## 4. Experiments

The research [2] describes classes $M_n$ of feedback functions of the aforementioned kind for $4 \leq n \leq 27$ that correspond to the shift registers with the cycle of length $2^n - 1$. The absence of non-trivial affine functions in the set $R(f_{n-2})$ for $4 \leq n \leq 24$ is empirically verified in this research. Thus taking into account Corollary 2 it can be concluded that for any feedback function $g \in M_n$ the outcome of a corresponding shift registers contains no affine functions.

It was also determined that for $n = 4$ the outcome of a shift register contains no affine functions.

In case of $n = 5$ there exist non-linear functions $f$ providing the presence of affine functions $L(x)$ in the set $R(f)$.

Example: $n = 5$ $f(x) = x_1 + x_2 + x_2x_4 + x_2x_3x_4 + x_5 + x_2x_5 + x_2x_3x_5$,
$g_{23} = L(x) = x_1 + x_3 + x_5$.

### СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Golomb S. W. Shift Register Sequences. — Laguna Hills, California: Aegean Park Press, 1982.

2. Rozhkov M. I. On some classes of nonlinear shift registers with the same cyclic structure // Discrete Mathematics and Applications. 2010. № 20(2). C. 127-155.

3. Zhao X. X, Tian T., Qi W. F. Ring-like cascade connection and a class of NFSRs with the same cycle structures // Designs, Codes and Cryptography. 2018. № 86(2). C. 1-16.

4. Ma Z., Qi W. F., Tian T. On the decomposition of an NFSR into the cascade connection of an NFSR into an LFSR // Journal of Complexity. 2013. № 29(2). C. 173-181.

5. Zang J. M., Qi W. F., Tian T., Wang Z. X. Further Results on the decomposition of an NFSR into the cascade connection of an NFSR into an LFSR // IEEE Transactions on Information Theory. 2015. № 61(1). C. 645-654.

6. Rothaus O. S. On bent functions // Journal of Combinational Theory. 1976. № 20(3). C. 300-305.

———————————————————————

УДК 511.1

## Быстрое перечисление рациональных чисел и задачи биоинформатики[1]

**А. В. Селиверстов (Россия, г. Москва)**
Институт проблем передачи информации им. А.А. Харкевича Российской академии наук
e-mail: slvstv@iitp.ru

## Fast enumeration of rational numbers and bioinformatics problems

**A. V. Seliverstov (Russia, Moscow)**
Institute for Information Transmission Problems of the Russian Academy of Sciences (Kharkevich Institute)

[1]Исследование выполнено при финансовой поддержке РФФИ № 18-29-13037

e-mail: slvstv@iitp.ru

Известны биекции между множествами рациональных и натуральных чисел, вычислимые за полиномиальное время [1, 2, 3]. Мы приведём ещё один способ нумерации, а также рассмотрим возможность его обобщения на другие случаи, включая нумерацию рациональных функций от одной переменной над полем. Близкие задачи возникают в биоинформатике, в частности, при оценке вероятности случайного совпадения рассматриваемых последовательностей, а также геномных структур или графов [4].

Через $\omega$ обозначим множество всех натуральных чисел $\{0, 1, \dots\}$, начиная с нуля. Натуральные числа отождествляются с их двоичными записями. Длина двоичной записи числа $n \in \omega$ равна $\lceil \log_2(n+1) \rceil$. Многочлены отождествляются с последовательностями их коэффициентов относительно лексикографического мономиального упорядочения. Для любого множества двоичных слов $X \subset \{0,1\}^*$ биекция $f : X \to \omega$ называется полиномиально вычислимой, если обе функции $f$ и обратная $f^{-1}$ вычислимы за полиномиальное время (на машине Тьюринга). Значение функции $f$ называется номером слова. Говоря о полиномиальной вычислимости функции на множестве $X \subset \{0,1\}^*$, мы подразумеваем, что соответствующая машина Тьюринга останавливается независимо от поданного на вход слова. Но если вход не принадлежит множеству $X$, то машина за полиномиальное время переходит в выделенное состояние VAGUE и останавливается. При этом содержание рабочей ленты может быть любым. Если же на вход подано слово из множества $X$, то машина не приходит в состояние VAGUE.

Например, существует полиномиально вычислимая биекция между множеством всех двоичных слов $\{0,1\}^*$ и множеством всех натуральных чисел $\omega$. Опишем некоторые полиномиально вычислимые биекции, которые будут использоваться. Обозначим через

$$\langle x, y \rangle = \frac{(x+y)^2 + 3x + y}{2}$$

номер пары натуральных чисел $x$ и $y$ при канторовской нумерации. По номеру пары каждое из двух чисел $x$ и $y$ вычисляется за полиномиальное время.

Индукцией по числу элементов $n$ определим номер последовательности из ровно $n \geqslant 1$ натуральных чисел. При $n = 1$ номер последовательности из одного числа равен этому числу. При $n > 1$ он равен номеру пары $\langle a, b \rangle$, где $a$ — номер подпоследовательности первых $\lceil n/2 \rceil$ членов, $b$ — номер подпоследовательности оставшихся членов. В частности, номер последовательности из двух элементов равен номеру пары. Номер последовательности из $n$ нулей равен нулю. Делить исходную последовательность посередине полезно для быстрой вычислимости номера. Такое вычисление соответствует пути длины $O(\log_2 n)$ в дереве номеров подпоследовательностей. На каждом ребре происходит вычисление номера пары. При этом длина двоичной записи номера пары не превышает суммы константы и удвоенной длины двоичной записи большего из элементов пары. После $O(\log_2 n)$ шагов размер двоичной записи номера остаётся ограниченным сверху некоторым многочленом от длины последовательности $n$ и от максимума длин двоичных записей элементов.

Номер последовательности неопределённой нечётной длины равен номеру пары $\langle n, m \rangle$ в случае, когда последовательность состоит из $2n+1$ чисел, а её номер среди всех последовательностей из $2n+1$ числа равен $m$. В частности, номер последовательности из одного нуля равен $\langle 0, 0 \rangle = 0$. Однако номер тройки нулей равен $\langle 1, 0 \rangle = 2$.

Термин *непрерывная дробь* введён Джоном Валлисом (John Wallis), но эти дроби применяли до него [5]. Каждое положительное рациональное число единственным способом разложимо в конечную обыкновенную непрерывную дробь

$$[a_0, \dots, a_{2m+1}] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}},$$

где все числа $a_k \in \omega$ и все кроме $a_0$ положительные [6]. Требование нечётности последнего индекса обеспечивает единственность, поскольку для каждого индекса $\ell$ выполнено $[a_0, \ldots, a_\ell + 1] = [a_0, \ldots, a_\ell, 1]$.

Итак, рациональные числа из открытого интервала $(0, 1)$ взаимно однозначно соответствуют непрерывным дробям вида $[0, a_1, \ldots, a_{2m+1}]$. В свою очередь эти дроби взаимно однозначно соответствуют последовательностям нечётной длины, состоящим из натуральных чисел $(a_1 - 1, \ldots, a_{2m+1} - 1)$. Такие последовательности нумеруются за полиномиаьное время. Разложение дроби в обыкновенную непрерывную дробь также вычислимо за полиномиальное время. Так получается следующий результат.

Теорема 1. *Существует полиномиально вычисимая биекция между множествами рациональных чисел из открытого интервала* $(0, 1)$*, каждое из которых задано парой взаимно простых числителя и знаменателя, и всех натуральных чисел* $\omega$.

Отсюда легко получается взаимно однозначная полиномиально вычислимая нумерация всех рациональных чисел, каждое из которых однозначно соответстует паре из целой и дробной частей.

Над бесконечным полем общая (почти любая) рациональная функция от одной переменной $x$ разлагается в конечную непрерывную дробь вида

$$\cfrac{a_1}{a_0 + \cfrac{a_2 x}{a_1 + \cfrac{a_3 x}{a_2 + \ldots}}},$$

где $a_k$ принадлежит полю коэффициентов [7]. Не каждая рациональная функция допускает такое разложение, а когда непрерывная дробь существует, её коэффициенты могут иметь очень большой размер, что служит препятствием для полиномиальной вычислимости.

## СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ


1. Calkin N., Wilf H. S. Recounting the rationals // The American Mathematical Monthly. 2000. Vol. 107, no. 4. P. 360–363. DOI: 10.2307/2589182

2. Backhouse R., Ferreira J. F. Recounting the rationals: twice! // Audebaud P., Paulin-Mohring C. (eds) Mathematics of Program Construction. MPC 2008. Lecture Notes in Computer Science, vol. 5133. Springer, Berlin, Heidelberg, 2008, pp. 79–91. DOI: 10.1007/978-3-540-70594-9

3. Bates B., Bunder M., Tognetti K. Linking the Calkin–Wilf and Stern–Brocot trees // European Journal of Combinatorics. 2010. Vol. 31, no. 7. P. 1637–1661. DOI: 10.1016/j.ejc.2010.04.002

4. Горбунов К. Ю., Любецкий В. А. Линейный алгоритм перестройки графа // Автоматика и телемеханика. 2018. Том 79, № 12. С. 124–141. DOI: 10.31857/S000523100002861-1,

5. Cretney R. The origins of Euler's early work on continued fractions // Historia Mathematica. 2014. Vol. 41. P. 139–156. DOI: 10.1016/j.hm.2013.12.004

6. Morier-Genoud S., Ovsienko V. Farey boat: continued fractions and triangulations, modular group and polygon dissections // Jahresbericht der Deutschen Mathematiker-Vereinigung. 2019. Vol. 121. P. 91–136. DOI: 10.1365/s13291-019-00197-7

7. Демидович Б. П., Марон И. А. Основы вычислительной математики. — М.: Наука, 1966. 688 с.