}$ для $0 \leqslant k \leqslant n$ имеет нетривиальный нуль. Если форма f имеет рациональные коэффициенты, то это условие можно проверить за экспоненциальное (от n) время. Более того, совместность любой системы алгебраических уравнений с рациональными коэффициентами может быть проверена за экспоненциальное время [3].

Назовем $(-1, 1)$-точкой всякую точку в проективном пространстве, чьи однородные координаты равны -1 или 1 с точностью до общего ненулевого множителя. Это вершины многомерного куба. Проверка принадлежности некоторой $(-1, 1)$-точки к данной гиперплоскости является NP-полной задачей [4]. Подходы к ее решению, основанные на теореме Гильберта

Nullstellensatz, обсуждаются в [5]. Отметим, что соответствующая задача оптимизации может быть решена псевдополиномиальным алгоритмом, основанным на методе динамического программирования [4]. Подсчет числа $(-1,1)$-точек на гиперплоскости значительно сложнее.

Покажем, что задача о распознавании гиперплоскости, на которой не лежит никакая вершина многомерного куба, сводится к проверке гладкости комплексной проективной гиперповерхности третьей степени (кубики) или пятой степени (квинтики). Эти результаты усиливают ранее полученные результаты из [2].

Далее рассматриваются проективные гиперповерхности, которые заданы формами с целыми коэффициентами.

Теорема 1. *Существует детерминированный алгоритм, который получает на вход гиперплоскость H, заданную линейной формой $h = \sum\limits_{k=0}^{n} \alpha_k x_k$ с ненулевыми целыми коэффициентами $\alpha_k \neq 0$ для каждого индекса k, где $n \geqslant 3$, и за полиномиальное время выдает такую кубику S, что H не содержит ни одной $(-1,1)$-точки тогда и только тогда, когда S гладкая. Более того, особые точки на S взаимно однозначно соответствуют $(-1,1)$-точкам, принадлежащим H.*

Доказательство. Сопоставим линейной форме h форму третьей степени $f = \sum\limits_{k=0}^{n} \alpha_k x_k^3$. Выходом алгоритма служит ограничение формы f на гиперплоскость H, которое определяет гиперплоское сечение S — гиперповерхность в H.

Форма f определяет гладкую гиперповерхность, поскольку все коэффициенты α_k отличны от нуля. Следовательно, особыми точками на S служат точки касания гиперплоскости H с кубикой, заданной формой f. Если в некоторой $(-1,1)$-точке $\mathbf{x}$ обе формы h и f обращаются в нуль, то проективные гиперповерхности, заданные этими формами, касаются друг друга в $\mathbf{x}$. Следовательно, S имеет особую точку $\mathbf{x}$.

Поскольку для каждого индекса k коэффициент α_k отличен от нуля, градиенты форм ∇h и ∇f коллинеарны в точках с координатами, удовлетворяющими равенствам $x_k^2 = x_j^2$ для всех индексов k и j. Такие точки — это $(-1,1)$-точки. В этом случае особые точки на S взаимно однозначно соответствуют $(-1,1)$-точкам, лежащим на H. Теорема доказана.

Ограничение $n \geqslant 3$ в условии теоремы 1 связано с тем, что в случае $n \leqslant 2$ пересечение S содержит не более трех точек.

В некоторых случаях кубика проективно эквивалентна таковой специального вида, позволяющего определять особые точки, если они существуют [6]. Возможно, изучение гиперповерхностей позволит уточнить результаты о сложности нахождения второго решения NP-полной задачи [7]. Действительно, если известна одна особая точка и проективный автоморфизм кубики, то образ особой точки тоже будет особой точкой. Так поиск второй особой точки сводится к поиску автоморфизма, не оставляющего первую точку неподвижной. Следующий результат говорит о нетривиальности группы автоморфизмов гладкой кубики.

Теорема 2. *Гладкая кубика обладает проективным автоморфизмом второго порядка.*

Результат, аналогичный теореме 1, справедлив и для квинтики, но без взаимно однозначного соответствия особых точек и вершин куба.

Теорема 3. *Существует детерминированный алгоритм, который получает на вход гиперплоскость H, заданную линейной формой $h = \sum\limits_{k=0}^{n} \alpha_k x_k$ с ненулевыми целыми коэффициентами $\alpha_k \neq 0$ для каждого индекса k, где $n \geqslant 3$, и за полиномиальное время выдает такую квинтику S, что H не содержит ни одной $(-1,1)$-точки тогда и только тогда, когда S гладкая. Более того, если S особая, то множество особых точек конечное и включает все $(-1,1)$-точки, принадлежащие H.*

Доказательство. Сопоставим линейной форме h форму пятой степени $f = \sum\limits_{k=0}^{n} \alpha_k x_k^5$. Выходом алгоритма служит ограничение формы f на гиперплоскость H, которое определяет

гиперплоское сечение S — гиперповерхность в H.

Особыми точками на S служат точки касания гиперплоскости H с квинтикой, заданной формой f. Если в некоторой $(-1,1)$-точке $\mathbf{x}$ обе формы h и f обращаются в нуль, то проективные гиперповерхности, заданные этими формами, касаются друг друга в $\mathbf{x}$. Следовательно, S имеет особую точку $\mathbf{x}$.

Поскольку для каждого индекса k коэффициент α_k отличен от нуля, градиенты форм ∇h и ∇f коллинеарны в точках с координатами, удовлетворяющими равенствам $x_k^4 = x_j^4$ для всех индексов k и j. Такие точки — это $(-1,1,-\sqrt{-1},\sqrt{-1})$-точки. Поскольку коэффициенты α_k целые, если на H лежит некоторая $(-1,1,-\sqrt{-1},\sqrt{-1})$-точка, то на ней лежит и $(-1,1)$-точка, получаемая заменой координат $\pm\sqrt{-1}$ на ±1. Теорема доказана.

Полученные результаты иллюстрируют вычислительную трудность проверки гладкости гиперповерхностей высших степеней, хотя для квадрики гладкость проверяется легко. С другой стороны, они могут быть полезны для анализа различных комбинаторных задач, поскольку взаимное расположение особых точек связано некоторыми ограничениями.

Литература

1. Емеличев В. А., Супруненко Д. А., Танаев В. С. *О работах белорусских математиков в области дискретной оптимизации* // Известия АН СССР. Техническая кибернетика. 1982. № 6. С. 25–45.

2. Латкин И. В., Селиверстов А. В. *Вычислительная сложность фрагментов теории поля комплексных чисел* // Вестник Карагандинского университета. Сер. Математика. 2015. № 1 (77). С. 47–55.

3. Чистов А. Л. *Алгоритм полиномиальной сложности для разложения многочленов и нахождение компонент многообразия в субэкспоненциальное время* // Записки научных семинаров ЛОМИ. 1984. Т. 137. С. 124–188.

4. Схрейвер А. *Теория линейного и целочисленного программирования.* М.: Мир, 1991. Т. 1.

5. Margulies S., Onn S., Pasechnik D. V. *On the complexity of Hilbert refutations for partition* // Journal of Symbolic Computation. 2015. V. 66. P. 70–83.

6. Селиверстов А. В. *Кубические формы без мономов от двух переменных* // Вестник Удмуртского университета. Математика. Механика. Компьютерные науки. 2015. Т. 25. № 1. С. 71–77.

7. Найденко В. Г. *О сложности нахождения второго решения NP-полной задачи* // Весці Нацыянальнай Акадэміі Навук Беларусі. Серыя фізіка-матэматычных навук. 2012. № 2. С. 114–118.

О МАТЕМАТИЧЕСКОМ ОБОСНОВАНИИ SOLID ПРИНЦИПОВ

Е.А. Тюменцев

ОмГУ им. Ф.М. Достоевского, Мира 55-А, 644077 Омск, Россия
etyumentcev@gmail.com

SOLID – это аббревиатура, образованная названиями пяти архитектурных принципов объектно-ориентированного программирования: The **S**ingle Reposnsibility Principle (SRP), The **O**pen-Closed Principle (OCP), The **L**iskov Substitution Principle (LSP), The **I**nterface Segregation Principle (ISP), The **D**ependency Inversion Principle (DIP). Впервые LSP был рассказан Барбарой Лисков на коференции OOPSLA'87 [1], оставльные принципы опубликованы в книге Бертрана Мейера [2] в 1988 году. Значительную роль в популяризации SOLID сыграл Роберт Мартин, который опубликовал серию статей [3–6] в журнале The C++ Report. Он же придумал аббревиатуру SOLID.

Для удобства читателя приведем формулировки данных принципов:

The Single Responsibility Principle. *Должна быть ровно одна причина для изменения класса.*

The Open-Closed Principle. *Программные сущности (классы, модули, функции и т.п.) должны быть открыты для расширения, но закрыты для изменения.*

The Liskov Substitution Principle. Функции, которые используют ссылки на базовые классы, должны иметь возможность использовать объекты производных классов, не зная об этом.

The Interface Segregation Principle. *Клиенты не должны зависеть от методов, которые они не используют.*

The Dependency Inversion Priciple. *Модули верхних уровней не должны зависеть от модулей нижних уровней. Оба типа модулей должны зависеть от абстракций. Абстракции не должны зависеть от деталей. Детали должны зависеть от абстракций.*

Несмотря на то, что принципам уже почти три десятка лет, до сих пор не сложилось единого мнения относительно целесообразности их применения на практике, потому что привычные для программистов конструкции: оператор для создания нового объекта *new*, *enum*, оператор множественного выборa*l switch*, цепочка вызовов *if–else–if*, операторы приведения типа и т.д, за редким исключением, противоречат SOLID.

Так, проблема со *switch* в том, что он требует явного перебора всех возможных вариантов, что на практике не всегда возможно. Например, в графическом редакторе в данной момент есть четрые графических примитива: линия, эллипс, прямоугольник, ломаная. Процедура отрисовки изображения использует *switch* по типу графического примитива для отрисовки каждого графического элемента рисунка. Нет никакой гарантии, что через некотрое время не потребуется добавить какой-нибудь новый элемент, скажем, встроенное изображение или распылитель. Тогда придется модифицировать *switch*, что прямо нарушает OCP.

Оператор *new* требует явного указания типа, который он создает. А это значит, что если потребуется создать объект другого типа, то придется модифицировать оператор *new*, что опять нарушает OCP. Чтобы избавиться от данного недостатка используется паттерн Абстрактная фабрика [7].

Возникает вопрос: можно ли формально доказать или опровергнуть SOLID?

Удалось получить математическое обоснование всех 5 принципов, используя логику Хоара [8]. Алфавитом в логике Хоара является так называемая тройка Хоара

$$\{P\}S\{Q\},$$

где P, Q – утверждения – формулы логики предикатов, P называют предусловием, Q – постусловием, S – команда какого-либо языка программирования.

В доказательстве задействованы только две аксиомы данной логики:

Аксиома композиции.

$$\{P\}S\{Q\}, \{Q\}T\{R\} \vdash \{P\}S;T\{R\}$$

Аксиома выводимости

$$P_1 \to P, \{P\}S\{Q\}, Q \to Q_1 \vdash \{P_1\}S\{Q_1\}$$

Считается, что SOLID — это принципы объектно-ориентированного программирования. Однако поскольку в доказательстве не делалось никаких предположений о структуре самих операторов, то SOLID принципы справедливы и для процедурного программирования. А поскольку не использовались аксиомы присваивания и цикла, то SOLID также справедливы и для функционального программирования.

Литература

1. Liskov B. Keynote address — data abstraction and hierarchy // ACM SIGPLAN Notices. 1988. Vol. 23. No. 5. P. 17–34.
2. Meyer B. Object-oriented Software Construction. Prentice Hall, New York 1988.
3. Martin R. The Open-Closed Principle // C++ Report. January 1996.
4. Martin R. The Liskov Substitution Principle // C++ Report. March 1996.
5. Martin R. The Dependency Inversion Principle // C++ Report. May 1996.
6. Martin R. The Interface Segregation Principle // C++ Report. June 1996.
7. Gamma E. Helm R. Larman C. Johnson R. Vlissides J. *Design Patterns: Elements of Reusable Object-Oriented Software*. Pearson Education, Limited, 2005.
8. Hoare C. A. R. An axiomatic basis for computer programming // Magazine Communications of the ACM. 1969. Vol. 12. No. 10. P. 576–580.

О ТИПИЗАЦИИ ИЕРАРХИЧЕСКИХ СТРУКТУР ДАННЫХ

Г.В. Чернышев

ФГБУН Институт информатики и проблем регионального управления КБНЦ РАН,
И. Арманд 37а, 360000 Нальчик, Россия chern_gen@mail333.com

Алгебраические методы, с учетом опыта их применения в теории баз данных реляционного типа [1,2], оказываются полезными в исследованиях информационных структур и других типов. В данной работе предлагается подход к типизации одного класса иерархических структур, основанный на теоретико-категорной характеристике элементов иерархии.

Понятие структуры данных является фундаментальным понятием, во многом определяющим построение алгоритмов обработки данных. Важнейшими свойствами структур данных, влияющих на качество алгоритмов, являются их однородность и регулярность.

Однородность структуры связывают с совокупностью используемых в ней (типов) элементов, а регулярность — с повторяемостью связей между ними (существованием закономерностей). Естественным представлением совокупности объектов, структуры каждого объекта, является иерархическое представление.

Будем рассматривать корневые деревья, структура которых содержит регулярности специального вида, в связи с чем будем называть их иерархическими структурами. Иерархические структуры представляем категорией путей $\mathbb{C}_{\mathrm{P}}$ [3], которая содержит:

1. класс объектов $\mathbf{O}_{\mathrm{P}} = \{v_1, v_2, \ldots, v_i, \ldots\}$ с выделенным объектом v_{R};
2. для каждой упорядоченной пары (v_i, v_j), $v_i, v_j \in \mathbf{O}_{\mathrm{P}}$ — множество морфизмов вида $\mathbf{M}_{\mathrm{P}}(v_i, v_j) = \{\langle v_i, v_{i_1}, \ldots v_{i_k}, v_j\rangle \,|\, \{v_i, v_{i_1}, \ldots v_{i_k}, v_j\} \subseteq \mathbf{O}_{\mathrm{P}}\}$, такое, что $|\mathbf{M}_{\mathrm{P}}(v_i, v_j)| = 1$ (поэтому $\mathbf{M}_{\mathrm{P}}(a, b)$ — единственный морфизм между объектами a и b);
3. для каждой упорядоченной тройки объектов (v_i, v_j, v_k) — функцию (композицию)

$$\mathbf{M}_{\mathrm{P}}(v_j, v_k) \circ \mathbf{M}_{\mathrm{P}}(v_i, v_j) \to \mathbf{M}_{\mathrm{P}}(v_i, v_k),$$

задаваемую правилом (конкатенация) $\langle v_i, \ldots, v_j\rangle \cdot \langle v_j, \ldots, v_k\rangle = \langle v_i, \ldots, v_j, \ldots, v_k\rangle$;

4. для каждого $v \in \mathbf{O}_{\mathrm{P}}$ единичный морфизм (единицу) $\mathbf{1}_v = \mathbf{M}_{\mathrm{P}}(v, v) = \langle v\rangle$.

Путь между объектами v_i и v_j в категории $\mathbb{C}_{\mathrm{P}}$ — это последовательность объектов в представлении морфизма $\mathbf{M}_{\mathrm{P}}(v_i, v_j)$.

Важнейшее понятие категории путей — характеристический терминальный путь χ_{v^t}, интерпретируется как последовательность вершин дерева от терминальной вершины v^t к

v_R. Совокупность всех характеристических путей однозначно определяет $\mathbb{C}_\mathrm{P}$. Для χ-путей вводятся понятия обратного пути, делителя, общего и наиболее общего делителя.

Разработка теоретико-категорных положений для иерархических структур ([4]) привела к описанию регулярностей, позволяющих обосновать введение для этих структур схемы. Схема, по сути, является типом соответствующей иерархической структуры, что позволяет все действия над иерархическими структурами и их составляющими выражать через действия со схемой.

Для категории $\mathbb{C}_\mathrm{P}$ схемой называется категория $\mathbb{S}_\mathrm{P}$, такая, что каждый терминальный χ-путь из $\mathbb{C}_\mathrm{P}$ изоморфен ровно одному терминальному χ-пути из $\mathbb{S}_\mathrm{P}$.

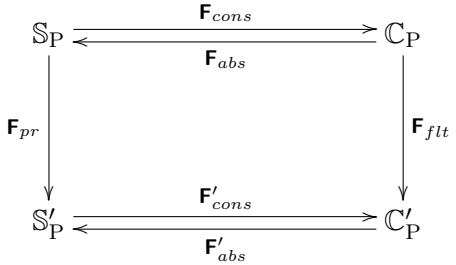
Любой нетерминальный χ-путь χ_v однозначно определяет множество χ-путей, для которых χ_v является наибольшим общим делителем: $\mathcal{S}(\chi_v) = \{\chi_{v_i} = \langle v_i, v, \ldots, v_R\rangle \mid i \in I_v\}$, где I_v — индексное множество для первых компонентов этих путей. При этом, χ_v назовем χ-путем типа *структура*, а элементы множества $\{\mathbf{M}_\mathrm{P}(v_i, v) \mid i \in I_v\}$ — *элементами структуры*. Здесь каждый объект структуры v_i может определять, либо терминальный χ-путь, либо χ-путь типа структура (структурный тип).

Введенные понятия структуры и ее элементов являются достаточными для представления произвольного дерева, в котором структурный тип характеризует нетерминальные вершины, а характеристистические терминальные пути — висячие вершины. Данные типы являются основными «структурообразующими» элементами как для категории $\mathbb{C}_\mathrm{P}$, так и для ее схемы $\mathbb{S}_\mathrm{P}$.

Любое подмножество χ-путей категории $\mathbb{C}_\mathrm{P}$ образует подкатегорию этой категории. Множество изоморфных подкатегорий $\mathcal{R}(\mathbb{C}_\mathrm{P}) = \left\{\mathbb{C}^i_\mathrm{P} \mid \mathbb{C}^i_\mathrm{P} \cong \mathbb{C}^j_\mathrm{P},\ \mathbb{C}^i_\mathrm{P}, \mathbb{C}^j_\mathrm{P} \subseteq \mathbb{C}_\mathrm{P},\ i \neq j\right\}$ категории $\mathbb{C}_\mathrm{P}$ назовем *регулярностью* в $\mathbb{C}_\mathrm{P}$. Регулярность в категорию $\mathbb{C}_\mathrm{P}$ вносят структуры. Изоморфными в структуре являются объекты, определяющие терминальные χ-пути.

Определим еще один вид регулярности. Если χ_{v_i} для фиксированного v_i не является терминальным χ-путем, то χ_{v_i} будет наибольшим общим делителем некоторого множества χ-путей, которое образует подкатегорию категории $\mathbb{C}_\mathrm{P}$. Обозначим эту подкатегорию, для каждого такого v_i, через $\mathbb{C}^{v_i}_\mathrm{P}$. Если все подкатегории из этой совокупности изоморфны друг другу, т.е. $\forall i, j \in I_v\ (i \neq j)$, $\mathbb{C}^{v_i}_\mathrm{P} \cong \mathbb{C}^{v_j}_\mathrm{P}$, то χ_v назовем χ-путем типа *массив*, а элементы множества $\left\{\mathbb{C}^{v_i}_\mathrm{P} \mid i \in I_v\right\}$ — *элементами массива*, где каждый v_i определяет, либо терминальный χ-путь, либо χ-путь типа массив. На самом деле, тип массива (как объект) можно ввести только в $\mathbb{S}_\mathrm{P}$.

Основные соотношения между категорией $\mathbb{C}_\mathrm{P}$, ее схемой $\mathbb{S}_\mathrm{P}$ и их подкатегориями $\mathbb{C}'_\mathrm{P} \subseteq \mathbb{C}_\mathrm{P}$ и $\mathbb{S}'_\mathrm{P} \subseteq \mathbb{S}_\mathrm{P}$ иллюстрирует следующая коммутативная диаграмма:



где $\mathbf{F}_{abs}$ — функтор абстрагирования, задающий типизацию категории $\mathbb{C}_\mathrm{P}$ посредством категории $\mathbb{S}_\mathrm{P}$, $\mathbf{F}_{cons}$ — функтор конкретизации, задающий конструктивное представление категории $\mathbb{S}_\mathrm{P}$ категорией $\mathbb{C}_\mathrm{P}$, $\mathbf{F}'_{cons}$ и $\mathbf{F}'_{abs}$ — аналогичные функторы, но действующие на соответствующих подкатегориях, $\mathbf{F}_{pr}$ — функтор проекции, $\mathbf{F}_{flt}$ — функтор фильтрации.

Смысл функтора проекции заключается в выделении подсхем в схеме $\mathbb{S}_\mathrm{P}$, при этом согласованное с ним действие функтора фильтрации выделяет соответствующую подкатегорию $\mathbb{C}'_\mathrm{P}$ в категории $\mathbb{C}_\mathrm{P}$. Согласование заключается в определении так называемого расширенно-

го естественного преобразования $\alpha : \mathbf{F}_{pr} \Rightarrow \mathbf{F}_{flt}$, которое позволит функтору $\mathbf{F}_{flt}$ выделить в $\mathbb{C}_{\mathrm{P}}$ конкретную подкатегорию $\mathbb{C}'_{\mathrm{P}}$, изоморфную подсхеме $\mathbb{S}'_{\mathrm{P}}$.

Литература

1. Плоткин Б.И. *Универсальная алгебра, алгебраическая логика и базы данных.* М.: Наука, 1991.

2. Бениаминов Е.М. *Алгебраические методы в теории баз данных и представлении знаний.* М.: Научный мир, 2003.

3. Чернышев Г.В. *Теоретико-категорное описание иерархических структур* // Материалы Второго Международного Российско-Узбекского симпозиума "Уравнения смешанного типа и родственные проблемы анализа и информатики". Нальчик: Издательство КБНЦ РАН, 2012. С. 278-280.

4. Чернышев Г.В. *Теоретико-методологические основы типизации иерархических структур* // Известия КБНЦ РАН, №5, 2013. С. 21–28.

О МИНОРАХ МАТРИЦЫ ОГРАНИЧЕНИЙ МНОГОИНДЕКСНЫХ ТРАНСПОРТНЫХ ЗАДАЧ

В.Н. Шевченко

Нижегородский Государственный Университет им. Лобачевского
просп. Гагарина 23, 603950 Нижний Новгород, Россия shev@vmk.unn.ru

Цель моего доклада — показать связь между триангуляциями многоиндексных транспортных многогранников [1–3] и некоторыми (как правило экстремальными) триангуляциями d-мерного куба [4, 5]. Пусть B_n — матрица, столбцами которой являются все различные булевы векторы длины n, а B_n^k — её подматрица, составленная из столбцов, содержащих ровно k единиц. Рассмотрим матрицу $A(i_1, i_2, \ldots, i_n; n)$, составленную из i_k экземпляров (i_k — неотрицательное целое число) матрицы B_n^k. Если считать столбцы рассматриваемых матриц лексикографически упорядоченными, то очевидно $B_n = A(1, 1, \ldots, 1; n)$. Известно [2, 3], что матрицы рассматриваемых классов обладают строчечной симметрией.

Средства.

Анализ характеристического многочлена матрицы $AA^\top$ позволяет получить ряд качественных результатов о минимальных триангуляциях кубов небольшой размерности [6], поскольку все его корни целые, а число различных среди них зависит только от n. Предлагается распространить этот подход на перманенты и подперманенты той же матрицы, обладающие аналогичными свойствами (см. [7]). В частности, этот подход позволяет уточнить понятие “небольшая размерность”.

Литература

1. Емеличев В.А., Ковалёв М.М., Кравцов М.К. *Многогранники, графы, оптимизация.* М.: Наука, 1981.

2. Емеличев В.А., Мельников О.И., Сарванов В.И., Тышкевич Р.И. *Лекции по теории графов.* Москва: Наука, 1990.

3. Шевченко В.Н. *Качественные вопросы целочисленного программирования.* Москва: Физматлит, 1995.

4. Шевченко В.Н., Груздев Д. В. *Модификация алгоритма Фурье-Моцкина для построения триангуляции и её звёздной развёртки.* // Дискретный анализ и исследование операций. Сер. 2. 2006. Т. 13. № 1. С. 77–94.

5. Шевченко В.Н. *Триангуляции выпуклых многогранников и их булевы функции* // Математические вопросы кибернетики. 2007. Вып. 16. С. 43–56.

6. Титова Е.Б., Шевченко В.Н. *О минорах матрицы ограничений многоиндексных транспортных задач* // Дискретная математика. 2012. Т. 24. № 4. С. 147–157.

7. Цветкович Д., Дуб М., Захс Х. *Спектры графов. Теория и применения.* Киев. Наукова думка. 1984.

ВОЗВРАЩЕНИЕ К МНОГОГРАННИКУ ГОМОРИ

В.А. Шлык

Командно-инженерный институт МЧС Республики Беларусь,
Машиностроителей 25, 220118 Минск, Беларусь
v.shlyk@gmail.com

Введение Ральфом Гомори [1] главного углового многогранника (главного многогранника Гомори) положило начало теоретико-групповому подходу в целочисленном линейном программировании. В середине 1990-х годов подтвердилась эффективность порождаемых с его помощью отсечений и оценок. С тех пор главный многогранник Гомори признан ключевым объектом в теории и практике целочисленного программирования. Автор начал изучать его по предложению Дмитрия Алексеевича Супруненко. Были доказаны новые свойства его фасет и субаддитивная характеризация фасет более общего многогранника на частичной алгебре вместо конечной абелевой группы в стандартном случае [2]. Высказанное Дмитрием Алексеевичем пожелание найти интересную интерпретацию введенного обобщенного многогранника удалось выполнить в 1996 г. — ею стал политоп разбиений чисел [3]. После описания его фасет [4] основное внимание было уделено вершинам. Главный многогранник Гомори обладает симметрией, обусловленной автоморфизмами его основной группы. Однако понять структуру множества вершин политопа разбиений чисел оказалось легче [5], поскольку части разбиений складываются обычным образом. Достигнутое понимание позволило продолжить начатое Гомори изучение вершин его многогранника, о которых после пионерской работы [1] существенных результатов получено не было. Ввиду практического значения фасет вершины выпали из поля зрения исследователей. Наиболее полно новые результаты о вершинах представлены в [6].

Далее G — конечная абелева группа, $\overline{0}$ — ее нулевой элемент, $G^+ = G \setminus \{\overline{0}\}$, $g_0 \in G$. Главным многогранником Гомори $P(G, g_0)$ (далее — ГМГ) называется выпуклая оболочка неотрицательных целочисленных решений $t = (t(g), g \in G^+)$ уравнения $\sum_{g\in G^+} t(g)g = g_0$. Множество вершин $P(G, g_0)$ обозначается $V(G, g_0)$

Гомори [1] доказал, что вершины ГМГ являются его неприводимыми точками, то есть такими $t \in P(G, g_0)$, что для любых $r = (r(g), g \in G^+)$ и $s = (s(g), g \in G^+)$ из условий $0 \le r(g) \le t(g)$, $0 \le s(g) \le t(g)$, $r \ne s$ следует неравенство $\sum_{g\in G^+} r(g)g \ne \sum_{g\in G^+} s(g)g$. Следующая теорема дает геометрическую характеризацию неприводимых точек.

Теорема 1. *Целочисленная точка $P(G, g_0)$ неприводима тогда и только тогда, когда она не является выпуклой комбинацией двух других целочисленных точек $P(G, g_0)$.*

Гомори рассматривал фасеты ГМГ как неравенства $\sum_{g\in G^+} \pi(g)t(g) \ge \pi_0$, обозначая их (π, π_0), где $\pi = (\pi(g), g \in G^+)$. Фасеты, отличные от $t(g) \ge 0$, он назвал нетривиальными. Обозначим $G_t = \{g \in G^+ | t(g) > 0\}$. Связи между вершинами ГМГ и содержащими их нетривиальными фасетами устанавливает

Теорема 2. *Пусть вершина $t \in V(G, g_0)$ лежит на нетривиальной фасете (π, π_0) и пусть $h = \sum_{g\in G^+} u(g)g$, $h \ne \overline{0}, t$, где все $u(g)$ целые, $0 \le u(g) \le t(g)$, $g \in G^+$. Тогда*

1. *точка $w = (w(g), g \in G^+)$ с компонентами $w(g) = t(g) - u(g)$, $g \in G^+$, $g \ne h$, и $w(h) = t(h) + 1$ лежит на фасете (π, π_0);*
2. *вектор коэффициентов π фасеты удовлетворяет соотношению $\pi(h) = \sum_{g\in G_t} u(g)\pi(g)$.*

Гомори доказал, что любой автоморфизм φ группы G преобразует каждую вершину $t \in V(G, g_0)$ в вершину $\overline{t} = \{\overline{t}(g), g \in G^+\} = \{t(\varphi^{-1}(g)), g \in G^+\}$ многогранника $P(G, \varphi(g_0))$. Введем две комбинаторные операции $\mu_{h,f}$ и μ_h, где $h, f \in G_t$ на $V(G, \varphi(g_0))$. Операция $\mu_{h,f}$ склеивает каждую из $k = \min(t_h, t_f)$ пар элементов h и f в элемент $h + f$, а операция μ_h склеивает t_h элементов h в элемент $t_h h$.

Теорема 3. *Если к вершине t многогранника $P(G, g_0)$ применима операция $\mu_{h,f}$ (или μ_h) с некоторыми $h, f \in G_t$, то $\mu_{h,f}(t)$ (соответственно, $\mu_h(t)$) также вершина $P(G, g_0)$ смежная вершине t.*

Отсюда следует, что все вершины $P(G, g_0)$ можно построить с помощью операций $\mu_{h,f}$ и μ_h из подмножества $S(G, g_0)$ тех вершин, которые нельзя получить из других вершин с помощью введенных μ-операций. Мы назвали их *опорными* вершинами.

Теорема 4. *Класс опорных вершин многогранников $P(G, g_0)$, $g_0 \in G$, инвариантен относительно действия*

$$\mathcal{V}(G) \times \mathrm{Aut}(G) \to \mathcal{V}(G) \ : \ (t, \varphi) \mapsto t \cdot \varphi = \overline{t},$$

группы автоморфизмов $\mathrm{Aut}(G)$ *группы G на множестве $\mathcal{V}(G) = \cup_{g_0 \in G} V(G, g_0)$ всех вершин всех ГМГ на группе G.*

Теорема 5. *С точностью до изменения элементов h и f операции $\mu_{h,f}$ и μ_h коммутируют с автоморфизмами: $(\mu_{h,f}(t)) \cdot \varphi = \mu_{\varphi(h),\varphi(f)}(t \cdot \varphi)$ и $(\mu_h(t)) \cdot \varphi = \mu_{\varphi(h)}(t \cdot \varphi)$.*

Следующая теорема суммирует основные результаты о структуре множества вершин $V(G, g_0)$ многогранника $P(G, g_0)$. В ней операции $\mu_{\varphi(h),\varphi(f)}$ и $\mu_{\varphi(h)}$ обозначены для простоты через μ_φ, и $\mathrm{Aut}_{g_0}(G)$ — стабилизатор элемента g_0 в $\mathrm{Aut}(G)$.

Теорема 6. *Множество $V(G, g_0)$ есть непересекающееся объединение орбит относительно действия* $\mathrm{Aut}_{g_0}(G)$. *Для любой вершины $t \in V(G, g_0)$ и любой операции $\mu_{h,f}$ или μ_h, применимой к t, преобразование $t \cdot \varphi \mapsto \mu_\varphi(t \cdot \varphi)$, $\varphi \in \mathrm{Aut}_{g_0}(G)$, отображает орбиту вершины t на орбиту вершины $\mu(t)$. Некоторые орбиты состоят только из опорных вершин, остальные орбиты опорных вершин не содержат. Таким образом, $S(G, g_0)$ есть непересекающееся объединение орбит, состоящих из опорных вершин $P(G, g_0)$. Для $V(G, \overline{0})$ выполняются аналогичные утверждения относительно* $\mathrm{Aut}(G)$.

Из теоремы следует, что в качестве вершинного базиса $P(G, g_0)$, из которого можно построить все его остальные вершины, и который, следовательно, полностью определяет этот многогранник, можно взять любую систему представителей орбит относительно действия $\mathrm{Aut}_{g_0}(G)$ на множестве опорных вершин $S(G, g_0)$.

Теорема 7. *Диаметр каждого главного многогранника Гомори равен 2.*

В 2012 г. на Европейской конференции по исследованию операций я имел честь рассказать изложенные результаты (тогда еще не опубликованные) Ральфу Гомори. В своем докладе о роли главного многогранника в ЦЛП он, по его словам, собирался специально подчеркнуть важность изучения его вершин.

Литература

1. Gomory R. E. *Some polyhedra related to combinatorial problems* // Linear Algebra Appl. 1969. Vol. 2. P. 451–558.

2. Шлык В. А. *Субаддитивная характеризация граней многогранных множеств на частичной алгебре* // Доклады АН БССР. 1984. Т. 28. № 11. С. 980–983.

3. Шлык В. А. *Политопы разбиений чисел* // Вес. Нац. акад. навук Беларусі. Сер. фіз.-мат. навук. 1996. № 3. С. 89–92.

4. Shlyk V. A. *Polytopes of partitions of numbers* // European J. Combin. 2005. Vol. 26. N 8. P. 1139–1153.

5. Shlyk V. A. *Polyhedral approach to integer partition* // J. Combin. Math. Combin. Comput. 2014. Vol. 89 (May). P. 113–128.

6. Shlyk V. A. *Master corner polyhedron: vertices* // European J. Oper. Res. 2013. Vol. 226. N. 2. P. 203–210.

ON CIRCULAR DISARRANGED STRINGS OF SEQUENCES

F. Beggas[1], M. M. Ferrari[2], H. Kheddouci[1], N. Zagaglia Salvi[2]

[1]University of Lyon, LIRIS UMR5205 CNRS, Claude Bernard Lyon 1 University
43 Bd du 11 Novembre 1918, F-69622, Villeurbanne, France
{fairouz.beggas,hamamche.kheddouci}@liris.cnrs.fr
[2] Dipartimento di Matematica, Politecnico di Milano
P.zza Leonardo da Vinci 32, 20133 Milano, Italy
{margheritamaria.ferrari,norma.zagaglia}@polimi.it

Two sequences $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_n)$, sharing $n-1$ elements, are said disarranged if for every subset $Q \subseteq [n]$, the sets $\{a_i \mid i \in Q\}$ and $\{b_i \mid i \in Q\}$ are different. In this paper we investigate properties of these pairs of sequences. Moreover we extend the definition of disarranged pairs to a circular string of n-sequences and prove that, for every positive integer m, except some initials values for n even, there exists a similar structure of length m.

Introduction

Let n be a positive integer, $R = (a_1, a_2, \ldots, a_n)$ and $S = (b_1, b_2, \ldots, b_n)$ n-sequences of distinct elements, sharing exactly $n-1$ elements.

We associate with R and S the bijection f defined by the relation $f(a_i) = b_i$, $1 \leq i \leq n$, and represented in two line notation by the $2 \times n$ array

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ b_1 & b_2 & \ldots & b_n \end{pmatrix}.$$

Let u and v be the different elements which belong to the first and the second line respectively. The function f is formed by the linear ordering $l(f) = (u, f(u), f^2(u), \ldots, f^{k-1}(u), v)$, where k is the minimum positive integer such that $f^k(u) = v$, and a permutation $\pi(f)$ on the remaining elements. In [2] a similar function, called widened permutation, is investigated in the context of the theory of species of Joyal. We say that R and S are **disarranged** if for every set $\{i_1, i_2, \ldots, i_r\} \subseteq \{1, 2, \ldots, n\}$ $\{a_{i_1}, a_{i_2}, \ldots, a_{i_r}\} \neq \{b_{i_1}, b_{i_2}, \ldots, b_{i_r}\}$.
The sequences R and S are called **1-disarranged** if there exists an index $i \in [n]$ such that $a_i = b_i$ and the sequences, obtained from R and S after deleting a_i and b_i, are disarranged. In this case we say that the pair (R, S) is 1-disarranged.

We extend the definition to a string of n-sequences.

Definition 1. Let $n, m \in \mathbb{N}$; an m-string $(S_1, S_2, \ldots, S_m)$ of n-sequences, is called **disarranged** if:

(A1) S_i is disjoint from S_{i-1} and S_{i+1},

(A2) S_{i-1} and S_{i+1} are disarranged.

for every $i = 2, \ldots, m-1$.

A disarranged m-string of n-sequences is *circular* when the properties **(A1)** and **(A2)** are satisfied for every $i = 1, 2, \ldots, m$ (taking the indices modulo m).

Main results

The notion of circular disarranged string of n-sequences has application in relation to an edge coloring problem of graphs [4]. In this paper we investigate properties of disarranged pairs of sequences and circular disarranged string of n sequences. In particular we prove that the n-sequences R and S, sharing exactly $n-1$ elements are disarranged if and only if the linear ordering $l(R, S)$ contains all the elements of R and S. Moreover we prove that, for every positive integer m,

there exists a circular disarranged string of n sequences of length m, except some initials values for n even.

The following theorem is a consequence of some Lemmas and Propositions.

Theorem 1. *Let m, n be positive integers. For n odd and every $m > 2$ or for n even and $m > 6$ even ($m \neq 14$) or for $m \geq 2n + 1$ odd ($m \neq 2n + 7$), there exists a circular disarranged m-string. For the remaining cases, there exists a circular 1-disarranged m-string.*

References

1. Baril J.-L., Kheddouci H., Togni O. *Vertex distinguishing edge- and total-colorings of Cartesian and other product graphs* // Ars Combinatoria. 2012. Vol. 107. P. 109–127.

2. Beggas F., Ferrari M. M., Zagaglia Salvi N. *Combinatorial interpretations and enumeration of particular bijections* // submitted.

3. M. Bona. *Combinatorics of Permutations*. Chapman and Hall/CRC Press, Boca Raton, FL, 2004.

4. Horňák M., Mazza D., Zagaglia Salvi N. *Edge colorings of the direct product of two graphs* // Graphs and Combinatorics. 2015. Vol. 1. No. 18.

5. Imrich W., Klavžar S. *Product Graphs: Structure and Recognition*. Wiley-Interscience, New York, 2000.

6. Munarini E., Perelli Cippo C., Zagaglia Salvi N. *On the adjacent vertex distinguishing edge colorings of direct product of graphs* // Recent results in designs and graphs: a Tribute to Lucia Gionfriddo. 2013. Vol. 28. Quaderni di Matematica, Aracne Ed. P. 369–392.

SPECTRAL CONDITION FOR HAMILTONICITY OF A GRAPH

V.I. Benediktovich

Institute of Mathematics, National Academy of Sciences of Belarus
11 Surganov str., 220072 Minsk, Belarus vbened@im.bas-net.by

Let $G = (V(G), E(G))$ be a simple undirected connected graph of order n and let $A = A(G)$ be its adjacency matrix. The largest eigenvalue of A, denoted by $\rho(G)$, is called *the spectral radius* of the graph G. According to the Perron-Frobenius theory of matrices [1] the spectral radius $\rho(G)$ is a positive real root of multiplicity 1 of the characteristic polynomial $\det(xE_n - A)$ and there exists a unique positive unit eigenvector corresponding to $\rho(G)$, called the *Perron* vector. Let $d_i = \deg_G(v_i)$ be the degree of any vertex $v_i \in V$ of the graph G and $(d_1, d_2, ..., d_n)$ be the degree sequence of the graph G, where $d_1 \leq d_2 \leq ... \leq d_n$. Then $d_1 = \delta$ is called *the minimum degree*.

The union of two graphs G and H is the graph $G \cup H$ with vertex set $V(G) \cup V(H)$ and edge set $E(G) \cup E(H)$. If graphs G and H are disjoint, then we call their union *a disjoint union* and denote it by $G + H$. The union of k disjoint copies of a graph G is denoted by kG. *The join* of two disjoint graphs G and H, denoted by $G \vee H$, is obtained from $G + H$ by joining each vertex of G to each vertex of H.

A cycle or path passing through all the vertices of a graph is called *Hamiltonian*. A graph G, containing Hamiltonian cycle or path, is called *Hamiltonian* or *traceable* correspondingly. It is known that the problem of deciding whether a given graph is Hamiltonian or traceable is NP-complete. Recently, spectral theory of graphs has been applied to this problem. In particular, the following Brualdi-Solheid-Turan type problem [2] has been intensively studied:

Problem. *For a given graph F, what is the maximum spectral radius of a graph G on n vertices without a subgraph isomorphic to F?*

This problem has been considered for the cases where F is a clique, an even or odd path (cycle) of the given length and a Hamiltonian path (cycle) ([3–6]). For example, sufficient spectral conditions for the existence of Hamiltonian paths and cycles are studied. Fiedler, Nikiforov gave tight sufficient conditions for the existence of Hamiltonian paths and cycles in terms of the spectral

radius of graphs or the complements of graphs [3]. Lu et al. [4] studied sufficient conditions for Hamiltonian paths in connected graphs and Hamiltonian cycles in bipartite graphs in terms of the spectral radius of a graph. Some other spectral conditions for Hamiltonian paths and cycles in graphs have been given in [7–8]. In 2014 [9] the sufficient condition of traceability of the graph was found in terms of the spectral radius:

Theorem 1 [9]. *Let G be a graph on $n \geq 4$ vertices with $\delta \geq 1$. If $\rho(G) > n-3$, then G contains a Hamiltonian path unless $G \in \{K_1 \vee (K_{n-3} + 2K_1), K_2 \vee 4K_1, K_1 \vee (K_1, 3 + K_1)\}$.*

In this work the following sufficient condition for the Hamiltonicity of a given graph in terms of its spectral radius has been obtained.

Theorem 2. *Let G be a simple connected graph on $n > 8$ vertices with $\delta \geq 2$. If $\rho(G) \geq n-3$, then the graph G is Hamiltonian unless $G \in \{5K_1 \vee K_4, K_3 \vee (K_{1,4} + K_1), K_2 \vee (K_{n-4} + 2K_1)\}$.*

The proof of the theorem is based on the following well-known facts.

Lemma 1 [10]. *Let G be a simple graph with n vertices and m edges and δ be the minimum degree of vertices of G. Then its spectral radius $\rho(G)$ satisfies the inequality:*

$$\rho(G) \leq \frac{\delta - 1 + \sqrt{(\delta+1)^2 + 4(2m - \delta n)}}{2}.$$

Lemma 2 [10]. *$f(x) = x - 1 + \sqrt{(x+1)^2 + 4(2m - xn)}$ is a decreasing function of x on the interval $[1; n-1]$, where $n - 1 \leq m \leq n(n-1)/2$ and $2m \geq xn$.*

From lemmas 1, 2, and the conditions of the theorem one can receive the following inequality:

$$n^2 - 5n + 10 \leq 2m. \tag{13}$$

Let us assume that the graph G is not Hamiltonian. Then according to the Chvatal theorem [11] there exists a number $k \in \mathbb{N}$, such that $d_k \leq k < n/2$ and $d_{n-k} \leq n - k - 1$ for the degree sequence of the graph G: $\delta = d_1 \leq d_2 \leq \ldots \leq d_n$. Therefore:

$$2m = \sum_{i=1}^{n} d_i \leq k \cdot k + (n-2k)(n-k-1) + k(n-1) = n^2 + 3k^2 + k - 2kn - n. \tag{14}$$

and one can show that $k \in \{1, 2, \ldots, 6\}$. However, from the condition $\delta \geq 2$ it follows, that $k \neq 1$.

In the case $k = 2$ the inequality (14) gives the upper bound: $2m \leq n^2 - 5n + 14$. Thus:

$$\frac{n(n-5)}{2} + 5 \leq m \leq \frac{n(n-5)}{2} + 7 = C^2_{n-2} + 4.$$

Note that the upper bound $C^2_{n-2} + 4$ for the number of edges m is reached only for the graph $G = K_2 \vee (K_{n-4} + 2K_1)$. Moreover, a graph H, obtained from the graph G by removing only one edge, can have only one of the following degree sequences:

1) $(2, 2, \underbrace{(n-3), \ldots, (n-3)}_{n-4}, (n-2), (n-2))$, i.e. $H = 2K_1 \vee (K_{n-4} + 2K_1)$;

2) $(2, 2, (n-4), (n-4), \underbrace{(n-3), \ldots, (n-3)}_{n-6}, (n-1), (n-1))$, i.e. $H = K_2 \vee (2K_1 \vee K_{n-6}) + 2K_1)$;

3) $(2, 2, (n-4), \underbrace{(n-3), \ldots, (n-3)}_{n-5}, (n-2), (n-1))$.

Using the structure of the adjacency matrices of these graphs we show that for them the inequality $\rho(H) < n - 3$ is valid. Hence, for the graph, obtained from the graph G by removing two edges, this inequality is valid as well according to the following statement:

Lemma 3 [1]. *Let G be a simple connected graph and H be its proper subgraph. Then $\rho(G) > \rho(H)$.*

For the cases $k = 3; 5; 6$ one can easily check that the spectral radius of G satisfies the inequality $\rho(H) < n - 3$. For the case $k = 4$ the unique graphs that satisfy the inequality $\rho(H) \geq n - 3$ are $5K_1 \vee K_4$ and $K_3 \vee (K_{1,4} + K_1)$.

This work is supported by the Institute of Mathematics of NAS of Belarus in the framework of the SPFR "Convergence" and the BRFFR No. F14RA-004.

References

1. Brouwer A.E., Haemers W.H. *Spectra of graphs*. Springer-Verlag, 2011.

2. Brualdi R.A., Solheid E.S. *On the spectral radius of complementary acyclic matrices of zeros and ones* // SIAM J. Algebraic Discrete Methods. 1986. V. 7. No. 2. P. 265–272.

3. Fiedler M., Nikiforov V. *Spectral radius and Hamiltonicity of graphs* // Linear Algebra Appl. 2010. V. 432. P. 2170–2173.

4. Lu M., Liu H., Tian F. *Spectral radius and Hamiltonian graphs* // Linear Algebra Appl. 2012. V. 437. P. 2670–2174.

5. Nikiforov V. *The spectral radius of graphs without paths and cycles of specified length* // Linear Algebra Appl. 2010. V. 432. P. 2243–2256.

6. Yuan W., Wang B., Zhai M. *On the spectral radii of graphs without given cycles* // Electron. J. Linear Algebra. 2012. V. 23. P. 599–606.

7. Krivelevich M., Sudakov B. *Sparse pseudo-random graphs are Hamiltonian* // J. Graph Theory. 2003. V. 42, No. 1. P. 17–33.

8. Mohar B. *A domain monotonicity theorem fgor graphs and hamiltonicity* // Discrete Appl. Math. 1992. V. 36, No. 2. P. 169–177.

9. Ning B., Ge J. *Spectral radius and Hamiltonian properties of graphs* // Linear and Multilinear Algebra. 2014. V. 63, No. 8. P. 1520–1530.

10. Hong Y., Shu J., Fang K. *A sharp upper bound of the spectral radius of graphs* // J. Combin. Theory. 2001. V. 81. P. 177–183.

11. Yemelichev V.A., Melnikov O.I., Sarvanov V.I., Tyshkevich R.I. *Lectures on Graph Theory*. M: Nauka, 1990.

CAN WE BORROW THE CONCEPT OF INDEPENDENT RELATION FROM LINEAR ALGEBRA IN SOME DISCRETE MATH APPLICATIONS

B.S. Chow

National Sun Yet-sen University,
Department of Electrical Engineering, 80424 Kaohsiung, Taiwan, ROC
bschow@mail.ee.nsysu.edu.tw

Sperner family [1, 2], formally an antichain in the inclusion lattice over the power set of a universal set X, is also called an independent system. The independence is defined as the non-containing-ship between every pair of members. In other words, the dependence is defined as the existence of a containing-ship for some pairs. This is a relation between two members. In contrast, the dependence in linear algebra is defined by the relation between one member and one group (many members). We therefore ask if this relational difference for the Sperner family is appropriate, borrowing the concept from linear algebra? We study the above question by starting from investigating the purpose of independence definition arranged for the Sperner family.

If the purpose is to make the family compact, there should be no redundant member in the family. An independent system (the Sperner family) is thus equivalent to a family without any redundant member. A redundant member is clearly understood by words is a member, whose existence or not does not make any difference for the family. By this interpretation, the dependence relation is built between the redundant member and the rest of the family.

To check if there is a difference made by the suspicious redundant member, the originally вЂњstaticвЂќ member needs to be regarded as a function to have the ability to influence (make

a difference). One simple arrangement is to regard the member as a Boolean function and the family (union of members) as a combination of functions. To be more specific, the member is a function composed of product (logic AND) of operands; the family is a function composed of a sum (logic OR) of products. For example, the member [01100] and the family [11000], [10100], [01100] are regarded as the Boolean functions bc and ab + ac + bc respectively.

To check if the family is compact (independent) needs to check for every member to be not redundant. The check for a specific member is to check if the reduced family (the original family excluding the specific member) behaves identically to the original family. The above two families (the reduced one the original one) are regarded as two Boolean functions. Two functions to be identical require the two corresponding outputs to be identical for every possible input. Therefore, we need to check the difference between the two outputs for every possible input. The requirements on checking every member (Boolean function) and every input (Boolean block) make the checking lengthy. To simplify and to visualize the checking, we design a full-pattern (the all possible Boolean block combination) image for the testing Boolean functions. In this sense, the checking work is implemented by an image processing. A full-pattern image for the case of the universal set X with cardinality five will be presented in the conference.

Acknowledgments

This research is partially supported by the National Science Council of the Republic of China under the contract NSC 99-2625-M-009-004-003.

References

1. Anderson, I. *Combinatorics of Finite Sets. "Sperner's theorem"*. Oxford University Press, 1987.

2. Knuth, D. E. *The Art of Computer Programming, IV. "Draft of Section 7.2.1.6: Generating All Trees"*. 2005. P. 17–19. `http://www-cs-faculty.stanford.edu/ knuth/fasc4a.ps.gz`.

COMBINATORICS AND ALGORITHMS FOR AUGMENTING GRAPHS

K.K. Dabrowski[1], D. de Werra[2], V.V. Lozin[3], V. Zamaraev[3]

[1]School of Engineering and Computing Sciences, Durham University, Science Laboratories, South Road, Durham DH1 3LE, UK konrad.dabrowski@durham.ac.uk

[2]Mathematics Institute, École Polytechnique Fédérale (EPFL), Switzerland dominique.dewerra@epfl.ch

[3]DIMAP and Mathematics Institute, University of Warwick, Coventry, CV4 7AL, UK

{V.Lozin,V.Zamaraev}@warwick.ac.uk

The notion of augmenting graphs generalizes Berge's idea of augmenting chains, which was used by Edmonds in his celebrated solution of the maximum matching problem. This problem is a special case of the more general maximum independent set (MIS) problem. Recently, the augmenting graph approach has been successfully applied to solve MIS in various other special cases. However, our knowledge of augmenting graphs is still very limited, and we do not even know what the minimal infinite classes of augmenting graphs are. In the present paper, we find an answer to this question and apply it to extend the area of polynomial-time solvability of the maximum independent set problem.

ON THE COMPLEXITY OF THE CLUSTERING MINIMUM BICLIQUE COMPLETION PROBLEM

O. Duginov

Institute of Mathematics, National Academy of Sciences of Belarus
11 Surganov str., 220072, Minsk, Belarus oduginov@gmail.com

We consider the complexity results for the Clustering Minimum Biclique Completion problem on some subclasses of bipartite graphs.

A finite undirected graph $G = (V, E)$ is bipartite if its vertex set V can be partitioned into two sets $X, Y \subseteq V$ (partite sets) such that every edge of G has its ends in different sets X, Y. For a vertex $v \in V$, the set of vertices of the graph G adjacent to v is denoted by $N_G(v)$. Let $G = (X \cup Y, E)$ be an arbitrary bipartite graph with non-empty partite sets X, Y and let p be a positive integer such that $p \leq |X|$. If we add all edges of the set $\overline{E} = \{\{x, y\} : x \in X, y \in Y, \{x, y\} \notin E\}$ to the graph G, we obtain a complete bipartite graph $G' = (X \cup Y, E \cup \overline{E})$ whose the partite set X can be partitioned into p non-empty sets $X_1, X_2, \ldots, X_p$ with the following condition: $N_{G'}(x) = N_{G'}(x')$ for every pair of vertices $x, x' \in X_i$, $i \in \{1, 2, \ldots, p\}$. The Clustering Minimum Biclique Completion problem is to find a minimum cardinality set $E' \subseteq \overline{E}$ to be added to the graph G so that the partite set X of the resulting bipartite graph $G' = (X \cup Y, E \cup E')$ can be partitioned into p non-empty sets $X_1, X_2, \ldots, X_p$ with the same condition. The decision version of the problem can be stated as follows:

Clustering Minimum Biclique Completion
Instance: A bipartite graph $G = (X \cup Y, E)$ with non-empty parts X and Y, two positive integers $p \leq |X|$ and k.
Question: Can G be transformed by adding at most k additional edges connecting vertices from different sets X, Y into a bipartite graph G' whose the partite set X can be partitioned into p non-empty sets $X_1, \ldots, X_p$ such that $N_{G'}(x) = N_{G'}(x')$ for any two vertices $x, x' \in X_i$, $i \in \{1, 2, \ldots, p\}$?

This problem, also known as the Multicast Partition problem, has been introduced by N. Faure [1, 2] and arises in telecommunication network technologies [2]. The computational complexity of the Clustering Minimum Biclique Completion problem for various subclasses of bipartite graphs is little-studied. To the best of our knowledge, there is only two results. N. Faure et. al. in [2] showed that: (a) the problem is NP-complete for fixed $p = 2$ (by a reduction from the Maximum Edge Biclique problem) and (b) the problem restricted to bipartite graphs $G = (X \cup Y, E)$ with degrees of vertices of Y at most 1 can be solved in strongly polynomial time by a dynamic programming algorithm. On the other hand, the problem is well-studied from a mathematical programming point of view [3–6].

We provide several well-known subclasses of bipartite graphs, for which the considered problem remains NP-complete. Recall that a graph G is H-free if G does not contain an isomorphic copy of the graph H as an induced subgraph.

Theorem 1. Clustering Minimum Biclique Completion *for P_4-free bipartite graphs is NP-complete.*

Corollary 1. Clustering Minimum Biclique Completion *is NP-complete for the following subclasses of bipartite graphs (for definitions we refer to* [7, 8]*): bipartite permutation graphs, convex graphs and chordal bipartite graphs.*

A bipartite graph $G = (X \cup Y, E)$ is $(3, 2)$-regular if the degree of every vertex of X is 3 and the degree of every vertex of Y is 2.

Theorem 2. Clustering Minimum Biclique Completion *for C_4-free $(3, 2)$-regular bipartite graphs and $p = 2$ is NP-complete.*

On the positive side, the Clustering Minimum Biclique Completion problem for $2K_2$-free bipartite graphs $G = (X \cup Y, E)$ can be solved in $O(|X|^4|Y|p)$ time, assuming that the input graph is represented by adjacency lists.

This work was supported by Belarusian Republican Foundation for Fundamental Research (project F14RA-004).

References

1. Faure N. *Contribution á la résolution de problémes de regroupement de sessions multicasts.* PhD thesis, Université Paris VI. 2006 (in French).

2. Faure N., Chrétienne P., Gourdin E., Sourd F. *Biclique completion problems for multicast network design* // Discrete Optimization. 2007. V. 4. P. 360–377.

3. Gualandi S. *k-Clustering Minimum Biclique Completion via a Hybrid CP and SDP Approach* // Proceedings of the 6th International Conference on Integration of AI and OR Techniques in Constraint Programming for Combinatorial Optimization Problems, CPAIOR 2009. 2009. V. 5547. P. 87–101.

4. Gualandi S., Maffioli F., Magni C. *A branch-and-price approach to k-clustering minimum biclique completion problem* // International Transactions in Operational Research. 2013. V. 20. P. 101–117.

5. Gualandi S., Malucelli F. *Weighted Biclique Completion via CP-SDP Randomized Rounding* // Proceedings of the European Workshop on Mixed Integer Nonlinear Programming. 2010. P. 223–230.

6. Magni C. *Biclique completion problem: models and algorithms.* MSc thesis, Politecnico di Milano. 2009.

7. Spinrad J.P. *Efficient Graph Representations.* Fields Institute Monographs, 2003.

8. Brandstädt A., Le V.B., Spinrad J.P. *Graph classes: a survey.* Society for Industrial and Applied Mathematics, 1999.

DOMINATION TRIANGLE, IRREDUNDANCE TRIANGLE AND 1-TRIANGLE GRAPHS

P.A. Irzhavski, Y.A. Kartynnik, Y.L. Orlovich

Belarusian State University, Faculty of Applied Mathematics and Computer Science
4 Nezavisimosti Ave, 220030, Minsk, Belarus
irzhavski@bsu.by, kartynnik@bsu.by, orlovich@bsu.by

1. Introduction. Orlovich et al. [1, 2] have used the non-hereditary class of *triangle graphs* as a model to establish computational complexity results for several independence and domination related parameters. We introduce some its non-hereditary subclasses and use them to study the computational complexity for other similar parameters.

Triangle graphs arise from the study of general partition graphs by DeTemple et. al. [3]. A *general partition graph* G is an intersection graph on a set S such that every maximal independent set of G corresponds to a partition of S. General partition graphs have been studied in connection to the lattice polygon triangulations and in a more general setting [4].

It has been noted by McAvaney et. al. [5] that for a graph G to be a general partition graph, the following *triangle condition* is sufficient: For every maximal independent set $I \subseteq V(G)$ and every edge $uv \in E(G - I)$ there exists a vertex $w \in I$ such that the vertices u, v, and w induce a triangle in G. Such graphs have been called *triangle graphs* by Orlovich et. al. [1].

According to Sampathkumar and Neeralagi [6], a vertex set $S \subseteq V(G)$ is called a *neighbourhood set* if

$$G = \bigcup_{v \in S} G(N[v]).$$

A neighbourhood set S is thus a dominating set having a property that every edge not covered by the vertices of S has both its ends adjacent to the same arbitrary vertex in S.

This definition obviously leads to the way to specify the triangle graphs equivalently as the graphs having the property of every maximal independent set being a neighbourhood set (actually an *independent neighbourhood set* [7]). As a consequence of this coincidence, Orlovich et. al. have established that the minimum independent neighbourhood set cardinality $n_i(G)$, which is equal to the independent domination number $i(G)$ in triangle graphs, is polynomially inapproximable in a triangle graph G up to the factor of $|V(G)|^{1-\varepsilon}$ for arbitrary $\varepsilon > 0$ unless $P = NP$ [1]; and for the maximum minimal independent neighbourhood set cardinality ($N_i(G)$, coinciding with $\alpha(G)$ in triangle graphs) they have shown the NP-hardness of the computation problem [2].

2. Domination and irredundance triangle graphs. We introduce *domination* and *irredundance triangle* graphs as the graphs having every dominating and maximal irredundant set, respectively, being a neighbourhood set. A set $S \subseteq V(G)$ is called *irredundant* [8] if $N[S \setminus \{s\}] \neq N[S]$ for every $s \in S$. Anbeek et. al. have noted that a sufficient condition for the graph to be a general partition graph is edge simpliciality (i.e. having every edge belong to a simplicial clique, a clique having a vertex adjacent only to the other vertices in that clique), which they have called the *edge condition* [9]. We give the following characterization:

Theorem 1. *The classes of domination triangle graphs and irredundance triangle graphs coincide and are precisely defined by the edge condition.*

It is also interesting to note that the edge condition in fact characterizes the class of upper-bound graphs known from the intersection graph theory and defined in terms of partially ordered sets [10].

We notice that the minimum-cardinality parameters for dominating, neighbourhood and maximal irredundant sets – respectively the domination number $\gamma(G)$, the neighbourhood number $\bar{n}(G)$ and the irredundance number $ir(G)$ for a graph G – coincide in such graphs. This observation is then used to prove the following result.

Theorem 2. *Computing the parameters $\gamma(G) = \bar{n}(G) = ir(G)$ for an arbitrary edge-simplicial graph is $c \log |V(G)|$-inapproximable in polynomial time for some fixed $c > 0$ unless $P = NP$.*

It is worth noting that we are not aware of any prior approximation bounds for $ir(G)$ and computational complexity results for $\bar{n}(G)$.

3. 1-triangle graphs. We then introduce the class of 1-*triangle* graphs which are triangle graphs with the restriction that every edge in $E(G-I)$ for every maximal independent set I forms a triangle with exactly one vertex in I. We provide the following characterization of 1-triangle graphs:

Theorem 3. *For every connected 1-triangle graph G, at least one of the following holds:*
1) G is a complete bipartite graph;
2) G is a graph isomorphic to $K_m \times K_m$ for some m;
3) G is a $(K_4 - e)$-free domination triangle graph.

We show that every maximal independent set in 1-triangle graphs is a perfect neighbourhood set, which is defined by Sampathkumar and Neeralagi [7] as a neighbourhood set in which the closed neighbourhoods of every two vertices are edge disjoint. This is used in the proof of the following

Theorem 4. *Computing the minimum and maximum cardinalities $n_p(G)$ and $N_p(G)$ of perfect neighbourhood sets in a 1-triangle graph G is NP-hard.*

To the best of our knowledge, this is the first account of computational complexity for n_p.

This work has been partially supported by the BRFFR grant (Project F15MLD-022).

References

1. Orlovich, Y.L., Zverovich, I.E. *Independent domination in triangle graphs* // Electronic Notes in Discrete Mathematics, 2007. V. 28. P. 341–348.

2. Orlovich Y., Blazewicz J., Dolgui A., Finke G., Gordon V. *On the complexity of the independent set problem in triangle graphs* // Discrete Mathematics, 2011. V. 311 (16). P. 1670–1680.

3. DeTemple, D., Harary, F., Robertson, J. *Partition graphs* // Soochow Journal of Mathematics, 1987. V. 13. P. 121–129.

4. DeTemple, D., Robertson, J. *Graphs associated with triangulations of lattice polygons* // Journal of the Australian Mathematical Society Series A, 1989. V. 47. P. 391–398.

5. McAvaney, K., Robertson, J., DeTemple, D. *A characterization and hereditary properties for partition graphs* // Discrete Mathematics, 1993. V. 113. No. 1. P. 131–142.

6. Sampathkumar, E., Neeralagi, P.S. *The neighbourhood number of a graph* // Indian Journal of Pure and Applied Mathematics, 1985. V. 16. P. 126–132.

7. Sampathkumar, E., Neeralagi, P.S. *Independent, perfect and connected neighbourhood numbers of a graph* // Journal of Combinatorics, Information & System Sciences, 1994. V. 19. P. 139–145.

8. Bollobaś, B., Cockayne, E.J. *Graph-theoretic parameters concerning domination, independence, and irredundance* // Journal of Graph Theory, 1979. V. 3. No. 3. P. 241–249.

9. Anbeek, C., McAvaney, K., Robertson, J. *When are chordal graphs also partition graphs?* // Australasian Journal of Combinatorics, 1997. V. 16. P. 285–293.

10. Cheston, G.A., Jap, T.S. *A survey of the algorithmic properties of simplicial, upper bound and middle graphs* // Journal of Graph Algorithms and Applications, 2006. V. 10. No. 2. P. 159–190.

GRAPHS WITH EQUAL DISTANCE PARAMETERS

Yury Kartynnik[1], Andrew Ryzhikov[2]

[1]Belarusian State University, Faculty of Applied Mathematics and Informatics
4 Nezavisimosti Ave, 220030, Minsk, Belarus
kartynnik@bsu.by
[2] United Institute of Informatics Problems, National Academy of Sciences, Belarus
6 Surganov str., 220072, Minsk, Belarus
ryzhikov.andrew@gmail.com

1. Introduction. The concepts of distance packing and covering in graphs was introduced by Meir and Moon in [1]. We consider finite, simple, undirected graphs without loops and multiple edges. A set P of vertices in a graph is called a *k-packing* (or a *k-independent set*) if the distance between any two distinct vertices in this set is larger than k. The maximum size of the k-packings in a graph G is called the *k-packing number* of G and is denoted by $\rho_k(G)$. A set D of vertices in a graph G is called a *k-covering* (or a *k-domination set*) if for any vertex v in $V(G)$ there is a vertex in D at a distance no more than k from v. The minimum size of the k-domination sets in a graph G is called the *k-domination number* of G and is denoted by $\gamma_k(G)$. A set I of vertices in a graph is called a *k-independent domination set* if it is both a k-packing and a k-covering. The minimum size of the k-independent domination sets in a graph G is called the *k-independent domination number* of G and is denoted by $i_k(G)$. For every graph G, the inequality $\gamma_k(G) \leq i_k(G) \leq \rho_k(G)$ holds.

The relation between the distance packing, domination and independent domination numbers has been widely studied in the literature. In [1] it is shown that the equality $\gamma_k(T) = \rho_{2k}(T)$ holds for any tree T. In [2] this equality is proved for a larger class of sun-free chordal graphs, which includes line graphs of trees, interval graphs and powers of block graphs. In [3] the graphs with equal k-packing and $2k$-packing numbers are characterized. This characterization implies a simple polynomial recognition algorithm for such graphs.

2. Recognition of k-equipackable graphs. A graph G is called *k-equipackable* if $i_k(G) = \rho_k(G)$. For $k = 1$ such graphs have been widely studied under the name *well-covered*, see the survey by Plummer [4]. In [5] it is shown that deciding whether a graph is not k-equipackable is an NP-complete problem. Lesk and Plummer [6] obtained that the recognition of line 1-equipackable graphs is a polynomially solvable problem. In [7] it is proved that recognizing non-2-equipackable line graphs is an NP-complete problem. Our following result establishes the computational complexity for the problem of recognizing k-equipackable line graphs for $k \geq 2$.

Theorem 1. *Deciding whether a given line graph is not k-equipackable is an NP-complete problem for any fixed $k \geq 2$.*

Corollary 1. *Let G be a line graph. Deciding whether G^k is not well-covered is an NP-complete problem for any fixed $k \geq 2$.*

3. Subclasses of k-equipackable graphs. Let k be a positive integer and $\mathcal{R}_k$ be the class of graphs with $\rho_k(G) = \rho_{2k}(G)$ for every $G \in \mathcal{R}_k$. In [3] a simple characterization of the class $\mathcal{R}_k$ is obtained. In [2] it is proved that for every sun-free chordal graph G the equality $\gamma_k(G) = \rho_{2k}(G)$ holds. Using this results, we obtain the following characterization.

Theorem 2. *The following statements are equivalent for a sun-free chordal graph G:*
1) $\gamma_k(G) = \rho_k(G)$;
2) $G \in \mathcal{R}_k$.

Corollary 2. *The problem of recognizing sun-free chordal graphs G having $\gamma_k(G) = \rho_k(G)$ is polynomially solvable.*

Using the characterization of the graphs with equal k-packing and $2k$-packing numbers from [3], we obtain the following.

Theorem 3. *Every graph in $\mathcal{R}_k$ is k-equipackable.*

Thus, all the sun-free chordal graphs with $\gamma_k(G) = \rho_k(G)$ are k-equipackable. It is an open question whether there are any other k-equipackable sun-free chordal graphs.

We thank Yury L. Orlovich for stating the question of recognizing the complexity of k-equipackable line graphs and multiple useful comments and suggestions during the course of this work.

This work has been partially supported by the Belarusian BRFFR grant (Project F15MLD-022).

References

1. Meir A., Moon J.W. Relation between packing and covering of a tree // Pacific Journal of Mathematics. 1975. V. 61. P. 225–233.

2. Chang G.J., Nemhauser G.L. The k-domination and k-stability problems on sun-free chordal graphs // SIAM Journal on Algebraic Discrete Methods. 1984. V. 5. No. 3. P. 332–345.

3. Joos F., Rautenbach D. Equality of distance packing numbers // Preprint, arxiv.org/abs/1402.6129.

4. Plummer M.D. Well-covered graphs: A survey // Quaestiones Mathematicae. V. 16. No. 3. P. 253-287.

5. Favaron O., Haynes T.W., Slater P.J. Distance-k independent domination sequences // The Journal of Combinatorial Mathematics and Combinatorial Computing. 2000. V. 33. P. 225-237.

6. Lesk M., Plummer M.D., Pulleyblank W.R. Equi-matchable graphs. In: Graph theory and combinatorics, Academic Press, London, 1984. P. 239–254.

7. Baptiste P., Kovalyov M. Y., Orlovich Y. L., Werner F., Zverovich I. E. Graphs with maximal induced matchings of the same size // Proc. of 14th IFAC Symposium on Control problems in Manufacturing. 2012. P. 518–523.

TRAPDOOR ONE-WAY PERMUTATIONS AND MULTIVARIATE POLYNOMIALS BASED ON RANDOM WALKS ON GRAPHS

M. Klisowski

Institute of Mathematics, Maria Curie Sklodowska University,
M. Curie-Sklodowska square 5, 20-031, Lublin, Poland
mklisow@hektor.umcs.lublin.pl

Public key cryptography is nowadays commonly used (electronic banking, etc.). Hovever, most of the currently used public key schemes may soon turn out to be completely insecure. As soon as sufficiently large quantum computer is built, most of the problems that are now considered computationally infeasible and are the basis of today's cryptography, will become easy to solve. These problems are integer factorization (the basis of RSA cryptosystem) and discrete logarithm problem (the basis of ElGamal cryptosystem, Diffie-Hellman key exchange and Elliptic Curve Cryptography). For both of these problems there are known efficient quantum algorithms [7,8].

Post-Quantum Cryptography [1] is the domain of Cryptography dealing with cryptographic algorithms that are considered secure against attacks by quantum computers. Multivariate Cryptography [2] is one of the most important directions of Post-Quantum Cryptography. The main idea of Multivariate Cryptography is to use the system of nonlinear polynomial equations as the trapdoor one-way permutations (the most important building blocks of public key cryptosystems). The system should be designed in such a way that solving it (and inverting the permutation) is impossible without some secret information. The problem of solving random system of nonlinear equations is known to be very hard (it is an NP-hard problem).

In papers [9] and [10] V. Ustymenko proposed a family of trapdoor one-way permutations based on the family of graphs of large girth $D(n, q)$. The main idea was to use random walks on these graphs as encryption tools. The vertices of the graph $D(n, q)$ are represented as the sequence of n elements of a finite field $\mathbb{F}_q$. The set of edges is defined by the system of polynomial equations. Consequently, the walk on the chosen path can be represented as a polynomial map $W : \mathbb{F}_q \to \mathbb{F}_q$. This map is further hidden using two invertible affine transformations A and B. The public information are the coefficients of the resulting polynomial map $E = B \circ W \circ A$. The secret information (trapdoor) is the walk on the graph and the affine transformations. Some aspects of the computer implementation of this family of permutations was given in [3], [4], [5] and [6].

In this talk we present the orignal construction of the graph based one-way permutation by V. Ustimenko. Next we show that this construction is not secure. We use the fact that the inverse of such permutation is a polynomial map of small degree. We show the way to recover the coefficients of this inverse without the knowledge of secret information by solving properly constructed large system of linear equations.

Finally we present the modification of the original construction. This modification results in a small decrease of efficiency of algorithms (generation of permutations, applying permutations). However the resulting permutation does not have the main defect of the original one — the degree of the inverse polynomial does not have to be small. The degree depends on the chosen finite field and we prove that we can choose a finite field, so that the degree was arbitrarily large.

References

1. Bernstein D.J., Buchmann J., Dahmen E. *Post-Quantum Cryptography.* Springer, 2009.

2. Ding J., Gower J.E., Schmidt D.S. *Multivariate Public Key Cryptosystems.* Advances in Information Security. Springer, 2006.

3. Klisowski M., Romanczuk U., Ustimenko V. The implementation of cubic public keys based on a new family of algebraic graphs // Annales UMCS, Informatica. 2011. V. 11. No. 2 P. 127–141.

4. Klisowski M., Ustimenko V. On the implementation of public keys algorithms based on algebraic graphs over finite commutative rings // Proceedings of the 2010 International Multiconference on Computer Science and Information Technology (IMCSIT) . 2010. P. 303–308

5. Klisowski M., Ustimenko V. On the implementation of cubic public keys based on algebraic graphs over the finite commutative rings and their symmetries // Albanian Journal of Mathematics. 2011. V. 5. No. 3, P. 139–149.

6. Klisowski M., Ustimenko V. On the comparison of cryptographical properties of two different families of graphs with large cycle indicator // Mathematics in Computer Science. 2012. V. 6. No. 2. P. 181–198.

7. Proos J., Zalka C. Shor's discrete logarithm quantum algorithm for elliptic curves // Quantum Information & Computation. 2003. V. 3. No.4. P. 317–344.

8. Shor P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM J. Comput. 1997. V. 26. No. 5. P. 1484–1509.

9. Ustimenko V.A. Graphs with special arcs and cryptography // Acta Applicandae Mathematicae. 2002. V. 74. No. 2. P. 117–153.

10. Ustimenko V.A. Maximality of affine group, and hidden graph cryptosystems // Algebra Discrete Math.. 2005. No. 1. P. 133–150.

CONSTRUCTION OF 4-CONNECTED GRAPHIC MATROIDS WITH ESSENTIAL ELEMENTS

P.P. Malavadkar[1], M.P. Gadiya[1], S.B. Dhotre[2], M.M. Shikare[2]

[1]MIT College of Engineering, Pune-411038, India
pmalavadkar@gmail.com, mahaveer.gadiya@mitcoe.edu.in
[2]Savitribai Phule Pune University, Pune-411007, India
dsantosh2@yahoo.co.in, mmshikare@gmail.com

An element e of an n-connected matroid M is called *essential element* if neither $M \setminus e$ nor M/e is n-connected. Tutte proved that in a 3-connected matroid M every element is essential if and only if M is wheel or whirl. We give construction of some families of 4-connected graphic matroids in which every element is essential.

CRITICAL HEREDITARY CLASSES FOR ALGORITHMIC GRAPH PROBLEMS

D.S. Malyshev

National Research University Higher School of Economics
25/12 Bolshaya Pecherskaya str., 603155 Nizhny Novgorod, Russia
dmalishev@hse.ru,dsmalyshev@rambler.ru

A *hereditary graph class* is a set of simple graphs closed under isomorphism and deletion of vertices. It is well-known that each hereditary class $\mathfrak{X}$ can be defined by a set of forbidden induced subgraphs $\mathfrak{Y}$, written $\mathfrak{X} = Free(\mathfrak{Y})$. If a hereditary class can be defined by a finite set of forbidden induced fragments, then it is called *finitely defined*. For example, the sets of line graphs and bounded degree graphs are finitely defined, but the sets of planar graphs and bipartite graphs do not.

Given an algorithmic graph problem, the problem of its complexity classification in the family of hereditary classes is of our attention. How to classify hereditary graph classes with respect to the complexity of a given problem? The first natural idea coming to mind is to consider phase transition between easy and hard hereditary classes under some definitions of easiness and hardness. It is like determining critical temperatures, when ice melts to water or water turns to steam. We know that the answer is zero and one hundred degrees Celsius, respectively. The phase-transition approach seams to be unsuccessful. For a given NP-complete graph problem Π, natural definitions of easy and hard instances are the following. A hereditary class is Π-*easy* if Π can be solved for its graphs in polynomial time. If Π is NP-complete for a hereditary class, then it is said

to be Π-*hard*. In fact, these notions were introduced in the paper of V.E. Alekseev [1], where the absence of maximal easy classes was also proved for any NP-complete graph problem. Minimal hard classes may exist or may not exist. It is easy to prove that the set of all complete graphs is a minimal hard case for the travelling salesman problem. The following result was proved in [2].

Theorem 1. *For each k, there are no minimal hard classes for the vertex and edge k-colorability problems.*

So, minimal hard classes could be called critical, as they play a specific role in the analysis of the computational complexity. But, they may be absent at all. In other words, both sets of easy and hard classes can be open with respect to the inclusion relation. That is why we consider the phase-transition approach to be useless.

To solve the major problem, we have to take into account the fact of the existence of infinite monotonically decreasing chains of hard classes. Intuitively, the limits of such kind sequences have a special role in the analysis of computational complexity. It is really true. This leads to the notion of a boundary class. A class $\mathcal{X}$ is Π-*limit* if there is an infinite monotonically decreasing chain $\mathcal{X}_1 \supseteq \mathcal{X}_2 \supseteq \ldots$ of Π-hard classes such that $\mathcal{X} = \bigcap\limits_{i=1}^{\infty} \mathcal{X}_i$. A minimal Π-limit class is said to be Π-*boundary*. This notion was introduced by V.E. Alekseev [1], who also proved the following theorem certifying its significance.

Theorem 2. *A finitely defined class is* Π*-hard if and only if it contains a* Π*-boundary class.*

By the theorem, if the set of all Π-boundary classes, called the Π-*boundary system*, is known, then, for the problem Π, we have a complete complexity dichotomy in the family of finitely defined classes. Moreover, any NP-complete graph problem has boundary classes. One more corollary is the fact that there are no finitely defined classes with an intermediate complexity, i.e. different from polynomial-time solvability and NP-completeness.

Assuming $P \neq NP$, one boundary class is known for the independent set problem [1], four boundary classes are known for the dominating set problem [3,4], two boundary classes are known for the Hamiltonian cycle problem [5]. Unfortunately, for all of the mentioned problems, there is no a complete description of a boundary system. Only one result of this type exists [6]. An idea arises that obtaining a complete description of the boundary system of a given graph problem may be a problem impossible to solve, because the structure of the answer is too complex. This is certified by the following result [5,7].

Theorem 3. *For each $k > 2$, the boundary systems for the vertex and edge k-colorability problems have the continuum cardinality.*

Sometimes, a known subset of a boundary system is enough to obtain a complexity dichotomy for some simple subfamily of the hereditary graph classes family. This idea really works sometimes. There is a dichotomy for the independent set problem within the family of classes defined by induced subgraphs with at most five vertices. Similar results exist for one forbidden induced structure for the dominating set problem [8] and the coloring problem [9]. There are some dichotomies for the vertex 3- and 4-colorability problems and one small forbidden induced structure [10,11]. There exist dichotomies for the vertex and edge 3-colorability problems and several small forbidden induced fragments [12,13].

The talk will be devoted to the results above and some other results in the theory of critical hereditary graph classes.

The article was prepared within the framework of the Academic Fund Program at the National Research University Higher School of Economics (HSE) in 2015–2016 (grant 15-01-0010) and supported within the framework of a subsidy granted to the HSE by the Government of the Russian Federation for the implementation of the Global Competitiveness Program.

References

1. Alekseev V.E. On easy and hard hereditary classes of graphs with respect to the independent set problem // Discrete Applied Mathematics. 2004. V. 132. No. 1–3. P. 17–26.

2. Malyshev D.S. On minimal hard classes of graphs // Diskretnyi Analiz i Issledovanie Operatsii. 2009. V. 16. No. 6. P. 43–51.

3. Alekseev V.E., Korobitsyn D.V., Lozin V.V. Boundary classes of graphs for the dominating set problem // Discrete Mathematics. 2004. V. 285. No. 1–3. P. 1–6.

4. Malyshev D.S. A complexity dichotomy and a new boundary class for the dominating set problem // Journal of Combinatorial Optimization. 2015. doi: 10.1007/s10878-015-9872-z.

5. Korpelainen N., Lozin V.V., Malyshev D.S., Tiskin A. Boundary properties of graphs for algorithmic graph problems // Theoretical Computer Science. 2011. V. 412. No. 29. P. 3545–3554.

6. Malyshev D.S. Critical graph classes for the edge list-ranking problem // Diskretnyi Analiz i Issledovanie Operatsii. 2013. V. 20. No. 6. P. 59–76.

7. Malyshev D.S. Continued sets of boundary classes of graphs for colorability problems // Diskretnyi Analiz i Issledovanie Operatsii. 2009. V. 16. No. 5. P. 41–51.

8. Korobitsyn D.V. On the complexity of domination number determination in monogenic classes of graphs // Discrete Mathematics and Applications. 1992. V. 2. No. 2. P. 191–199.

9. Kral' D., Kratochvil J., Tuza Z., Woeginger G. Complexity of coloring graphs without forbidden induced subgraphs // Lecture Notes in Computer Science. 2001. V. 2204. P. 254–262.

10. Broersma H., Golovach P., Paulusma D., Song J. Updating the complexity status of coloring graphs without a fixed induced linear forest// Theoretical Computer Science. 2012. V. 414. No. 1. P. 9–19.

11. Golovach P., Paulusma D., Song J. 4-coloring H-free graphs when H is small // Discrete Applied Mathematics. 2013. V. 161. No. 1–2. P. 140–150.

12. Malyshev D.S. The complexity of the edge 3-colorability problem for graphs without two induced fragments each on at most six vertices // Siberian Electronic Mathematical Reports. 2014. V. 11. P. 811–822.

13. Malyshev D.S. The complexity of the 3-colorability problem in the absence of a pair of small forbidden induced subgraphs // Discrete Mathematics. 2015 (accepted).

LOGICAL CHARACTERIZATIONS OF COMPLEXITY CLASSES

V.G. Naidenko

Institute of Mathematics, National Academy of Belarus,
11 Surganov str., 220072 Minsk, Belarus naidenko@open.by

Since 1974, descriptive complexity characterizes computational complexity in terms of logical languages. Fagin [1] first shown that the complexity class NP coincides with the set of problems expressible in second order existential (SO$\exists$) logic. Stockmeyer [2] extended Fagin's result to the polynomial-time hierarchy (PH) characterized by second order logic. Further research revealed logical characterizations for various complexity classes [3].

However, there are complexity classes such as PSPACE-complete problems, NP-complete problems, coNP-complete problems, P-complete problems, NL-complete problems, and NP $\cap$ coNP for which no logics were known till now. The purpose of our research is to develop logics for these classes.

Let us give necessary definitions. We use notations and definitions of finite model theory as stated in [4]. For convenience and without loss of generality, we consider vocabularies without constant symbols and without function symbols. So, a vocabulary is a finite set $\tau = \{R_1^{a_1}, \ldots, R_m^{a_m}\}$ of relation symbols of specified arities. A structure is a tuple $A = (|A|, R_1^A, \ldots, R_m^A)$, where $|A|$ is a nonempty finite set, and each R_i^A is a relation on A such that $\text{arity}(R_i^A) = a_i$, $1 \leq i \leq m$. By a model class we mean a set structures of a fixed vocabulary τ that is closed under isomorphism. By STRUC[τ] we denote the model class of all structures for the vocabulary τ.

We define a logic $\mathcal{L}$ as follows. For every vocabulary τ, the language $\mathcal{L}(\tau)$ is the recursive set of all well-formed sentences (whose elements are called $\mathcal{L}$-sentences) with the symbols of τ and with the symbols predefined for the logic $\mathcal{L}$. In addition, $\models$ is a binary relation between $\mathcal{L}$-sentences and structures, so that for each $\mathcal{L}$-sentence Γ with the vocabulary τ, the set $\{A \in \mathrm{STRUC}[\tau] \mid A \models \Gamma\}$ denoted by $\mathrm{MOD}[\Gamma]$ is a model class. Also, we say that a $\mathcal{L}$-sentence Γ defines a model class K if $K = \mathrm{MOD}[\Gamma]$.

We will characterize a model class as a complexity theoretic problem. Let $\mathcal{L}$ be a logic, $\mathcal{C}$ a complexity class, and τ a vocabulary. We say that $\mathcal{L}$ captures $\mathcal{C}$ if for every vocabulary τ, the following two conditions are satisfied:

1) For every $\mathcal{L}$-sentence Γ with the vocabulary τ, the model class $\mathrm{MOD}[\Gamma]$ belongs to $\mathcal{C}$.

2) For every model class $K \subseteq \mathrm{STRUC}[\tau]$ in $\mathcal{C}$, there exists a $\mathcal{L}$-sentence Γ that defines K.

Let us proceed to our results. First of all, note that it is very unlikely that one could construct a complete problem (for any reasonable complexity class) using structures which interpret only unary relation symbols. The argument is essentially that such classes of structures are interpretable with sparse languages for which it is highly improbable to find a complete problem. Therefore, we consider complete problems on structures containing at least one binary relation in what follows.

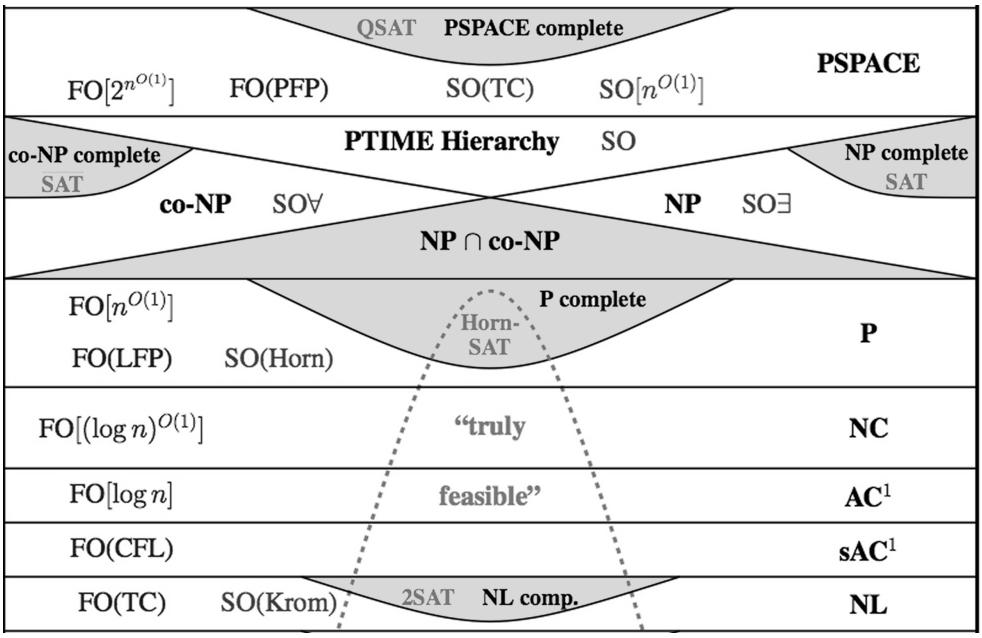


Fig. 1: The World of Computability and Complexity from NL to PSPACE
(a fragment of Immerman's diagram [3])

Let $\mathcal{C}$ denote one of the following complexity classes: NL, P, NP, coNP, and PSPACE if we allow linear order $<$ in structures and without linear order $<$ just the last three of them. The technique used in all cases is the same. We start out with a logic $\mathcal{L}$ that captures the complexity class $\mathcal{C}$ (for definiteness, by $\mathcal{L}$ we mean one of the following logics: FO(TC), FO(LFP), SO$\exists$, SO$\forall$, and SO(PFP), respectively). Then, for each $\mathcal{L}$-sentence Γ and for each Turing machine T, we take the sentence

$$(\gamma \wedge \Gamma) \vee (\neg\gamma \wedge \Upsilon) \tag{1}$$

where Υ is a fixed $\mathcal{L}$-sentence defining some $\mathcal{C}$-complete problem, and γ is constructed so that γ is satisfied for a structure A if and only if on all sufficiently small structures B (taking $\|B\| \leq \log\log\log\|A\|$ enough), the machine T witnesses that the models of Υ are reducible to those of Γ. It then follows that the sentence (1) defines a class which is the same as Γ if Γ defines a

$\mathfrak{C}$-complete problem and is finitely different from Υ otherwise. In the presence of linear order $<$, γ can be chosen to be a first-order sentence, while without linear order $<$ it can be chosen to be an existential sentence. Thus, there exist logics capturing complete problems in the complexity classes NL, P, coNP, NP, and PSPACE, based on the canonical form (1).

Besides, we extend our approach beyond complete problems. One can build a class of logical sentences that defines exactly the problems being in $\mathrm{NP} \cap \mathrm{coNP}$. The technique is analogous to the one above. For a pair (Λ, Γ) of sentences (Λ is universal second-order and Γ existential second-order), we take the existential second-order sentence

$$\gamma \wedge \Gamma \tag{2}$$

where γ is an existential second-order sentence constructed so that γ is satisfied for a structure A if and only if Λ and Γ are equivalent for all sufficiently small structures B (taking $\|B\| \leq \log\log\|A\|$ enough). Then, either γ is identically true, or γ defines a finite set. Therefore, $\mathrm{MOD}[\gamma \wedge \Gamma]$ is in $\mathrm{NP} \cap \mathrm{coNP}$. Thus, there exists a logic capturing $\mathrm{NP} \cap \mathrm{coNP}$, based on the canonical form (2).

In conclusion, we have modified a fragment of Immerman's diagram [3] in respect to the complexity classes from NL to PSPACE, as shown in Figure 1.

For purposes of clarity, in the diagram we have permitted ourself to shade areas depicting the following complexity classes: PSPACE-complete problems, NP-complete problems, coNP-complete problems, P-complete problems, NL-complete problems, and $\mathrm{NP} \cap \mathrm{coNP}$ for which we have developed logics for the first time.

References

1. Fagin R. *Generalized first-order spectra and polynomial-time recognizable sets* // Complexity of Computation, ed.: R. Karp. SIAM-AMS Proceedings. 1974. Vol. 7. P. 27–41.

2. Stockmeyer L. *The polynomial-time hierarchy* // Theoretical Computer Science. 1977. V. 3. P. 1–22.

3. Immerman N. *Diagram of the world of computability and complexity* [Electronic resource]. Mode of access: `http://people.cs.umass.edu/~immerman/descriptive_complexity.html`. Date of access: May 19, 2015.

4. Naidenko V. *Logics for complexity classes* // Logic Journal of the IGPL. 2014. V. 22. No 6. P. 1075–1093.

INTERVAL SELECTION PROBLEMS WITH LIMITED OVERLAP

Andrew Ryzhikov, Mikhail Y. Kovalyov

United Institute of Informatics Problems, National Academy of Sciences, Belarus
6 Surganov str., 220072, Minsk, Belarus
kovalyov_my@yahoo.co.uk, ryzhikov.andrew@gmail.com

1. Introduction. Let $\mathcal{I}$ be a finite set of intervals on the real line. We assume that the endpoints of all intervals have rational coordinates. Every element $I \in \mathcal{I}$ has a non-negative rational weight $w(I)$. A set of intervals is called *independent* if no two intervals in this set have a common interior point, and *k-independent* if it is a union of k pairwise disjoint independent sets. Here k is a non-negative integer number. In the problem Weighted k-Independent Set of Intervals the objective is to find a k-independent subset of $\mathcal{I}$ with maximum total weight. This problem is widely studied and has a lot of applications in interval scheduling, resource allocation, etc. For more details see surveys by Kovalyov et al. [1] and Kolen et al. [2]. It can be solved in polynomial time (Bouzina and Emmons [3]). We consider a generalization of this problem where the selected set of intervals must not be k-independent, but some overlap measure (which we call *composite u-redundancy*) of this set must be limited by a given number R. We define the composite u-redundancy in Section 2.

A special case of the Weighted 1-Independent Set of Intervals problem is the problem where the weight of every interval is equal to its length. For arbitrary positive k we generalize this problem in the following way.There is a set $\mathcal{I}$ of intervals on the real line and the objective is to find a k-independent subset of $\mathcal{I}$ with maximum measure of the union. We call this problem Maximum Coverage by k-independent Set of Intervals. We study this problem and also its generalization where the selected set must not be k-independent, but the composite u-redundancy of this set must be limited by a given number R.

2. Main definitions. Let u be a non-negative integer number and $\mathcal{J}$ be a subset of $\mathcal{I}$. We define the *set of projective u-redundancy* of $\mathcal{J}$ to be the set of such points on the real line that belong to at least $u+1$ intervals from $\mathcal{J}$. The measure of this set, that is, the total length of intervals in it, is called the *projective u-redundancy* of $\mathcal{J}$ and is denoted by $P(\mathcal{J}, u)$.

Further, let $x_1, \ldots, x_m$ be all the distinct left and right endpoints of intervals from $\mathcal{J}$ sorted in the increasing order. Let s_j be the number of intervals in $\mathcal{J}$ containing the interval $[x_j, x_{j+1}]$, $1 \le j \le m-1$. We define the *total u-redundancy* of the set $\mathcal{J}$ as

$$T(\mathcal{J}, u) = \sum_{j=1}^{m-1} \max\{(x_{j+1} - x_j) \cdot (s_j - u), 0\}.$$

Thus, in the projective u-redundancy, only one excessive interval of the intersection contributes to the redundancy value, and in the total u-redundancy all the excessive intervals of the intersection contribute to the redundancy value.

Let p and t be non-negative rational numbers such that $p + t > 0$. We define the *composite u-redundancy* of a set $\mathcal{J}$ to be the value $p \cdot P(\mathcal{J}, u) + t \cdot T(\mathcal{J}, u)$.

Both projective and total u-redundancy can be viewed as the measures that indicate the extent to which the set of intervals is not u-independent. In particular, the following lemma is true.

Lemma 1. *A finite set of intervals is k-independent if and only if its projective (or total) k-redundancy is equal to zero.*

3. Maximum weight selection problem. In the problem MaxWeight we are given three integer numbers u, p, and t, an upper bound R on the composite u-redundancy and a ground set $\mathcal{I} = \{I_1, \ldots, I_n\}$ of intervals. Each interval is associated with a non-negative rational weight. The objective is to select a subset $\mathcal{J} \subseteq \mathcal{I}$ of the maximum total weight, provided that its composite u-redundancy does not exceed R. For $R = 0$ this problem is precisely the Weighted u-Independent Set of Intervals problem.

The complexity of the MaxWeight problem is characterized by the following theorem.

Theorem 1. *The* MaxWeight *problem is NP-hard (in the ordinary sense) for any fixed u, p, t even if the weight of every interval is equal to its length and all endpoints of the intervals have integer coordinates.*

The next two theorems show that for any fixed u two restricted cases of the considered problem can be solved by pseudo-polynomial algorithms.

Theorem 2. *Let W be the total weight of all intervals in $\mathcal{I}$. There exists a pseudo-polynomial dynamic programming algorithm with running time $O(u^2 W n^{u+2})$ for the case where the weights of all intevals are integer numbers.*

Theorem 3. *There exists a pseudo-polynomial dynamic programming algorithm with running time $O(u^2(R+1)n^{u+2})$ for the case where the endpoints of all intervals have integer coordinates.*

It is an open question whether the general MaxWeight problem is strongly NP-hard or pseudo-polynomially solvable.

4. Maximum coverage selection problem. The problem MaxCoverage differs from the MaxWeight problem in that the criterion is to maximize the measure of the union of the selected intervals, that is, the total length of the intervals of this union. For $R = 0$ this problem is precisely the Maximum Coverage by u-independent Set of Intervals problem. The complexity of the MaxCoverage problem is characterized by the following theorem.

Theorem 4. *The* MaxCoverage *problem is NP-hard (in the ordinary sense) for arbitrary fixed non-negative rational numbers p and t, and for both $u = 0$ and $u = 1$.*

One special case of this problem can be solved in pseudo-polynomial time.

Theorem 5. *Let L be the union measure of all intervals in $\mathcal{I}$. There exists a pseudo-polynomial dynamic programming algorithm with running time $O(Ln^{u+2})$ for the case where $u \in \{0, 1\}$ and the endpoints of all intervals have integer coordinates.*

Theorem 6. *There exists a $\frac{1}{2}$-approximation algorithm with running time $O(n \log n)$ for the* MaxCoverage *problem with $u = 1$.*

We also prove that for the developed algorithm the number $\frac{1}{2}$ in this bound cannot be replaced with a larger constant.

According to the following theorem, the case $u \geq 2$ is much simpler.

Theorem 7. *There exists an algorithm with running time $O(n \log n)$ that finds a 2-independent subset $\mathcal{J}$ of intervals such that the union of the intervals in $\mathcal{J}$ coincides with the union of the intervals in $\mathcal{I}$.*

This implies that the problems MaxCoverage and Maximum Coverage by u-independent Set of Intervals are solvable in $O(n \log n)$ time for $u \geq 2$.

The work is partially supported by the Belarusian Republican Foundation for Fundamental Research under the grant number Ф15СО-043.

References

1. Kovalyov M.Y., Ng C.T., Cheng T.C.E. *Fixed interval scheduling: Models, applications, computational complexity and algorithms* // European Journal of Operational Research. 2007. V. 178. No. 2. P. 331–342.

2. Kolen A.W.J., Lenstra J.K., Papadimitriou C.H., Spieksma F.C.R. *Interval scheduling: A survey* // Naval Research Logistics. 2007. V. 54. No. 5. P. 530–543.

3. Bouzina K.I., Emmons H. *Interval Scheduling on identical machines* // Journal of Global Optimization. 1996. V. 9. No. 3–4. P. 379–393.

FAST ALGORITHM FOR 3D RECONSTRUCTION OF ANATOMICAL SURFACES FROM A SET OF CONTOURS OF RADIAL BONE

A.O. Sanakoyeu

Belarusian State University, Department of Applied Mathematics and Computer Science
4 Nezavisimosti Square, 220050, Minsk, Belarus a.sanakoyeu@gmail.com

Anatomical ultrasound (B-Mode ultrasound) is an essential diagnosing tool in medical practice, especially in pediatrics, cardiology and emergency, due to its high availability, absence of any risk both for patients and medical staff, compact size as well as low costs of examinations. The area of ultrasound applications can be easily extended utilizing the fact that this imaging technique has a relative high time resolution comparing with other medical image modalities. It allows to create real-time diagnosing tools in two, three and even in four dimensions. Musculoskeletal ultrasound is successfully applied for diagnosing injured extremities, as the most frequent trauma in children and adults [5]. Today, the high-end systems are able not only to to detect fractures of long bones as reposition of their fragments but, under special conditions, to help recognizing cracks and deformation of bone surfaces (cortical bones) [8] as well. However, the conventional clinical systems provide only manual approach called freehand ultrasound examinations [7]. A linear transducer (ultrasound head) is usually placed on the patient's skin using gel or over a gel pillow [2]. To acquire one or more sonograms (ultrasonic images) a diagnosing physician tries to find an optimal position and orientation of the transducer relative to the patient's anatomy. Then he or she applies some forces on the ultrasound head in the direction of the patient to avoid attenuation of ultrasound waves in air. The examination of musculoskeletal

structures can be carried out usually up to 10–15 cm of depth, depending on the transducer model, selected working wave frequency and quantity of patient's fat in the examination area. This approach has many serious drawbacks for the required diagnosing. Firstly, the examination produces additional pain for injured patients. Secondly, the procedure is very time-consuming. The diagnosing strongly depends on sonographic skills of the operator and is practically restricted for dimensions higher than two. More complex ultrasound scanners that can work in higher dimensions in semi-automatic or automatic modes are commercially available for acquisition of patient anatomy in gynaecology, echocardiography, endocrinology, etc. [1, 4]. They use either special (usually mechanical) transducers or linear transducers coupled with optical, magnetic or mechanical tracking systems. However, the application of similar scanners for examinations of long bones is not a simple task, due to a high variability of the bone anatomy, scattering and total reflection of ultrasound waves from bone surfaces. Developing new scanning principles, approaches to the rapid and accurate processing of the acquired data for analysing injured extremities remain being the challenging tasks, which are especially important for diagnosing injures in children, who are limited in their ability to remain immobile during the scanning time.

In this work we aim at a possible solution of the aforementioned problems for the task of diagnosing injures of long bones. The following results were obtained. Firstly, we created a software simulator of automated ultrasound-based 3D scanner UFASS (Ultrasound-based Fracture Analysis Scanning System, an improved robotized version of the scanner patented in [6]), which is able to acquire a series of realistic ultrasonic images of the long bones' cortical surfaces. Contours are represented by a reference 3D volumetric model of the human limb, obtained using Computed Tomography (CT). The proposed simulator is a virtual device intended for positioning and orienting of the virtual transducers in automatic mode relatively to the scanned 3D object (human limb) and image acquisition utilizing a cross-section of the scanned object and predefined physical properties of the ultrasound. The simulator allows to carry out experiments with realistic results without significant expenses of human and material resources. Secondly, we designed and implemented an efficient algorithm for 3D reconstruction of the anatomical surface of the radial bone using a set of mechanically tracked 2D sonograms. The algorithm includes the following ideas: tiling original data on a set of patches, building a space subdivision inside each patch (interpolating contours lying between pair of neighboring original contours), building a triangulation of each patch and stitching together the resulted surface patches into one mesh. The implementation of the algorithm utilizes kd-trees for the sufficient processing speed. The proposed approach works effectively on irregular, sparse and noisy data, obtained by the software simulator of automated ultrasound-based 3D scanner UFASS.

A series of experiments showed that our algorithm can successfully reconstruct surfaces from anatomical structures with relatively simple geometry (e.g. body of the radial bone) as well as surfaces from objects with more complex geometrical structure and higher curvature (e.g. metaphysis and epiphysis of distal radius), which could not be effectively handled by the prior algorithms [3]. The proposed algorithm reconstructs surfaces with relatively high accuracy, which was confirmed by the quantitative estimation of the root mean square (RMS) of the distances between points of the resulted mesh and points of the reference mesh, obtained from the CT-image of the same bone by the marching cubes algorithm, and the RMS of the distances between points of the not smoothed resulted mesh and the points of the smoothed one. The reconstructed surface correctly interpolates the initial data and demonstrates an appropriate smoothness. It is worth to note that the algorithm builds "almost" regular triangulation of the surface in the sense that almost all triangles have the same dimensions. Moreover, it was experimentally showed that due to the inherently smooth geometry of the radial bone it is possible to emphasize bone areas with possible fractures by calculating local distances from the not smoothed reconstructed surface to the smoothed reconstructed surface. And this potentially can speed up the process of detecting fractures in traumatology. For the visual perception of the experiments we implemented a graphical

representation of the results of comparing two meshes, where distances between corresponding points of compared meshes were mapped over a color space and used for visualization of the mesh reconstruction accuracy and locating fractures of the bone.

This work could not be possible without the exceptional contribution of Dr. Aleh Kryvanos. I would like to thank him for the invaluable scientific support and productive discussions during our collaboration.

References

1. *ACUSON S2000 ABVS 3D Total Breast Ultrasound Solution* // Siemens Healthcare. Mode of access: http://www.healthcare.siemens.com/ultrasound/radiology/acuson-s2000-abvs-ultrasound-system. Date of access: June 10, 2015.

2. Hacihaliloglu I., Abugharbieh R., Bodgson A.J., Rohling R.N. *Bone surface localization in ultrasound using image phase-based features* // Ultrasound in Med. & Biol. 2009. V. 35. No. 9. P. 1475–1487.

3. Hlidzich D. *Medical image analysis methods for anatomical surface reconstruction using tracked 3D ultrasound*. Dissertation, Ruperto-Carola University of Heidelberg, Germany, 2014.

4. Hung J., Lang R., Flachskampf F., Shernan S.K., McCulloch M.L., Adams D.B., Thomas J., Vannan M., Ryan T. *3D echocardiography: a review of the current status and future directions* // Journal of the American Society of Echocardiography. 2007. Vol. 20. No. 3. P. 213–233.

5. Kraus R., Schneidmüller D., Röder C. *Häufigkeit von Frakturen der langen Röhrenknochen im Wachstumsalter* // Dtsch Arztebl. 2005. V. 102. No. 12. P. 838–842.

6. Kryvanos A., Schwarz M., Obertacke U., Schleich D. *Vorrichtung zur Gewinnung von Bilddaten von knöchernen Strukturen, insbesondere zur Diagnose von Knochenfrakturen.* Patent. DE 102010014467 A1, June 2011.

7. Solberg O.V., Lindseth F., Torp H., Blake R.E., Nagelhus Hernes T.A. *Freehand 3D Ultrasound Reconstruction Algorithms — a Review* // Ultrasound in Med. & Biol. 2007. V. 33. No. 7. P. 991–1009.

8. Swiatek-Najwer E., Bedzinski R., Krowicki P., Krysztoforski K., Keppler P., Kozak J. *Improving surgical precision — application of navigation system in orthopedic surgery* // Acta of Bioengineering and Biomechanics. 2008. V. 10. No. 4.

ON DOUBLY CHORDAL GRAPHS

M. Talmaciu[1], **V.V. Lepin**[2]

[1] Vasile Alecsandri University of Bacau, România,
Department of Mathematics, Informatics and Education Sciences
mtalmaciu@ub.ro
[2] Institute of Mathematics, National Academy of Sciences of Belarus
11 Surganov str., 220072 Minsk, Belarus lepin@im.bas-net.by

The triangulated graphs (chordal) class has been noticed because of their properties. Among these properties we mention: perfection, recognition algorithms and ability to solve some combinatorial optimization problems (determining the stability number and minimum number of covering cliques) with linear complexity algorithms. Because of this, various ways of generalizing this notion were introduced.

Interest for strongly chordal (M. Farber [45], see [3], [5]. A graph G is strongly chordal if and only if every induced subgraph of G has a simple vertex. A vertex v of the graph G is simple in G if the set $\{N[u] : u \in N[v]\}$ is linearly ordered by inclusion.) graphs arises in several ways. The problems of locating minimum weight dominating sets and minimum weight independent dominating sets in strongly chordal graphs with real vertex weights can be solved in polynomial time, whereas each of these problems is NP-hard for chordal graphs.

Graphs with maximum neighborhood orderings were characterized and turned out to be algorithmically useful. These graphs are dual (in the sense of hypergraphs) to chordal graphs [1]. The graph G is *dually chordal* [1] iff G has a maximum neighborhood ordering. In [9] specifies that

the doubly chordal graphs holds: clique problem can be solved in polynomial time, independent set in linear time, the recognition problem in linear time.

Many problems efficiently solvable for strongly chordal and doubly chordal graphs remain efficiently solvable for dually chordal graphs too [2]. A. Brandstadt, V. Chepoi, F. Dragan, in [2] gives an algorithm for solving the connected r-domination and Steiner tree problem in linear time on doubly chordal graphs and in quadratic time on dually chordal graphs.

We say that v is simplicial in G if $N[v]$ is complete. A vertex $u \in N[v]$ is a *maximum neighbor* of v if for all $w \in N[v]$ the inclusion $N[w] \subseteq N[u]$ holds (note that $u = v$ is not excluded). A vertex v is *doubly simplicial* if it is simplicial and has a maximum neighbor. A graph is *doubly chordal* if it admits a *doubly perfect elimination ordering* $v_1, v_2, ..., v_n$ of vertices such that for each $1 \leq i \leq n$, v_i is doubly simplicial in the subgraph induced by $\{v_i, ..., v_n\}$.

A set $A \subset V(G)$ is called a *weak set* of the graph G if $N_G(A) \neq V(G) - A$ and $G[A]$ is connected. If A is a weak set, maximal with respect to set inclusion, then $G[A]$ is called a weak component.

Let $G = (V, E)$ be a connected and non-complete graph. If A is a weak set, then the partition $\{A, N(A), V \setminus A \setminus N(A)\}$ is called a *weak decomposition* of G with respect to A.

A graph G is *hereditary doubly chordal* if any induced subgraph of G is doubly chordal. A new characterization of hereditary doubly chordal graphs, using weakly decomposition, is given below.

Theorem. *Let $G = (V, E)$ be a connected and non-complete graph, $G[A]$ is a weak component. The graph G is hereditary doubly chordal if and only if the following hold: (1) $N(A)$ is clique; (2) $G - A - N(A)$, $G(A \cup N(A))$ are hereditary doubly chordal graphs.*

The above results lead to a recognition algorithm with running time $O(n(n+m))$ for hereditary doubly chordal graphs.

Corollary. *Let $G = (V, E)$ be a connected and non-complete graph with $G(A)$ a weak component in G. If G is hereditary doubly chordal then*

$$\alpha(G) = \max\{\alpha(G(A)) + \alpha(R), \alpha(G(A \cup N(A)))\};$$

$$\omega(G) = \max\{|N(A)| + \omega(R), \omega(G(A \cup N(A)))\},$$

where $R = G - A - N(A)$.

The Corollary implies an algorithm with running time $O(n(n + m))$ for the construction of a stable set of maximum cardinal and a clique of maximum cardinal in a hereditary doubly chordal graph.

References

1. Brandstadt A., Dragan F., Chepoi V., Voloshin V. *Dually chordal graphs* // SIAM J.Discrete Math. 1998. Vol. 11, P. 437–455.

2. Brandstadt A., Chepoi V., Dragan F. *The algorithmic use of hypertree structure and maximum neighbourhood orderings* // Discrete Applied Mathematics 1998. Vol. 82, P. 43–77.

3. Dahlhaus E., Manuel P.D., Miller M. *A characterization of strongly chordal graphs*, // Discrete Mathematics 1998. Vol. 187, P. 269–271.

4. Farber M., *Characterizations of Strongly Chordal Graphs* // Discrete Mathematics 1983. Vol. 43, P. 173–189.

5. McKee T. A., *A new characterization of strongly chordal graphs* // Discrete Mathematics 1999. Vol. 205, P. 245–247.

6. Moscarini M., *Doubly chordal graphs. Steiner trees and connected domination* // Network 1993. Vol. 2.3, P. 59–69.

7. Talmaciu M., Croitoru C. *Structural Graph Search* // Stud.Cercet.Stiint., Ser.Mat., 16 (2006), Supplement, Proceedings of ICMI 45, Bacau, Sept.18-20, 2006, P. 573–588

8. Talmaciu M., *Fast algorithms of dually chordal graphs* // Scientific Studies and Research, Series Mathematics and Informatics, 2015. Vol. 25, No. 1, P. 77–86.

9. http://www.graphclasses.org/classes/gc_181.html

ON THE NEW APPLICATIONS OF ALGEBRAIC GRAPH THEORY TO MULTIVARIATE CRYPTOGRAPHY

V.A. Ustimenko[1], U. Romańczuk-Polubiec[2], A. Wróblewska[1], M. Polak[1]

[1] The University of Maria Curie Sklodowska, Institute of Mathematics,
pl. Marii Curie-Skiodowskiej 1, 20-031 Lublin, Poland,
vasyl@hektor.umcs.lublin.pl, awroblewska@hektor.umcs.lublin.pl, monika.katarzyna.plak@gmail.com
[2] The Independent Polish Researcher, urszula_romanczuk@yahoo.pl

Presented research of authors is partially supported through the project "Scientific fellowships for PhD students working in research teams", which is realized by Self-Ggovernment of the of Lubelskie Voivodeship and Regional Operational Programme Department of the Marshal's Office of Lubelskie Voivodeship in Lublin, Poland, within the framework of Sub-measure 8.2.2 Regional Innovation Strategies, Measure 8.2 Transfer of knowledge, Priority VIII Regional human resources for the economy Human Capital Operational Programme co-financed by European Social Fund and state budget. The authors team together with the firm LabSQL.pl collaborate on the above project.

The RSA is one of the most popular cryptosystems. It is based on number factorisation problem and Euler Theorem. Peter Shor discovered that factorisation problem can be effectively solved with the usage of theoretical quantum computer. It means that RSA could not be a security tool in the future postquantum era. One of the research directions which can lead to a postquantum secure public key is the Multivariate Cryptography which uses a polynomial maps of affine space K^n defined over a finite commutative ring into itself as encryption tools (see [1]). This is a young promising research area with the current lack of known cryptosystems with the proven resistence against attacks with the use of Turing machines. Other important direction of Postquantum Cryptography is the studies of Elliptic Curves cryptosystems.

Applications of Algebraic Graph Theory to Multivariate Cryptography were observed in our talks at Erdos Centennial (2013, Budapest) and Central European Conference on Cryptology 2014 (Alfred Renyi Institute, Budapest) [2, 3]. This talk was devoted to algorithms based on bijective maps of affine spaces into itself. Applications of algebraic graphs to cryptography started from symmetric algorithms based on explicit constructions of extremal graph theory and their directed analogue (see survey [4, 5]). The main idea is to convert an algebraic graph in finite automaton and use the preudorandom walks on the graph as encryption tools. This approach can be also used for the key exchange protocols. Nowadays the idea of "symbolic walks" on algebraic graphs when the walk on the graph depends on parameters given as special multivariate polynomials in variables depending from plainspace vector brings several public key cryptosystems. Other source of graphs suitable for cryptography is connected with finite geometries and their flag system (see [4], [11] and further references).

Our presentation at DIMA 2015 includes new cryptoalgorithms in terms of Algebraic Combinatorics which use non bijective transformations of K^n.

Multivariate cryptography started from studies of potential for the special quadratic encryption multivariate bijective map of K^n, where K is an extention os finite field F_q of characteristic 2. One of the first such cryptosystems were proposed by Imai and Matsumoto, cryptanalysis for this system was invented by J. Patarin. The survey on various modifications of this algorithm and corresponding cryptanalysis the reader can find in [1]. Bijective multivariate sparse encryption maps of rather high degree based on walks in algebraic graphs were proposed in [6].

One of the first usage of non bijective map of multivariate cryptography was in *oil and vinegar* crytosystem proposed in [7] and analysed in [8]. Nowadays this general idea is strongly supported by publication [9] devoted to security analysis of direct attacks on modified unbalanced oil and vinegar systems. It looks like such systems and rainbow signatures schemes may lead to promising Public Key Schemes of Multivariate Encryption defined over finite fields. Non bijective multivariate

sparse encryption maps of degree 3 and ≥ 3 based on walks on algebraic graphs $D(n, K)$ defined over general commutative ring and their homomorphic images were proposed in [10].

The new cryptosystems with non bijective multivariate encryption maps on the affine space ${Z_m}^n$ into itself will be presented. It uses the plainspace ${Z_m^*}^n$, where $n = k(k-1)/2$, $k \geq 2$ can be arbitrary natural number. The private key space is formed by sequence of general multivariate polynomials from $Z_m[x_1, x_2, \ldots, x_{k-1}]$ and sequence of parameters l_i, $i = 1, 2, \ldots, k-1$ which are mutually prime with $\phi(m)$. The properties of the encryption map depends heavily on the prime factorisation of m. This non bijective encryption map is the deformation of special computation generated by Schubert automaton of "$k-1$ dimensional projective geometry" over Z_m. This method does not use the partition of variables into groups, non bijective nature of the map caused by zero devisors of composite integer m. In fact the idea of multiple "hidden RSA" is used.

This algorithm is a modification of public key cryptosystem based on the computation of Tits automaton in the case of finite projective geometry [11], which were presented at the conference ALCOMA 2015.

The talk is dedicated to the memory of D. A. Suprunenko whose research is an inspirational example of multifaceted work in Pure and Applied Mathematics in areas of Algebra and Discrete Mathematics.

References

1. Ding J., Gower J. E., Schmidt D. S. *Multivariate Public Key Cryptosystems*. Springer. Advances in Information Security. V. 25. 2006.

2. Polak M., Romańczuk U., Ustimenko V., Wróblewska A. On the applications of Extremal Graph Theory to Coding Theory and Cryptography // Erdős Centennial, Proceedings of Erdős Centennial (EP 100). Electronic Notes in Discrete Mathematics. 2013. V. 43. P. 329–342.

3. Ustimenko V. A. Explicit constructions of extremal graphs and new multivariate cryptosystems // Studia Scientiarum Mathematicarum Hungarica, Special issue "Proceedings of The Central European Conference, 2014, Budapest" (to appear in 2015).

4. Ustimenko V. A. Graphs with Special Arcs and Cryptograph // Acta Applicandae Mathematicae. 2002. V. 71. No 2. P. 117–153.

5. Ustimenko V. On the extremal graph theory for directed graphs and its cryptographical applications // In: T. Shaska, W.C. Huffman, D. Joener and V. Ustimenko. Advances in Coding Theory and Cryptography. Series on Coding and Cryptology. 2007. V. 3. P. 181–200.

6. Ustimenko V. On Multivariate Cryptosystems Based on Computable Maps with Invertible Decompositions // Annales of UMCS. Informatica (special issue "Proceedings of International Conference Cryptography and Security Systems"). 2014. V. 14. P. 7–18.

7. Patarin J. The Oil i Vinegar digital signatures // Dagstuhl Workshop on Cryptography. 1997.

8. Kipnis A., Shamir A. Cryptanalisis of the Oil and Vinegar Signature Scheme // Advances in Cryptology, Crypto 96. Lecture Notes in Computer Science. 1996. V. 1462. P. 257–266.

9. Bulygin S., Petzoldt A., Buchmann J. Towards provable security of the unbalanced oil and vinegar signature scheme under direct attacks // In "Progress in Cryptology, INDOCRYPT", eds.: Guang Gong, KishanChand Gupta editors, Lecture notes in Computer Science. 2010. V. 6498. P. 17–32.

10. Romańczuk-Polubiec U., Ustimenko V. On two windows multivariate cryptosystem depending on random parameters // Algebra and Discrete Mathematics. 2015. V. 19. No. 1. P. 101–129.

11. Ustimenko V. A. On the flag geometry of simple group of Lie type and Multivariate Cryptography // Algebra and Discrete Mathematics. 2015. V. 19. No 1. P. 130–144.

СОДЕРЖАНИЕ

Алгебра и алгебраическая геометрия

Дискретная математика и математическая кибернетика

Научное издание

Дискретная математика, алгебра и их приложения

Тезисы докладов

Редакторы *И. Д. Супруненко, В. В. Лепин, О. И. Дугинов*
Компьютерная верстка *О. И. Дугинов*

Подписано в печать 26.8.2015 г.
Формат $60 \times 84\,{}^{1}/_{8}$. Усл. печ. л. 20,46. Уч.-изд. л. 18,32. Тираж 110 экз. Заказ № 3.

Отпечатано на ризографе Института математики НАН Беларуси.
Издатель и полиграфическое исполнение:
Институт математики НАН Беларуси.
Свидетельство о государственной регистрации
издателя, изготовителя, распространителя печатных изданий
№ 1/257 от 2 апреля 2014 г.
200072, Минск, ул. Сурганова, 11.