НЕРАЗВЕТВЛЕННОЕ ВЫНУЖДЕНИЕ *)

1. Введение

Метод вынуждения был придуман Коэном для решения некоторых классических проблем независимости. Как только стало ясно, что сам метод применим в гораздо более общих случаях, специалисты по теории множеств упростили и обобщили этот метод. Одним из результатов таких попыток являются булевозначные модели, исследуемые в статье Скотта и Соловея **).

Характерная черта булевозначного подхода состоит в том, что использование разветвленной иерархии конструктивных множеств становится ненужным. Так как модели вынуждения могут быть получены из булевозначных моделей, то очевидно, что эта иерархия не нужна также и для моделей вынуждения.

Одна из целей настоящей статьи — дать прямую конструкцию моделей вынуждения, не использующую разветвленную иерархию. В дополнение к этому я попытался дать сводку некоторых упрощений и обобщений теории вынуждения, упомянутой выше. Многие из этих результатов в настоящее время содержатся лишь в малодоступных источниках.

Было бы невозможно перечислить всех лиц, добившихся каких-либо продвижений в этой проблематике. Наши исторические справки будут по крайней мере указывать, кем были получены основные результаты. Общая картина заимствована из заметок Скотта и Сильвера **) и лекций Роуботтома в Калифорнийском университете, прочитанных осенью 1967 г. Беседы с Чжаном и Роуботтомом были также очень полезны.

---

*) J. R. Shoenfield, Unramified forcing, Proc. Symp. Pure Math. **13**, № 1 (1971), 357—380.

) Статьи Скотта и Соловея, Скотта и Сильвера публикуются в Proc. Symp. Pure Math. **13, №1, №2.

2. Предварительные сведения

Здесь мы перечислим основные результаты теории множеств, которые нам нужны.

Обозначим через ZF аксиоматическую систему Цермело — Френкеля (аксиомы объемности, регулярности, бесконечности, объединения, замены и степени), а через ZFC систему ZF с аксиомой выбора. При рассмотрении функций как некоторых множеств упорядоченных пар мы считаем, что значение функции есть первая, а аргумент функции — вторая компонента упорядоченной пары. Таким образом, областью значений (областью определения) f является множество первых (вторых) элементов упорядоченных пар из f. Обозначения: $U(x)$ — объединение всех множеств из x, $S(x)$ — множество степени множества x, $\langle x, y\rangle$ — упорядоченная пара, $\mathrm{Ra}(x)$ — область значений множества x, $\mathrm{Do}(x)$ — область определения множества x, ${}^x y$ — множество всех отображений из множества x в y.

Мы отождествляем ординал с множеством предшествующих ординалов, а кардинал с наименьшим ординалом, имеющим заданную мощность (таким образом, $\aleph_\alpha = \omega_\alpha$). Греческие буквы используются для обозначения ординалов, а готические — для обозначения бесконечных кардиналов (или бесконечных мощностей моделей). Через $|x|$ будем обозначать мощность (кардинал) множества x и через $\mathfrak{m}^+$ — следующий за $\mathfrak{m}$ кардинал. Напомним, что $\mathrm{cf}(\alpha)$ означает наименьшее β такое, что существует отображение β на конфинальное подмножество из α. Бесконечный кардинал $\mathfrak{m}$ называется *регулярным*, если $\mathrm{cf}(\mathfrak{m}) = \mathfrak{m}$, и *сингулярным*, если $\mathrm{cf}(\mathfrak{m}) < \mathfrak{m}$. В любом случае $\mathrm{cf}(\alpha)$ всегда равно 1 или является регулярным кардиналом. Если $\mathfrak{m}$ — регулярный кардинал, то объединение $< \mathfrak{m}$ множеств, мощность каждого из которых $< \mathfrak{m}$, имеет мощность $< \mathfrak{m}$. Через $S_{\mathfrak{m}}(x)$ обозначаем $[y \mid y \subset x \mathbin{\&} |y| < \mathfrak{m}]$.

$V(\alpha)$ (иногда используется обозначение $R(\alpha)$) определяется трансфинитной индукцией следующим образом:

$$V(\alpha) = \bigcup_{\beta<\alpha} S(V(\beta)).$$

Рангом множества x, обозначаемым через $\mathrm{rk}(x)$, называется наименьшее α такое, что $x \in V(\alpha+1)$. Это понятие всюду определено и из $x \in y$ следует $\mathrm{rk}(x) < \mathrm{rk}(y)$. Более того, $\mathrm{rk}(\alpha) = \alpha$.

Мы предполагаем известными некоторые факты элементарной арифметики кардиналов. Напомним, что

$$|{}^x y| = |y|^{|x|}, \qquad |S(x)| = 2^{|x|}.$$

Теорема Кёнига утверждает, что $\mathrm{cf}(2^{\mathfrak{m}}) > \mathfrak{m}$. Обозначим через GCH обобщенную гипотезу континуума: $\forall \mathfrak{n}\, (2^{\mathfrak{n}} = \mathfrak{n}^{+})$. *Слабые степени* определяются следующим образом:

$$\mathfrak{m}^{\mathfrak{n})} = \sum_{\mathfrak{p} < \mathfrak{n}} \mathfrak{m}^{\mathfrak{p}}.$$

(Здесь мы допускаем случай, когда $\mathfrak{p}$ конечны, но эти члены могут быть опущены, если $\mathfrak{n} > \aleph_0$.) Тогда $\mathfrak{m}^{\mathfrak{n}^{+})} = \mathfrak{m}^{\mathfrak{n}}$. Так как каждое подмножество множества x мощности $\mathfrak{p}$ является областью значений некоторого элемента из ${}^{\mathfrak{p}}x$, то мы имеем $|S_{\mathfrak{n}}(x)| \leqslant |x|^{\mathfrak{n})}$.

Имеем

$$\mathfrak{n} < \mathrm{cf}(\mathfrak{m})\ \&\ \forall \mathfrak{p} < \mathfrak{m}\, (2^{\mathfrak{p}} \leqslant \mathfrak{m}) \rightarrow \mathfrak{m}^{\mathfrak{n}} = \mathfrak{m}. \tag{2.1}$$

Действительно, из $\mathfrak{n} < \mathrm{cf}(\mathfrak{m})$ следует ${}^{\mathfrak{n}}\mathfrak{m} = \bigcup_{\alpha < \mathfrak{m}} {}^{\mathfrak{n}}\alpha$. Однако $|{}^{\mathfrak{n}}\alpha| = |\alpha|^{\mathfrak{n}} \leqslant 2^{|\alpha| \cdot \mathfrak{n}} \leqslant \mathfrak{m}$ по предположению, поэтому $\mathfrak{m}^{\mathfrak{n}} \leqslant \mathfrak{m} \cdot \mathfrak{m} = \mathfrak{m}$. Если GCH выполняется, то утверждение (2.1) сводится к $\mathfrak{n} < \mathrm{cf}(\mathfrak{m}) \rightarrow \mathfrak{m}^{\mathfrak{n}} = \mathfrak{m}$. Из (2.1) следует, что

$$\mathfrak{m} \text{ регулярное } \& \forall \mathfrak{p} < \mathfrak{m}\, (2^{\mathfrak{p}} \leqslant \mathfrak{m}) \rightarrow \mathfrak{m}^{\mathfrak{m})} = \mathfrak{m}.$$

Так, например, если $\mathfrak{m}$ есть $\aleph_0$, то $\mathfrak{m}^{\mathfrak{m})} = \mathfrak{m}$ является сильно недостижимым, и если GCH выполняется, то $\mathfrak{m}^{\mathfrak{m})} = \mathfrak{m}$ для всех регулярных $\mathfrak{m}$.

Обратимся теперь к моделям теории множеств. Модель называется *транзитивной*, если ее универсум является транзитивным множеством и ее предикат принадлежности является обычным предикатом принадлежности, ограниченным до ее универсума. Метод сжатия М о с т о в с к о г о [8] показывает, что каждая вполне фундированная модель аксиомы объемности изоморфна транзитивной модели. В дальнейшем под моделью мы будем понимать транзитивную модель и будем отождествлять модель с ее универсумом.

Пусть M — некоторая модель. Чтобы отметить, что какой-то объект рассматривается в модели M, мы будем добавлять фразу «в M» или верхний индекс M. Так, если Φ — предложение (возможно, содержащее имена элементов из M), то будем сокращать фразу «Φ истинно при интерпретации в M» до «Φ выполняется в M» или просто до Φ^M.

Кардиналом в M называется элемент a из M такой, что «a есть кардинал» выполняется в M. Через ω_1^M мы обозначаем элемент a из M такой, что $\Phi(a)^M$, где $\Phi(x)$ — предложение теории множеств, утверждающее, что x есть ω_1. Подобным же образом интерпретируются и другие примеры.

Классом в M называется множество $[a \mid a \in M \& \Phi(a)^M]$, где $\Phi(x)$ содержит только символы языка теории ZFC и символы для множеств из M. Каждое множество из M есть класс в M. Если M — модель теории ZFC, то каждый класс в M, который включается в некоторое множество из M, сам является множеством из M. *Функционалом в M* называется функция F такая, что для некоторой формулы $\Phi(x, y)$ описанного выше типа $F(a) = b$ тогда и только тогда, когда $a, b \in M$ и $\Phi(a, b)^M$. Если M — модель теории ZFC, то образ множества из M относительно функционала в M есть множество из M.

Л е м м а 2.1. *Каждое транзитивное множество M, удовлетворяющее следующим четырем условиям, является моделью теории* ZF.

(а) $\omega \in M$.

(б) *Каждый класс в M, который включается в некоторое множество из M, сам является множеством из M.*

(в) *Для каждого функционала F в M и каждого множества a из M, включенного в область определения функционала F, множество $U([F(b) \mid b \in a])$ включено в некоторое множество из M.*

(г) *Для каждого множества a из M множество $S(a) \cap M$ включается в некоторое множество из M.*

Предикатный символ P, определяемый в теории ZFC, называется *абсолютным*, если для каждой модели M теории ZFC предикат P^M совпадает с P на аргументах из M. Подобное определение вводится для функциональных символов (в том числе и для констант как функциональных символов с нулевым числом аргументов). Большинство символов, введенных при изучении ординалов, абсолютны, за исключением S. Детали смотри в [9] или в данной книге. Если F абсолютный, то F принимает значения из M (так как F^M таков). Из абсолютного предиката « ... есть ординал» следует, что ординалы в M являются настоящими ординалами, принадлежащими M.

Аксиома конструктивности (см. [5]) утверждает, что каждое множество конструктивно. Отсюда следует, что существует определяемое вполне упорядочение универсума и что выполняется GCH. Если M — модель теории ZFC, то конструктивные множества в M образуют модель теории ZFC с аксиомой конструктивности. Каноническая функция, отображающая ординалы на конструктивные множества, абсолютна, поэтому конструктивные множества в некоторой модели M теории ZFC являются образами ординалов в M относительно этой функции. Таким образом, если M и N имеют одинаковые ординалы, то они имеют и одинаковые конструктивные множества.

3. Понятия вынуждения

Предположим, что M — модель теории ZFC и a, $b \in M$. Мы хотим расширить M до модели N, в которой существует отображение F множества a на b. Чтобы избежать очевидных трудностей, допустим, что a бесконечно и $b \neq 0$.

Пусть C — множество всех отображений всевозможных конечных подмножеств множества a в b. Тогда $C \in M$ в силу абсолютности. Множество G всех конечных подмножеств множества F будет подмножеством множества C, но оно не обязательно будет в M. Наша идея состоит в том, чтобы, во-первых, подобрать G, а затем, используя G, построить N.

Каждое $p \in C$ дает некоторое условие, которому должно удовлетворять F, чтобы p было в G, а именно, мы должны иметь $p \subset F$. Если $p \subset q$, то условие q дает больше информации, чем условие p. Тогда мы говорим, что q есть расширение p, и пишем $q \leqslant p$. (Такое обозначение должно намекать на то, что q допускает меньше моделей N, чем p.) Тогда C является частично упорядоченным множеством с наибольшим элементом 0.

Имеются три очевидных условия, которым должно удовлетворять G: (а) $0 \in G$; (б) если $p \in G$ и $p \leqslant q$, то $q \in G$; (в) любые два элемента из G имеют общее расширение в G. Если G удовлетворяет этим условиям, то $F = U(G)$ будет отображением некоторого подмножества множества a на некоторое подмножество множества b.

Для того чтобы получить $\mathrm{Do}(F) = a$ и $\mathrm{Ra}(F) = b$, множество G должно, кроме того, пересекаться с некоторыми множествами, а именно, с каждым множеством $[p \mid x \in \mathrm{Do}(p)]$ для $x \in a$ и с каждым множеством $[p \mid y \in \mathrm{Ra}(p)]$ для $y \in b$. Эти множества являются множествами в M и имеют следующее свойство: каждое условие из C имеет расширение в каждом таком множестве. Поэтому мы будем требовать, чтобы G пересекалось с каждым множеством в M, имеющим это свойство.

Теперь обобщим эти понятия. *Понятие вынуждения* есть частично упорядоченное множество C, имеющее наибольший элемент. Мы обозначим этот порядок через $\leqslant_C$ или $\leqslant$, а наибольший элемент через 1_C или 1. Элементы множества C называются *условиями*. Обычно условия будут обозначаться через p, q и r. Если $p \leqslant q$, то мы скажем, что p есть *расширение* q. Подмножество D множества C назовем *C-плотным* (или просто *плотным*), если каждое условие из C имеет расширение в D.

Пусть C — некоторое понятие вынуждения, а M — некоторое множество. Подмножество G множества C называется *C-генерическим* над M (или просто *генерическим*), если справедливы следующие утверждения:

(G1) $1 \in G$;

(G2) для каждых $p \in G$ и $q \geqslant p$ имеем $q \in G$;

(G3) для каждых p, $q \in G$ условия p и q имеют общее расширение в G;

(G4) для каждого плотного множества D в M имеем $G \cap D \neq 0$.

Теорема существования. *Пусть C — некоторое понятие вынуждения, M — счетное множество, $p \in C$. Тогда существует C-генерическое над M множество G, содержащее p.*

Доказательство. Пусть a_0, a_1, ... — элементы M. Выбираем p_n индуктивно следующим образом: $p_0 = p$, p_{n+1} — некоторое расширение условия p_n из a_n, если такое расширение существует, и $p_{n+1} = p_n$ в противном случае. Тогда множество $G = [q \mid \exists n\, (p_n \leqslant q)]$ имеет требуемые свойства.

Замечание. Это единственное место, где мы прямо используем счетность M. Очевидно, достаточно было бы предположить, что $M \cap S(C)$ счетно.

Пусть $H_{\mathfrak{m}}(A; B)$ — множество всех отображений p всевозможных элементов множества $S_{\mathfrak{m}}(A)$ в B. Если $p, q \in H_{\mathfrak{m}}(A; B)$, то мы пишем $p \leqslant q$ вместо $q \subset p$. Тогда $H_{\mathfrak{m}}(A; B)$ есть понятие вынуждения с наибольшим элементом 0. Мы пишем $H(A; B)$ вместо $H_{\aleph_0}(A; B)$. Заметим, что $H(A; B)$ абсолютно.

Теперь предположим, что M — модель теории ZFC, $a, b \in M$, $b \neq 0$, $\mathfrak{m}$ — бесконечный кардинал в M такой, что $\mathfrak{m} \leqslant |a|$ в M, $C = H^M_{\mathfrak{m}}(a; b)$, G — C-генерическое над M множество и $F = U(G)$. Тогда замечания в начале параграфа показывают, что F — отображение из a на b. (Нам нужно $\mathfrak{m} \leqslant |a|$ в M для того, чтобы гарантировать, что для каждого $y \in b$ множество $[p \mid y \in \mathrm{Ra}(p)]$ плотно.) Таким образом, если мы можем построить расширение N модели M, содержащее G, то мы получим расширение, в котором существует отображение из a на b.

Замечание. Это показывает, что если a счетно и бесконечно и b несчетно, то не существует C-генерического множества над M. Поэтому требование счетности в теореме существования не может быть опущено.

Историческая справка. Основные идеи этого параграфа принадлежат Коэну [1], [2]. Понятие плотного множества принадлежит Соловею.

4. Построение модели

Теперь предположим, что C — понятие вынуждения *) в некоторой счетной модели M теории ZFC и G — C-генерическое множество над M. Мы собираемся построить расширение модели M, содержащее G.

Вначале определим структуру, универсумом которой является M, а отношение принадлежности $\in_G$ определяется следующим образом: $a \in_G b \leftrightarrow \exists p \in G\ (\langle a, p\rangle \in b)$ (здесь и в дальнейшем a, b, c и d обозначают элементы множества M). Теперь мы применим метод сжатия, чтобы переделать $\langle M, \in_G\rangle$ в транзитивную модель. Сначала заметим, что

$$a \in_G b \rightarrow a \in \mathrm{Ra}(b) \tag{4.1}$$

*) Понятие вынуждения C лежит в некоторой модели M, если множество C и отношение $\leqslant$ лежат в M.

и, следовательно,

$$a \in_G b \rightarrow \mathrm{rk}(a) < \mathrm{rk}(b). \tag{4.2}$$

Затем мы определяем

$$K_G(b) = [K_G(a) \mid a \in_G b].$$

По (4.2) это есть правильное определение индукцией по $\mathrm{rk}(b)$. Наконец, определим

$$M[G] = [K_G(a) \mid a \in M].$$

Главная теорема. *Пусть M — счетная модель теории ZFC, C — некоторое понятие вынуждения в M, G — некоторое C-генерическое над M множество. Тогда $M[G]$ — счетная модель теории ZFC, расширяющая M и содержащая G, и это есть наименьшая такая модель.*

Доказательство этой фундаментальной теоремы будет дано здесь и в следующих двух параграфах. Мы предполагаем, что всюду дальше в этой статье M, C и G удовлетворяют условиям основной теоремы, за исключением специально оговоренных случаев. Мы будем писать $\bar{a}$ вместо $K_G(a)$.

Начнем с некоторых простых замечаний. Из определения $M[G]$ и счетности M видно, что $M[G]$ счетно и транзитивно. Теперь определим

$$\hat{b} = [\langle \hat{a}, 1\rangle \mid a \in b]$$

индукцией по $\mathrm{rk}(b)$. Это определение может быть дано в M, поэтому отображение, переводящее a в $\hat{a}$, есть функционал в M. В частности, $\hat{a} \in M$. Простая индукция (использующая (G1)) показывает, что $K_G(\hat{b}) = b$; таким образом, $M \subset M[G]$. Теперь положим (обозначая несколько неправильно)

$$\hat{G} = [\langle \hat{p}, p\rangle \mid p \in C].$$

Тогда $\hat{G} \in M$ и $K_G(\hat{G}) = G$. Следовательно, $G \in M[G]$. Итак, $M[G]$ — счетное транзитивное множество, расширяющее M и содержащее G. Проверка того, что это есть модель теории ZFC, требует одного нового понятия, к которому мы сейчас и переходим.

5. Вынуждение

Введем язык, называемый *языком вынуждения*, подходящий для исследования $M[G]$. Символами языка вынуждения являются символы теории ZFC и все элементы *) множества M. Каждый элемент a множества M считается константой, которая отмечает элемент $\bar{a}$ из $M[G]$; мы называем a *именем* элемента $\bar{a}$. Если Φ — предложение языка вынуждения, то $\vdash_G \Phi$ означает, что Φ истинно в $M[G]$.

Пусть $p \in C$ и Φ — предложение языка вынуждения. Скажем, что p *вынуждает* Φ, и записываем это $p \Vdash \Phi$, если $\vdash_G \Phi$ для каждого множества G, являющегося C-генерическим над M и содержащего p.

Наша первоочередная задача — доказать три леммы о вынуждении.

Лемма определимости. *Если $\Phi(x_1, \ldots, x_n)$ — формула теории ZFC, содержащая только указанные свободные переменные, то*

$$[\langle p, a_1, \ldots, a_n\rangle \mid p \Vdash \Phi(a_1, \ldots, a_n)]$$

является классом в M.

Лемма о расширении. *Если $p \Vdash \Phi$ и $q \leqslant p$, то $q \Vdash \Phi$.*

Лемма об истинности. *Если G генерическое, то $\vdash_G \Phi$ тогда и только тогда, когда $\exists p \in G\ (p \Vdash \Phi)$.*

Наш метод состоит в следующем. Мы определим видоизмененное понятие вынуждения, обозначаемое через $p \Vdash^* \Phi$. Затем докажем, что эти три леммы выполняются при замене $\Vdash$ на $\Vdash^*$. Далее мы покажем, что

$$p \Vdash \Phi \leftrightarrow p \Vdash^* \neg\neg\Phi. \qquad (5.1)$$

Затем, беря эти три леммы для $\Vdash^*$ и заменяя Φ на $\neg\neg\Phi$, получим леммы для $\Vdash$.

Вначале укажем неопределяемые символы языка вынуждения. Считаем, что $\neg$ и $\vee$ — неопределяемые пропозициональные связки и $\exists$ — неопределяемый квантор. В качестве неопределяемых символов отношений мы берем $\in$ и $\neq$.

*) Те, кому не нравится использование множеств в качестве символов, могут ввести некоторое новое множество символов, которое находится во взаимно однозначном соответствии с M.

Конечно, $x \notin y$ определяется как $\neg(x \in y)$, $x = y$ определяется как $\neg(x \neq y)$.

Теперь определяем $p \Vdash^* \Phi$ с помощью следующих пяти пунктов.

(а) $p \Vdash^* a \in b$, если $\exists c \exists q \geqslant p\ (\langle c, q\rangle \in b\ \&\ p \Vdash^* a = c)$.

(б) $p \Vdash^* a \neq b$, если $\exists c \exists q \geqslant p\ (\langle c, q\rangle \in a\ \&\ p \Vdash^* c \notin b)$ или $\exists c \exists q \geqslant p\ (\langle c, q\rangle \in b\ \&\ p \Vdash^* c \notin a)$.

(в) $p \Vdash^* \neg\Phi$, если $\forall q \leqslant p\ \neg(q \Vdash^* \Phi)$.

(г) $p \Vdash^* \Phi \vee \Psi$, если $p \Vdash^* \Phi$ или $p \Vdash^* \Psi$.

(д) $p \Vdash^* \exists x \Phi(x)$, если $\exists b\ (p \Vdash^* \Phi(b))$.

Сначала мы должны убедиться, что в этом определении нет порочных кругов. Если мы проанализируем определение $p \Vdash^* a \neq b$, то найдем, что оно определяется в терминах $p' \Vdash^* a' \neq b'$ и $p' \Vdash^* b' \neq a'$, где $\mathrm{rk}(a') < \mathrm{rk}(a)$ и $\mathrm{rk}(b') < \mathrm{rk}(b)$. Тем самым мы можем определить $p \Vdash^* a \neq b$ индукцией по $\max(\mathrm{rk}(a), \mathrm{rk}(b))$. Затем мы применяем (в) для определения $p \Vdash^* a = b$, (а) для определения $p \Vdash^* a \in b$ и (в) для определения $p \Vdash^* a \notin b$. Тогда мы можем получить (б). Это определяет $p \Vdash^* \Phi$ для атомных формул Φ. Затем применяем (в), (г) и (д) для определения $p \Vdash^* \Phi$ для всех Φ индукций по длине Φ.

Лемма определимости для $\Vdash^*$ тривиально доказывается индукцией по длине $\Phi(x_1, \ldots, x_n)$ (замечая, что область действия кванторов в (а) — (д) есть M или множество C в M). Конечно, определение класса $[\langle p, a, b\rangle \mid p \Vdash^* a \neq b]$ должно быть проведено трансфинитной индукцией в M так, как описано выше.

Мы докажем другие две леммы, доказывая их для предложений в левых частях (а) — (д) при предположении, что эти леммы являются истинными для предложений в правых частях; как мы видели выше, это правильный метод доказательства. Лемма о расширении совсем тривиальна, поэтому мы рассмотрим лишь лемму об истинности.

Вначале покажем, что если лемма об истинности выполняется для Φ, то

$$a \in_G b\ \&\ \vdash_G \Phi \leftrightarrow$$
$$\leftrightarrow \exists p \in G \exists q \geqslant p\ (\langle a, q\rangle \in b\ \&\ p \Vdash^* \Phi). \qquad (5.2)$$

Если левая часть выполняется, то существуют $q, r \in G$ такие, что $\langle a, q\rangle \in b$ и $r \Vdash^* \Phi$. Выбирая общее расширение p для q и r в G по (G3), получаем $p \Vdash^* \Phi$ ввиду леммы о расширении. Обратно, пусть правая часть (5.2) выполняется для p и q. Тогда $\vdash_G \Phi$ ввиду леммы об истинности. Также $q \in G$ ввиду (G2), следовательно, $a \in_G b$.

Теперь обратимся к пяти случаям леммы об истинности.

(а) $\vdash_G a \in b$ эквивалентно $\exists c (c \in_G b \mathbin{\&} \vdash_G a = c)$ по определению $\bar{b}$. По предложению и (5.2) это эквивалентно

$$\exists c \exists p \in G \exists q \geqslant p \ (\langle c, q \rangle \in b \mathbin{\&} p \Vdash^* a = c)$$

и, следовательно, эквивалентно $\exists p \in G \ (p \Vdash^* a \in b)$.

(б) Ясно, что $\vdash_G a \neq b$ тогда и только тогда, когда или $\exists c (c \in_G a \mathbin{\&} \vdash_G c \notin b)$, или $\exists c (c \in_G b \mathbin{\&} \vdash_G c \notin a)$. По предположению и (5.2) это эквивалентно

$$\exists c \exists p \in G \exists q \geqslant p \ (\langle c, q \rangle \in a \mathbin{\&} p \Vdash^* c \notin b) \vee$$
$$\vee \exists c \exists p \in G \exists q \geqslant p \ (\langle c, q \rangle \in b \mathbin{\&} p \Vdash^* c \notin a)$$

и, следовательно, эквивалентно $\exists p \in G (p \Vdash^* a \neq b)$.

(в) По предположению $\vdash_G \neg \Phi$ тогда и только тогда, когда $\neg \exists p \in G (p \Vdash^* \Phi)$. Поэтому мы должны доказать, что выполняется в точности одно из двух: $\exists p \in G (p \Vdash^* \Phi)$ или $\exists p \in G (p \Vdash^* \neg \Phi)$. Чтобы доказать, что по крайней мере одна из формул выполняется, по (G4) достаточно показать, что $D = [p \mid p \Vdash^* \Phi$ или $p \Vdash^* \neg \Phi]$ является плотным множеством в M. По лемме определимости множество D является множеством в M, поэтому мы должны лишь показать, что каждое p имеет расширение в D. Но либо p имеет расширение q такое, что $q \Vdash^* \Phi$ и, следовательно, $q \in D$, либо $p \Vdash^* \neg \Phi$ и, следовательно, p само находится в D.

Теперь предположим, что существуют $p, q \in G$ такие, что $p \Vdash^* \Phi$ и $q \Vdash^* \neg \Phi$. По (G2) p и q имеют общее расширение r, а по лемме о расширении $r \Vdash^* \Phi$. Это противоречит тому, что $q \Vdash^* \neg \Phi$.

Легкие доказательства (г) и (д) оставляем читателю.

Теперь докажем (5.1). Предположим, что $p \Vdash^* \neg\neg \Phi$. Если множество G генерическое и $p \in G$, то по лемме об истинности $\vdash_G \neg\neg \Phi$, поэтому $\vdash_G \Phi$. Таким образом, $p \Vdash \Phi$. Теперь предположим, что $\neg (p \Vdash^* \neg\neg \Phi)$. Тогда $q \Vdash^* \neg \Phi$ для некоторого $q \leqslant p$. Выберем такое генерическое множество G, что $q \in G$. Ввиду леммы об истинности $\vdash_G \neg \Phi$, а по (G2) $p \in G$. Следовательно, $\neg (p \Vdash \Phi)$.

Таким образом, мы показали все наши леммы. Подставляя $\neg\neg \Phi$ вместо Φ в (в), получаем

$$p \Vdash \neg \Phi \text{ тогда и только тогда, когда } \forall q \leqslant p \neg (q \Vdash \Phi). \tag{5.3}$$

Заменяя Φ на $\neg \Phi$ и замечая, что $p \Vdash \neg\neg \Phi$ эквивалентно $p \Vdash \Phi$, получаем

$$p \Vdash \Phi \text{ тогда и только тогда, когда } \forall q \leqslant p \neg (q \Vdash \neg \Phi). \tag{5.4}$$

Историческая справка. По существу понятие вынуждения Коэна есть наше $\Vdash^*$. Часть (в) определения, которая упрощает определение Коэна, введена Скоттом. Наше понятие вынуждения введено Феферманом [4], который назвал его *слабым вынуждением*. Все три фундаментальные леммы доказаны Коэном.

6. Завершение доказательства

Покажем, что $M[G]$ — модель теории ZF, доказав, что $M[G]$ удовлетворяет всем условиям леммы 2.1. Так как $\omega \in M \subset M[G]$, то условие (а) выполняется.

Лемма 6.1. *Пусть A — класс в $M[G]$ такой, что $A \subset \bar{a}$. Тогда $A \in M[G]$ и A имеет имя c такое, что $c \subset \mathrm{Ra}(a) \times C$.*

Доказательство. Существует формула $\Phi(x)$ языка вынуждения такая, что

$$\bar{b} \in A \leftrightarrow \vdash_G \Phi(b) \tag{6.1}$$

для всех b. Положим

$$c = [\langle b, p \rangle \mid b \in \mathrm{Ra}(a) \mathbin{\&} p \Vdash \Phi(b)].$$

Ввиду леммы определимости c есть класс в M. А так как $c \subset \mathrm{Ra}(a) \times C$, то $c \in M$.

Мы должны показать, что

$$\bar{b} \in \bar{c} \leftrightarrow \bar{b} \in A.$$

Если $\bar{b} \in \bar{c}$, то мы можем предположить, изменив b, но не изменяя $\bar{b}$, что $b \in_G c$. Тогда для некоторого $p \in G$ имеем $\langle b, p \rangle \in c$ и, следовательно, $p \Vdash \Phi(b)$. Таким образом, $\vdash_G \Phi(b)$, поэтому $\bar{b} \in A$ в силу (6.1). Пусть теперь $\bar{b} \in A$. Тогда $\bar{b} \in \bar{a}$, поэтому мы можем предположить, что $b \in_G a$. Ввиду (4.1) $b \in \mathrm{Ra}(a)$. Ввиду

(6.1) $\vdash_G \Phi(b)$, поэтому по лемме об истинности некоторое $p \in G$ вынуждает $\Phi(b)$. Тогда $\langle b, p\rangle \in c$, поэтому $b \in_G c$, таким образом, $\bar{b} \in \bar{c}$.

Из леммы 6.1 следует, что утверждение (б) леммы 2.1 выполняется.

Лемма 6.2. *Если $x \subset M[G]$ и каждый элемент из x имеет имя в a, то x включается в некоторое множество в $M[G]$.*

Доказательство. Пусть $b = a \times \{1\}$. Любой элемент из x есть $\bar{c}$ для некоторого $c \in a$. Но $c \in_G b$ в силу (G1), следовательно, $\bar{c} \in \bar{b}$. Таким образом, $x \subset \bar{b}$.

Теперь докажем, что утверждение (в) леммы 2.1 выполняется. Пусть F — функционал в $M[G]$ и $\bar{a}$ — множество в $M[G]$, входящее в область определения для F. Существует формула $\Phi(x, y)$ языка вынуждения такая, что для всех b, c имеем

$$F(\bar{b}) = \bar{c} \leftrightarrow \vdash_G \Phi(b, c).$$

Выберем множество d в M со следующим свойством: для каждого $p \in C$ и каждого $b \in \mathrm{Ra}(a)$, если существует c такое, что $p \Vdash \Phi(b, c)$, то существует такое же множество в d. Заменяя d его транзитивным замыканием, мы можем предполагать, что d транзитивно.

Теперь покажем, что каждый элемент x из $U([F(\bar{b}) \mid \bar{b} \in \bar{a}])$ имеет имя в d; ввиду леммы 6.2 на этом наше доказательство будет закончено. Имеем $x \in F(\bar{b})$, где $\bar{b} \in \bar{a}$. Мы можем предположить, что $b \in_G a$. Пусть c будет именем $F(\bar{b})$. Имеем $\vdash_G \Phi(b, c)$, поэтому некоторое $p \in G$ вынуждает $\Phi(b, c)$. Следовательно, для некоторого $c' \in d$ имеем $p \Vdash \Phi(b, c')$. Тогда $\vdash_G \Phi(b, c')$, поэтому $F(\bar{b}) = \bar{c}'$. Следовательно, $x \in \bar{c}'$, откуда $x = \bar{a}'$ для $a' \in_G c'$, а поэтому $a' \in \mathrm{Ra}(c')$. Так как $c' \in d$ и d транзитивно, то $a' \in d$, что и требовалось.

Наконец, докажем, что утверждение (г) леммы 2.1 выполняется. Пусть $\bar{a} \in M[G]$, и пусть $\bar{b} \in S(\bar{a}) \cap M[G]$. Ввиду леммы 6.1 $\bar{b}$ имеет имя c такое, что $c \subset \mathrm{Ra}(a) \times C$ и, значит, $c \in S^M(\mathrm{Ra}(a) \times C)$. Требуемый результат теперь следует из леммы 6.2. Тем самым $M[G]$ является моделью теории ZF.

Лемма 6.3. *Если N — модель теории ZF, расширяющая M и содержащая G, то существует функционал в N, ограничением которого на M является K_G.*

Доказательство. Определим (в N)

$$x \in^* y \leftrightarrow \exists p \in G(\langle x, p\rangle \in y),$$
$$K^*(y) = [K^*(x) \mid x \in^* y]$$

(индукцией по $\mathrm{rk}(y)$). Легко видеть (используя транзитивность M), что $\in^*$ и K^* совпадают соответственно с $\in_G$ и K_G для аргументов из M.

Из леммы следует, что $K_G(a) \in N$ для всех $a \in M$, так что $M[G] \subset N$. Поэтому $M[G]$ является даже наименьшей моделью теории ZF, расширяющей M и содержащей G. Далее, можно применить лемму 6.3 к $M[G]$. Мы получим функцию K в $M[G]$, ограничение которой на M есть K_G.

Пусть теперь $\bar{a} \in M[G]$. Тогда в M и, значит, в $M[G]$ существует отображение некоторого ординала на $\mathrm{Ra}(a)$. Комбинируя K с этим отображением, получим в $M[G]$ отображение некоторого ординала на

$$[K(x) \mid x \in \mathrm{Ra}(a)] = [\bar{b} \mid b \in \mathrm{Ra}(a)].$$

Но ввиду (4.1) это множество включает $\bar{a}$. Поэтому в $M[G]$ выполняется следующее: для каждого x существует отображение некоторого ординала на некоторое множество, содержащее x. Из этого следует, что аксиома выбора выполняется в $M[G]$. Итак, мы завершили доказательство главной теоремы.

Историческая справка. Большинство идей этого параграфа принадлежит Коэну. Доказательство того, что аксиома степени выполняется в $M[G]$, по существу принадлежит Соловею; оно проще, чем доказательство Коэна.

7. Аксиома конструктивности

Для наилучшего применения фундаментальной теоремы нам нужна информация про отношение между M и $M[G]$. Следующий простой результат часто бывает полезен.

Лемма 7.1. *M и $M[G]$ имеют одинаковые ординалы.*

Доказательство. Так как $M \subset M[G]$, то нам нужно лишь показать, что каждый ординал α из $M[G]$ есть в M. Простая индукция показывает, что $\mathrm{rk}(\bar{a}) \leqslant \mathrm{rk}(a)$ для всех a. Пусть a будет именем α, тогда $\alpha = \mathrm{rk}(\alpha) \leqslant \mathrm{rk}(a)$. Так как rk абсолютно, то $\mathrm{rk}(a) \in M$, поэтому $\alpha \in M$ в силу транзитивности M.

Следствие. *M и $M[G]$ имеют одинаковые конструктивные множества.*

Пусть теперь M — счетная модель теории ZFC, и пусть $C=H(\omega;\ 2)$. В силу абсолютности, C лежит в M. Возьмем G генерическим над M и положим $F=U(G)$. Как мы видели в § 3, F — отображение из ω на 2. Очевидно, $F\in M[G]$; мы утверждаем, что $F\notin M$. Чтобы показать это, допустим, что f — произвольное отображение из ω на 2, лежащее в M. Тогда $[p\,|\,\exists n\in\omega\ (n\in \mathrm{Do}(p)\ \&\ p(n)\neq f(n))]$ — множество в M, которое является, как легко видеть, плотным. Поэтому оно содержит некоторое $p\in G$, а отсюда следует, что $F\neq f$.

Поэтому множество A, характеристическая функция которого есть F, лежит в $M[G]-M$. По следствию A не является конструктивным в $M[G]$. Поэтому $M[G]$ — это модель теории ZFC′, где теория ZFC′ — теория ZFC с дополнительной аксиомой: существует неконструктивное подмножество множества ω.

Мы показали, как построить модель теории ZFC′ из счетной модели M теории ZFC. Существование M может быть показано следующим образом. Мы начинаем с любой модели N теории ZFC. Применяя теорему Левенгейма — Скулема для того, чтобы получить счетную подмодель, и применяя технику сжатия, мы получим счетную модель M теории ZFC.

К несчастью, существование (транзитивной) модели N теории ZFC не может быть доказано в теории ZFC даже в предположении, что теория ZFC непротиворечива. Поэтому, если мы хотим иметь финитное доказательство относительной непротиворечивости теории ZFC′ по отношению к теории ZFC, то мы должны сделать небольшие изменения. Добавим к теории ZFC константу N и аксиомы, которые утверждают, что N транзитивно и непусто и каждая аксиома теории ZFC выполняется в N. Принцип отражения (см. [6]) показывает, что это будет консервативным расширением теории ZFC. Затем определим M и $M[G]$, как раньше. Наше доказательство будет тогда показывать, что каждая аксиома теории ZFC′ выполняется в $M[G]$. Немного другой метод изложен в данной книге.

Мы можем получить более сильный результат с помощью «сжатия» кардинала в M. Допустим, что M удовлетворяет аксиоме конструктивности. (Мы можем получить такую модель из любой счетной модели N теории ZFC, взяв множества, конструктивные в N.) Возьмем $C=H(\aleph_0;\ \aleph_1^M)$. Тогда в $M[G]$ существует отображение из $\aleph_0$ на $\aleph_1^M$; таким образом, $\aleph_1^M$ счетно в $M[G]$. Существует одно-однозначное соответствие между $S^M(\omega)$ и $\aleph_1^M$, которое лежит в M, и, следовательно, в $M[G]$, поэтому $S^M(\omega)$ счетно в $M[G]$. Но в силу следствия каждое подмножество множества ω, которое конструктивно в $M[G]$, есть в M и, следовательно, в $S^M(\omega)$. Таким образом, в $M[G]$ существует только счетное число конструктивных подмножеств множества ω.

Историческая справка. Независимость аксиомы конструктивности была доказана Коэном. Кардинальное сжатие введено Леви.

8. Произведения

Пусть C_1 и C_2 — некоторые понятия вынуждения в M. Мы будем снабжать индексами 1 или 2 все ранее введенные понятия, чтобы отличать, что относится к C_1, а что к C_2; например, p_1 — некоторый элемент из C_1, G_2 — некоторое C_2-генерическое множество. Будем писать $M[G_1,\ G_2]$ вместо $(M[G_1])[G_2]$.

Определим частичный порядок на $C_1\times C_2$ следующим образом:

$$\langle p_1,\ p_2\rangle\leqslant\langle q_1,\ q_2\rangle\leftrightarrow p_1\leqslant q_1\ \&\ p_2\leqslant q_2.$$

Ясно, что $C_1\times C_2$ является понятием вынуждения в M с наибольшим элементом $\langle 1_1,\ 1_2\rangle$.

Теорема о произведении. *Пусть C_1 и C_2 — произвольные понятия вынуждения в M. Если G_1 является C_1-генерическим над M, а G_2 — C_2-генерическим над $M[G_1]$, то $G_1\times G_2$ является $(C_1\times C_2)$-генерическим над M, и $M[G_1\times G_2]=M[G_1,\ G_2]$. Каждое множество, являющееся $(C_1\times C_2)$-генерическим над M, получается таким путем.*

Доказательство. Легко проверить (G1), (G2) и (G3) для $G_1\times G_2$. Пусть D — произвольное $(C_1\times C_2)$-плотное множество в M. Мы должны показать, что $(G_1\times G_2)\cap D\neq 0$, т. е. что $G_2\cap D_2\neq 0$, где

$$D_2=[p_2\,|\,\exists p_1\in G_1\,(\langle p_1,\ p_2\rangle\in D)].$$

Так как $D_2\in M[G_1]$, то достаточно показать, что D_2 является C_2-плотным.

Пусть $q_2 \in C_2$; мы должны найти $p_2 \leqslant q_2$ и $p_1 \in G$ такие, что $\langle p_1, p_2 \rangle \in D$. Другими словами, мы должны показать, что $G_1 \cap D_1 \neq 0$, где

$$D_1 = [p_1 \mid \exists p_2 \leqslant q_2 (\langle p_1, p_2 \rangle \in D)].$$

Так как $D_1 \in M$, то достаточно показать, что D_1 является C_1-плотным. Пусть $q_1 \in C_1$, и выберем $\langle p_1, p_2 \rangle \leqslant \langle q_1, q_2 \rangle$ так, чтобы $\langle p_1, p_2 \rangle \in D$. Тогда $p_1 \leqslant q_1$ и $p_1 \in D_1$.

Равенство $M[G_1 \times G_2] = M[G_1, G_2]$ выполняется, потому что оба множества являются наименьшими моделями теории ZFC, расширяющими M и содержащими G_1 и G_2.

Пусть теперь G будет $(C_1 \times C_2)$-генерическим над M, а G_1 и G_2 — проекции G на C_1 и C_2 соответственно. Ясно, что $G \subset G_1 \times G_2$. Чтобы доказать, что $G = G_1 \times G_2$, допустим, что $\langle p_1, p_2 \rangle \in G_1 \times G_2$. Для некоторых q_1 и q_2 имеем $\langle p_1, q_2 \rangle$, $\langle q_1, p_2 \rangle \in G$. Поэтому они имеют общее расширение $\langle r_1, r_2 \rangle$ в G. А так как $\langle r_1, r_2 \rangle \leqslant \langle p_1, p_2 \rangle$, то получаем $\langle p_1, p_2 \rangle \in G$.

Проверка (G1), (G2) и (G3) для G_1 и G_2 совсем легкая. Чтобы проверить (G4) для G_1, допустим, что D_1 является C_1-плотным множеством в M. Тогда $D_1 \times C_2$ является $(C_1 \times C_2)$-плотным множеством в M. Поэтому $G \cap (D_1 \times C_2) \neq 0$; таким образом, $G_1 \cap D_1 \neq 0$.

Чтобы проверить (G4) для G_2, допустим, что D_2 — C_2-плотное множество в $M[G_1]$. Пусть a — имя D_2, и пусть Φ — предложение языка вынуждения, утверждающее, что $\bar{a}$ является C_2-плотным.

Покажем, что

$$D = [\langle p_1, p_2 \rangle \mid p_1 \Vdash \Phi \to \hat{p}_2 \in a]$$

плотно. Пусть дано $\langle q_1, q_2 \rangle$. Выберем G_1' C_1-генерическое над M так, чтобы $q_1 \in G_1'$. Если $K_{G_1'}(a)$ является C_2-плотным, то выберем $p_2 \leqslant q_2$ так, чтобы $p_2 \in K_{G_1'}(a)$, в противном случае положим $p_2 = q_2$. В любом случае имеем $\vdash_{G_1'} \Phi \to \hat{p}_2 \in a$. Поэтому некоторое $p_1 \in G_1'$ вынуждает $\Phi \to \hat{p}_2 \in a$, а по (G3) и лемме о расширении мы можем предположить, что $p_1 \leqslant q_1$. Тогда $\langle p_1, p_2 \rangle \leqslant \langle q_1, q_2 \rangle$ и $\langle p_1, p_2 \rangle \in D$.

Так как $D \in M$, то отсюда следует, что $G \cap D \neq 0$. Пусть $\langle p_1, p_2 \rangle \in G \cap D$. Поскольку $p_1 \in G_1$ и $p_1 \Vdash \Phi \to \hat{p}_2 \in a$, то мы имеем $\vdash_{G_1} \Phi \to \hat{p}_2 \in a$. Но $\vdash_{G_1} \Phi$, поэтому $p_2 \in \bar{a} = D_2$. Но $p_2 \in G_2$, следовательно, $G_2 \cap D_2 \neq 0$.

Следствие. *Пусть C_1 и C_2 — произвольные понятия вынуждения в M. Пусть G_1 — C_1-генерическое множество над M, а G_2 — C_2-генерическое множество над $M[G_1]$. Тогда G_1 является C_1-генерическим над $M[G_2]$ и $M[G_2, G_1] = M[G_1, G_2]$.*

Доказательство. По предыдущей теореме $G_1 \times G_2$ является $(C_1 \times C_2)$-генерическим над M. Применяя очевидный изоморфизм между $C_1 \times C_2$ и $C_2 \times C_1$, получаем, что $G_2 \times G_1$ является $(C_2 \times C_1)$-генерическим над M. Снова применяя теорему, получаем, что G_1 является C_1-генерическим над $M[G_2]$. Имеем

$$M[G_2, G_1] = M[G_1, G_2],$$

так как оба эти множества являются наименьшими моделями теории ZFC, расширяющими M и содержащими G_1 и G_2.

Рассмотрим только один пример бесконечных произведений, так называемую *слабую степень*. Если C — понятие вынуждения, а I — произвольное множество, то C^I — множество всех отображений p множества I в C таких, что множество $[i \mid i \in I \,\&\, p(i) \neq 1]$ конечно. Пусть $p \leqslant q$ означает $\forall i \in I\,(p(i) \leqslant q(i))$. Ясно, что C^I — понятие вынуждения, наибольший элемент которого — функция, тождественно равная 1_C. Если C и I принадлежат модели M теории ZFC, то и C^I принадлежит модели M; именно для этого мы ограничиваемся конечностью.

Если J и K — не пересекающиеся подмножества множества I такие, что $J \cup K = I$, то C^I изоморфно $C^J \times C^K$ естественным образом. В частности, если $i \in I$ и $J = I - \{i\}$, то C^I естественно изоморфно $C^J \times C$. В обоих случаях мы можем применять теорему о произведении.

9. Аксиома выбора

Под *автоморфизмом* понятия вынуждения C мы понимаем автоморфизм частично упорядоченного множества C.

Лемма 9.1. *Пусть π — некоторый автоморфизм понятия вынуждения C, который находится в M. Тогда $\pi(G)$ является C-генерическим над M и $M[G] = M[\pi(G)]$.*

Доказательство. Так как π отображает множества из M в множества из M, то первое утверждение тривиально.

Поскольку $M[G]$ содержит G и π, оно также содержит и $\pi[G]$, поэтому в силу фундаментальной теоремы $M[\pi(G)] \subset \subset M[G]$. Подставляя $\pi(G)$ вместо G и π^{-1} вместо π, получаем $M[G] \subset M[\pi(G)]$. Таким образом, $M[G] = M[\pi(G)]$.

Пусть $\mathfrak{A}$ — некоторое множество автоморфизмов C такое, что $\mathfrak{A} \in M$. Элемент a множества M называется *$\mathfrak{A}$-инвариантным*, если $K_G(a) = K_{\pi(G)}(a)$, для каждого $\pi \in \mathfrak{A}$. Например, каждое $\hat{a}$ инвариантно, так как $K_G(\hat{a}) = K_{\pi(G)}(\hat{a}) = a$. Предложение Φ языка вынуждения называется *$\mathfrak{A}$-инвариантным*, если каждая константа в Φ является $\mathfrak{A}$-инвариантной.

Пусть $\mathfrak{A}$ — некоторое множество автоморфизмов C. Скажем, что C является *$\mathfrak{A}$-однородным*, если для каждых p, $q \in C$ существует $\pi \in \mathfrak{A}$ такое, что $\pi^{-1}(p)$ и q имеют общее расширение. Если $\mathfrak{A}$ — множество всех автоморфизмов C, то мы говорим об *однородности* вместо $\mathfrak{A}$-однородности.

Если A — бесконечное множество, то $H(A; B)$ однородно. Для данных p, $q \in H(A; B)$ мы выбираем перестановку σ множества A такую, что $\sigma(\mathrm{Do}(p)) \cap \mathrm{Do}(q) = 0$, и определим автоморфизм π так: $\pi(r) = r \circ \sigma$. Тогда $\pi^{-1}(p) \cup q$ — общее расширение для $\pi^{-1}(p)$ и q.

Лемма 9.2. *Пусть $\mathfrak{A}$ — некоторое множество автоморфизмов C такое, что $\mathfrak{A} \in M$ и C является $\mathfrak{A}$-однородным. Пусть Φ — некоторое предложение языка вынуждения, являющееся $\mathfrak{A}$-инвариантным. Тогда $\vdash_G \Phi$ тогда и только тогда, когда $1 \Vdash \Phi$.*

Доказательство. Так как $1 \in G$, то из $1 \Vdash \Phi$ следует $\vdash_G \Phi$. Теперь предположим, что $\vdash_G \Phi$, но $\neg(1 \Vdash \Phi)$. В силу первого некоторое p вынуждает Φ, а в силу последнего и (5.4) некоторое q вынуждает $\neg\Phi$. Выберем $\pi \in \mathfrak{A}$ так, чтобы $\pi^{-1}(p)$ и q имели общее расширение. Ввиду теоремы существования и (G2) существует генерическое множество G', содержащее $\pi^{-1}(p)$ и q. По лемме 9.1 $\pi(G')$ генерическое. Так как $p \in \pi(G')$ и $q \in G'$, получаем $\vdash_{\pi(G')} \Phi$ и $\vdash_{G'} \neg\Phi$. Но $M[\pi(G')] = M[G']$ по лемме 9.1, а константы в Φ представляют одинаковые множества в этих двух моделях. Поэтому $\vdash_{\pi(G')} \Phi$ тогда и только тогда, когда $\vdash_{G'} \Phi$; получили противоречие.

Мы предполагаем, что читатель знаком с OD (ординально определимыми) и HOD (наследственно ординально определимыми множествами *)). Мы нуждаемся в небольшом обобщении этих понятий.

Скажем, что u OD *через* $v_1, \ldots, v_k$, если существует α такой, что $v_1, \ldots, v_k \in V(\alpha)$ и u определимо в $\langle V(\alpha), \in, v_1, \ldots, v_k\rangle$. Скажем, что u OD *над* w, если u OD через $v_1, \ldots, v_k$, w для некоторых $v_1, \ldots, v_k \in w$. Скажем, что u HOD *над* w, если u OD над w и каждый элемент из u HOD над w. Это определение индукцией по $\mathrm{rk}(u)$.

Основные результаты про OD и HOD множества переносятся на эту ситуацию. Так, например, каждый ординал OD через любые $v_1, \ldots, v_k$ и, следовательно, OD над любым w. Если $u_1, \ldots, u_m$ OD над $v_1, \ldots, v_k$ (или над w), то $\mu(u_1, \ldots, u_k)$ такое же (где μ — терм, определимый в теории ZFC). Класс всех множеств HOD над w является моделью теории ZF (но не обязательно аксиомы выбора). Также ясно, что каждый элемент из w OD над w.

Лемма 9.3. *Пусть $\mathfrak{A}$ — некоторое множество автоморфизмов C такое, что $\mathfrak{A} \in M$, и предположим, что C является $\mathfrak{A}$-однородным. Пусть u OD через $v_1, \ldots, v_k$ в $M[G]$ и $v_1, \ldots, v_k$ имеют $\mathfrak{A}$-инвариантные имена. Тогда $u \cap M \in M$.*

Доказательство. Существует формула $\Phi(x)$ языка вынуждения, содержащая только имена для $v_1, \ldots, v_k$ и некоторое $\alpha \in M[G]$ такое, что

$$\bar{a} \in u \leftrightarrow \vdash_G \Phi(a) \tag{9.1}$$

для всех a. Так как $\alpha \in M$ по лемме 7.1, то $\hat{\alpha}$ является $\mathfrak{A}$-инвариантным; поэтому мы можем предположить, что каждое имя в $\Phi(x)$ является $\mathfrak{A}$-инвариантным. Тогда, полагая $\hat{a}$ вместо a в (9.1) и применяя лемму 9.2, получим

$$a \in u \leftrightarrow \vdash_G \Phi(\hat{a}) \leftrightarrow 1 \Vdash \Phi(\hat{a}).$$

Таким образом, $u \cap M = [a \mid 1 \Vdash \Phi(\hat{a})]$ — класс в M. Но если $\beta = \mathrm{rk}(u)$, то $u \cap M \subset V(\beta) \cap M = V^M(\beta)$; следовательно, $u \cap M$ — множество в M.

Теорема 9.1. *Пусть C — однородно в M. Если u OD в $M[G]$, то $u \cap M \in M$; если u HOD в $M[G]$, то $u \in M$.*

*) J. Myhill, D. Scott, Ordinal definability, Proc. Symp. Pure Math. 13, № 1 (1971), 271—278.

Доказательство. Первое утверждение есть специальный случай леммы 9.3. Второе легко следует из первого индукцией по $\operatorname{rk}(u)$.

Пусть теперь M удовлетворяет аксиоме конструктивности, и пусть $C=H(\omega;\ 2)$. Применяя теорему 9.1, следствие леммы 7.1 и тот факт, что каждое конструктивное множество HOD, мы видим, что в $M[G]$ конструктивные множества совпадают с HOD множествами. Как мы видели в § 7, существует подмножество множества ω, не являющееся конструктивным в $M[G]$. Так как каждый элемент из ω HOD, то отсюда следует, что такое множество не OD в $M[G]$. Из этого следует, что в $M[G]$ не существует OD отображения какого-либо ординала на $S(\omega)$, ибо если бы F было OD, то таким же было бы каждое $F(\alpha)$.

Теперь предположим, что $C=H(\omega;\ 2)^\omega$. Пусть G_i — множество i-х координат элементов из G, и пусть $H=[G_i \mid i\in\omega]$. Пусть N — множество всех множеств, являющихся HOD над H в $M[G]$. Тогда N — модель теории ZF. Сейчас мы покажем, что N не является моделью аксиомы выбора; в действительности мы покажем, что в N не существует отображения какого-либо ординала на $S(\omega)$.

Предположим, что такое отображение F существует. Тогда F OD через $G_0,\ G_1,\ \ldots,\ G_{n-1},\ H$ для некоторого n (в $M[G]$). Каждый элемент из $S(\omega)\cap N$ есть $F(\alpha)$ для некоторого α в $M[G]$ и, следовательно, OD через G_0, $G_1,\ \ldots,\ G_{n-1},\ H$.

Рассмотрим C как произведение $C'\times C''$, где $C'=H(\omega;\ 2)^n$ и $C''=H(\omega;\ 2)^{\omega-n}$. Пусть G' и G'' — проекции G на C' и C'' соответственно. По теореме о произведении G' является C'-генерическим над M, G'' является C''-генерическим над $M'=M[G']$ и $M'[G'']=M[G]$. Снова применяя теорему о произведении, получаем, что G_n будет $H(\omega;\ 2)$-генерическим над M'. Поэтому множество A, имеющее $U(G_n)$ своей характеристической функцией, является подмножеством множества ω, не лежащим в M'. Так как $A\subset\omega\subset M'$, то $A\cap M'=A$; следовательно, $A\cap M'$ не лежит в M'.

Завершим доказательство, применив лемму 9.3, чтобы показать, что $A\cap M'\in M'$. Для каждой перестановки π множества $\omega-n$ определим автоморфизм π^* множества C'' следующим образом: $(\pi^*(p))_i=p_{\pi(i)}$. Пусть $\mathfrak{A}$ — множество всех π^* для π из M. Ясно, что $\mathfrak{A}\in M'$. Заметив, что каждая перестановка множества $\omega-n$, которая передвигает только конечное число элементов, содержится в M', мы видим, что C'' будет $\mathfrak{A}$-однородным. Теперь A OD через G_n и, следовательно, лежит в N. Таким образом, A OD через $G_0,\ G_1,\ \ldots,\ G_{n-1},\ H$ в $M[G]=M'[G'']$. Поэтому нам нужно лишь показать, что $G_0,\ G_1,\ \ldots,\ G_{n-1},\ H$ имеют $\mathfrak{A}$-инвариантные имена в M'.

Так как $G_0,\ G_1,\ \ldots,\ G_{n-1}$ лежат в M', то они имеют $\mathfrak{A}$-инвариантные имена $\hat{G}_0,\ \hat{G}_1,\ \ldots,\ \hat{G}_{n-1}$. Положим

$$a_i=\hat{G}_i, \qquad \text{если} \quad i<n,$$

$$a_i=[\langle\hat{p}_i,\ p\rangle \mid p\in C''], \quad \text{если} \quad i\geqslant n,$$

$$a=[a_i \mid i\in\omega]\times\{1\}.$$

Легко видеть, что a_i — имя G_i, а a — имя H. В $M'[\pi^*(G'')]$ a_i есть имя G_i, если $i<n$, и имя $\pi^*(G'')_i=G_{\pi^{-1}(i)}$, если $i\geqslant n$; таким образом, a — имя H. Это показывает, что a будет $\mathfrak{A}$-инвариантным.

Историческая справка. Независимость аксиомы выбора доказана Коэном. Модели теории ZFC, в которых нет OD отображений никакого ординала на $S(\omega)$, были впервые построены Феферманом [4]. Теорема 9.1 принадлежит Леви [7].

10. Сохранимость кардиналов

Теперь обратимся к исследованию отношения между кардиналами в M и кардиналами в $M[G]$.

Лемма 10.1. *Каждый кардинал в $M[G]$ является кардиналом в M.*

Доказательство. Пусть $\mathfrak{m}$ — некоторый кардинал в $M[G]$. По лемме 7.1 $\mathfrak{m}$ — ординал в M. Если $\mathfrak{m}$ не является кардиналом в M, то существует отображение некоторого ординала, меньшего $\mathfrak{m}$, на $\mathfrak{m}$, которое лежит в M и, следовательно, в $M[G]$. Но это невозможно.

Так как $0,\ 1,\ \ldots,\ \omega$ абсолютны, то они являются кардиналами как в M, так и в $M[G]$. С другой стороны, несчетные кардиналы в M не обязаны быть кардиналами в $M[G]$, как мы видели в предыдущем параграфе.

Если α — ординал в M, то, так как $M\subset M[G]$, имеем

$$\operatorname{cf}^{M[G]}(\alpha)\leqslant\operatorname{cf}^{M}(\alpha). \tag{10.1}$$

Равенство выполняется, когда $\mathrm{cf}^M(\alpha) \leqslant \omega$, так как свойства «быть предельным ординалом» абсолютно. И опять-таки предыдущий параграф показывает, что равенство может нарушаться, когда $\mathrm{cf}(\alpha)$ несчетно в M.

Теперь мы получим некоторые достаточные условия для того, чтобы достигалось равенство.

Пусть C — понятие вынуждения и $p, q \in C$. Будем говорить, что p и q *совместны*, если они имеют общее расширение; в противном случае называем p и q несовместными. Будем говорить, что C *удовлетворяет условию* $\mathfrak{m}$-*цепи*, если каждое множество попарно несовместных элементов в C имеет кардинал $< \mathfrak{m}$.

Лемма 10.2. *Пусть $\mathfrak{m}$ — регулярный кардинал в M такой, что C удовлетворяет условию $\mathfrak{m}$-цепи в M. Тогда*

(а) *если $\alpha \in M$ и $\mathfrak{m} \leqslant \mathrm{cf}^M(\alpha)$, то $\mathrm{cf}^M(\alpha) = \mathrm{cf}^{M[G]}(\alpha)$;*

(б) *каждый кардинал в M, который $\geqslant \mathfrak{m}$, есть кардинал в $M[G]$.*

Доказательство. Пусть $x(y) = z$ — формула теории множеств, которая утверждает, что x — функция, значение которой для аргумента y равно z. Будем говорить, что γ есть *возможное значение* a в β, если некоторое p вынуждает $a(\hat{\beta}) = \hat{\gamma}$. Мы утверждаем, что множество возможных значений a в β имеет кардинал $< \mathfrak{m}$. Для каждого такого возможного значения γ пусть p_γ вынуждает $a(\hat{\beta}) = \hat{\gamma}$. Ясно, что достаточно показать, что если $\gamma \neq \delta$, то p_γ и p_δ несовместны. Предположим, что они имеют общее расширение q. Выберем генерическое G' такое, что $q \in G'$. По лемме о расширении q вынуждает $a(\hat{\beta}) = \hat{\gamma}$ и $a(\hat{\beta}) = \hat{\delta}$; тогда по лемме об истинности $\vdash_{G'} a(\hat{\beta}) = \hat{\gamma}$ и $\vdash_{G'} a(\hat{\beta}) = \hat{\delta}$. Следовательно, $\gamma = \bar{a}(\beta) = \delta$.

Теперь пусть α таково, как утверждается в (а). Пусть $\mathfrak{n} = \mathrm{cf}^{M[G]}(\alpha)$. Тогда $\mathfrak{n}$ — некоторый кардинал в $M[G]$ и, следовательно, в M. Пусть $\bar{a}$ — отображение из $\mathfrak{n}$ на конфинальное подмножество множества α. Пусть b — множество возможных значений a среди ординалов $< \mathfrak{n}$. Ясно, что $b \in M$. Если $\sigma < \mathfrak{n}$ и $\bar{a}(\sigma) = \tau$, то некоторое $p \in G$ вынуждает $a(\hat{\sigma}) = \hat{\tau}$; таким образом, τ — возможное значение a в σ. Поэтому $\mathrm{Ra}(\bar{a}) \subset b$; таким образом, b конфинально в α. Следовательно, $\mathrm{cf}(\alpha) \leqslant |b|$ в M.

В силу вышеприведенного результата, b — объединение $\mathfrak{n}$ множеств в M, кардинал каждого из которых $< \mathfrak{m}$.

Если $\mathfrak{n} < \mathfrak{m}$, то $|b| < \mathfrak{m}$ в M (так как $\mathfrak{m}$ регулярен в M). Это невозможно, так как $\mathfrak{m} \leqslant \mathrm{cf}(\alpha) \leqslant |b|$ в M. Таким образом, $\mathfrak{m} \leqslant \mathfrak{n}$, поэтому $|b| \leqslant \mathfrak{m} \cdot \mathfrak{n} = \mathfrak{n}$ в M. Следовательно, $\mathrm{cf}(\alpha) \leqslant |b| \leqslant \mathfrak{n}$ в M, т. е. $\mathrm{cf}^M(\alpha) \leqslant \mathrm{cf}^{M[G]}(\alpha)$. Применяя (10.1), получаем равенство.

Пусть теперь $\mathfrak{n}$ — кардинал в M такой, что $\mathfrak{m} \leqslant \mathfrak{n}$. Покажем индукцией по $\mathfrak{n}$, что $\mathfrak{n}$ — кардинал в $M[G]$. Если $\mathfrak{n}$ — регулярный в M, то $\mathrm{cf}^M(\mathfrak{n}) = \mathfrak{n} \geqslant \mathfrak{m}$, тогда $\mathrm{cf}^{M[G]}(\mathfrak{n}) = \mathrm{cf}^M(\mathfrak{n}) = \mathfrak{n}$ по (а); следовательно, $\mathfrak{n}$ — кардинал в $M[G]$. Если $\mathfrak{n}$ сингулярный в M, то $\mathfrak{n}$ — точная верхняя грань множества кардиналов $\mathfrak{p}$ в M таких, что $\mathfrak{m} \leqslant \mathfrak{p} < \mathfrak{n}$. Так как все они являются кардиналами в $M[G]$, а точная верхняя грань множества кардиналов является кардиналом, то $\mathfrak{n}$ — кардинал в $M[G]$.

Следствие. *Если C удовлетворяет условию $\aleph_1$-цепи в M, то $\mathrm{cf}^M = \mathrm{cf}^{M[G]}$, а M и $M[G]$ имеют одинаковые кардиналы.*

Мы хотим применить эти результаты к $H_\mathfrak{m}(A; B)$. Сначала заметим, что для каждого $\mathfrak{p} < \mathfrak{m}$ (включая конечные $\mathfrak{p}$) существует самое большее $|A|^\mathfrak{p}$ подмножеств D множества A таких, что $|D| = \mathfrak{p}$, и для каждого такого D существует $|B|^\mathfrak{p}$ отображений из D в B. Поэтому

$$|H_\mathfrak{m}(A;\ B)| \leqslant \sum_{\mathfrak{p} < \mathfrak{m}} |A|^\mathfrak{p} |B|^\mathfrak{p};$$

таким образом,

$$|H_\mathfrak{m}(A;\ B)| \leqslant (|A| \cdot |B|)^{\mathfrak{m})}. \tag{10.2}$$

Лемма 10.3. *Если $\mathfrak{m}^{\mathfrak{m})} = \mathfrak{m}$ и $|B| \leqslant \mathfrak{m}$, то $H_\mathfrak{m}(A; B)$ удовлетворяет условию $\mathfrak{m}^+$-цепи.*

Доказательство. Пусть I — множество попарно несовместных элементов из $H_\mathfrak{m}(A; B)$. Индуктивно определим подмножество A_α множества A для каждого α. Пусть $A_0 = 0$; для предельного числа α положим $A_\alpha = \bigcup_{\beta < \alpha} A_\beta$. Пусть теперь A_α выбрано. Для каждого $p \in H_\mathfrak{m}(A_\alpha; B)$ выберем $q \in I$, ограничение которого до A_α есть p, при условии, что такое q существует. Пусть $A_{\alpha+1}$ будет объединением A_α и областей определения всех таких q.

Докажем индукцией, что $|A_\alpha| \leqslant \mathfrak{m}$ для $\alpha \leqslant \mathfrak{m}$. Случай тривиален, когда $\alpha = 0$ или α — предельный ординал.

Предположим, что $|A_\alpha| \leqslant \mathfrak{m}$. По (10.2)

$$|H_\mathfrak{m}(A_\alpha;\ B)| \leqslant (\mathfrak{m} \cdot |B|)^{\mathfrak{m})} = \mathfrak{m}^{\mathfrak{m})} = \mathfrak{m}. \qquad (10.3)$$

Теперь ясно, что

$$|A_{\alpha+1}| \leqslant |A_\alpha| + |H_\mathfrak{m}(A_\alpha;\ B)| \cdot \mathfrak{m} \leqslant \mathfrak{m} + \mathfrak{m} \cdot \mathfrak{m} = \mathfrak{m}.$$

В частности, $|A_\mathfrak{m}| \leqslant \mathfrak{m}$; таким образом, $|H_\mathfrak{m}(A_\mathfrak{m};\ B)| \leqslant \mathfrak{m}$ по (10.3).

Завершим доказательство, показав, что $I \subset H_\mathfrak{m}(A_\mathfrak{m};\ B)$. Пусть $p \in I$. Так как $|\mathrm{Do}(p)| < \mathfrak{m}$, то существует $\alpha < \mathfrak{m}$ такое, что $\mathrm{Do}(p) \cap A_\alpha = \mathrm{Do}(p) \cap A_{\alpha+1}$. Выберем $q \in I$ так, чтобы p и q имели одинаковое ограничение до A_α и $\mathrm{Do}(q) \subset A_{\alpha+1}$. Если $x \in \mathrm{Do}(p) \cap \mathrm{Do}(q)$, то $x \in A_{\alpha+1}$; тогда $x \in \mathrm{Do}(p) \cap A_{\alpha+1} \subset A_\alpha$, поэтому $p(x) = q(x)$. Отсюда следует, что p и q совместны. Так как $p,\ q \in I$, то $p = q$. Поэтому $\mathrm{Do}(p) \subset A_{\alpha+1} \subset A_\mathfrak{m}$ и, следовательно, $p \in H_\mathfrak{m}(A_\mathfrak{m};\ B)$.

Условия, при которых выполняется $\mathfrak{m}^{\mathfrak{m})} = \mathfrak{m}$, см. в § 2.

Подмножество D множества C называется *сечением*, если каждое расширение условия из D лежит в D.

Лемма 10.4. *Пусть D — сечение в M. Если $D \cap G' \neq 0$ для каждого G', являющимся C-генерическим над M, то D плотно.*

Доказательство. Для данного p выберем G' генерическим так, что $p \in G'$. Выберем $q \in D \cap G'$, и пусть r — общее расширение p и q. Тогда $r \leqslant p$ и $r \in D$.

Понятие вынуждения C называется *$\mathfrak{m}$-замкнутым*, если для каждого $\alpha < \mathfrak{m}$ и для каждой убывающей последовательности $\{p_\beta\}_{\beta<\alpha}$ условий в C существует $p \in C$ такое, что $p \leqslant p_\beta$ для всех $\beta < \alpha$. Например, если $\mathfrak{m}$ регулярно, то $H_\mathfrak{m}(A;\ B)$ будет $\mathfrak{m}$-замкнутым; действительно, мы можем взять $p = \bigcup_{\beta<\alpha} p_\beta$.

Лемма 10.5. *Если C является $\mathfrak{m}$-замкнутым в M, $\alpha < \mathfrak{m}$ и $\{D_\beta\}_{\beta<\alpha}$ — последовательность плотных сечений в M, то $\bigcap_{\beta<\alpha} D_\beta$ плотно.*

Доказательство. Для данного p мы можем определить индуктивно в M убывающую последовательность $\{p_\beta\}_{\beta<\alpha}$ такую, что $p_\beta \in D_\beta$ и $p_\beta \leqslant p$. (Мы должны использовать предположение о том, что C является $\mathfrak{m}$-замкнутым

в случае, когда β — предельный ординал.) Выбирая q так, чтобы $q \leqslant p_\beta$ для всех $\beta < \alpha$, получаем $q \leqslant p$ и $q \in \bigcap_{\beta<\alpha} D_\beta$.

Лемма 10.6. *Пусть C является $\mathfrak{m}$-замкнутым в M и $\alpha < \mathfrak{m}$. Тогда $({}^\alpha a)^M = ({}^\alpha a)^{M[G]}$ для каждого $a \in M$, а также $S^M(\alpha) = S^{M[G]}(\alpha)$.*

Доказательство. Ясно, что $({}^\alpha a)^M \subset ({}^\alpha a)^{M[G]}$. Пусть теперь $\bar{b} \in ({}^\alpha a)^{M[G]}$. Пусть $\Phi(x,\ y)$ будет

$$\exists z\,(z \in \hat{a}\ \&\ \langle z,\ y\rangle \in b) \rightarrow \langle x,\ y\rangle \in b,$$

и для каждого $\beta < \alpha$ положим

$$D_\beta = [p \mid \exists c\,(p \Vdash \Phi(\hat{c}, \hat{\beta}))].$$

Тогда D_β — сечение в M. Применим лемму 10.4, чтобы доказать, что оно плотно. Пусть G' генерическое. Тогда для некоторого $c \in a$ имеем $\vdash_{G'} \Phi(\hat{c},\ \hat{\beta})$; таким образом, по лемме об истинности $D_\beta \cap G' \neq 0$.

По лемме 10.5 множество $D = \bigcap_{\beta<\alpha} D_\beta$ плотно. Поэтому существует $q \in G \cap D$. Если $q \Vdash \Phi(\hat{c},\ \hat{\beta})$, то $c = \bar{b}(\beta)$. Следовательно, $\bar{b}(\beta)$ — единственное c такое, что $q \Vdash \Phi(\hat{c},\ \hat{\beta})$. Отсюда легко следует, что $\bar{b} \in M$.

Последнее утверждение доказывается, если взять $a = 2$ и использовать соответствие между множеством и его характеристической функцией.

Следствие. *Пусть C является $\mathfrak{m}$-замкнутым в M. Тогда*

(а) *если $\alpha \in M$ и $\mathrm{cf}^M(\alpha) \leqslant \mathfrak{m}$, то $\mathrm{cf}^M(\alpha) = \mathrm{cf}^{M[G]}(\alpha)$,*

(б) *каждый кардинал $\mathfrak{n}$ в M, который $\leqslant \mathfrak{m}$, есть кардинал в $M[G]$.*

Доказательство. (а) Если утверждение ложно, то $\mathrm{cf}^{M[G]}(\alpha) < \mathrm{cf}^M(\alpha) \leqslant \mathfrak{m}$. Пусть f — отображение из $\mathrm{cf}^{M[G]}(\alpha)$ на конфинальное подмножество α в $M[G]$. По лемме $f \in M$; таким образом, $\mathrm{cf}^{M[G]}(\alpha) \geqslant \mathrm{cf}^M(\alpha)$, и мы получили противоречие. (б) Если утверждение ложно, то существует отображение f ординала $< \mathfrak{n}$ на $\mathfrak{n}$ в $M[G]$. По лемме $f \in M$, а это невозможно.

Отметим, что во всех утверждениях этого параграфа, если мы доказали, что M и $M[G]$ имеют одинаковые кардиналы, то всегда оказывалось, что $\mathrm{cf}^M = \mathrm{cf}^{M[G]}$. В связи с этим возникает одна проблема: можно ли выбрать C так, чтобы M и $M[G]$ имели одинаковые кардиналы, но $\mathrm{cf}^M \neq \mathrm{cf}^{M[G]}$? Прикри показал, что это возможно, если существует измеримый кардинал в M.

Историческая справка. Результаты о $\mathfrak{m}$-замкнутых понятиях принадлежат Соловею, а остальные результаты принадлежат Коэну.

11. Гипотеза континуума

Вначале исследуем величину множества степени в $M[G]$.

Лемма 11.1. *Пусть C удовлетворяет условию $\mathfrak{m}$-цепи в M. Тогда для каждого бесконечного кардинала $\mathfrak{n}$ в M*

$$|S(\mathfrak{n})|^{M[G]} \leqslant ((|C|^{\mathfrak{m}})^{\mathfrak{n}})^M.$$

Доказательство. Для $a \in M$ и $\alpha < \mathfrak{n}$ пусть $\varphi_a(\alpha) = [p \mid p \Vdash \hat{\alpha} \in a]$. Тогда

$$\bar{a} \subset \mathfrak{n} \,\&\, \bar{b} \subset \mathfrak{n} \,\&\, \varphi_a = \varphi_b \to \bar{a} = \bar{b}.$$

Ввиду симметрии достаточно показать, что $\bar{a} \subset \bar{b}$. Пусть $\alpha \in \bar{a}$. Тогда некоторое $p \in G$ есть в $\varphi_a(\alpha)$ и, следовательно, в $\varphi_b(\alpha)$; таким образом, $\vdash_G \hat{\alpha} \in b$, а поэтому $\alpha \in \bar{b}$.

Отсюда следует, что

$$|S(\mathfrak{n})|^{M[G]} \leqslant |[\varphi_a \mid a \in M]|^M.$$

Далее, φ_a — отображение из $\mathfrak{n}$ в Q, где Q — множество всех множеств $[p \mid p \Vdash \Phi]$. Поэтому достаточно будет доказать, что $|Q| \leqslant |C|^{\mathfrak{m}}$ в M.

Пусть $a \in Q$. Применяя лемму Цорна, выберем максимальное подмножество b множества a, состоящее из попарно несовместных элементов. Тогда a может быть восстановлена из b с помощью следующей эквивалентности:

$$p \in a \leftrightarrow \forall q \leqslant p \exists r \in b \quad (q \text{ и } r \text{ совместны}).$$

Импликация слева направо выполняется в силу леммы о расширении и максимальности b. Предположим $p \notin a$. Если $a = [p \mid p \Vdash \Phi]$, то по (5.4) существует $q \leqslant p$ такое, что $q \Vdash \neg\Phi$. По (5.3) и лемме о расширении элемент r, совместный с q, не может вынуждать Φ, поэтому такого r не может быть в b.

Отсюда следует, что $|Q|$ равно самое большее числу подмножеств b из C, состоящих из попарно несовместных элементов. Так как $|b| < \mathfrak{m}$ для каждого такого b, то

$$|Q| \leqslant |S_{\mathfrak{m}}(C)| \leqslant |C|^{\mathfrak{m}}.$$

Пусть теперь $\mathfrak{m}$ и $\mathfrak{n}$ — кардиналы в M. Можно ли выбрать C так, чтобы M и $M[G]$ имели одинаковые кардиналы и $2^{\mathfrak{m}} = \mathfrak{n}$ в $M[G]$? Если это можно сделать, то

$$\mathfrak{n}^{\mathfrak{m}} = (2^{\mathfrak{m}})^{\mathfrak{m}} = 2^{\mathfrak{m}} = \mathfrak{n}$$

в $M[G]$. Так как $({}^{\mathfrak{m}}\mathfrak{n})^M \subset ({}^{\mathfrak{m}}\mathfrak{n})^{M[G]}$, а M и $M[G]$ имеют одинаковые кардиналы, то мы имеем $(\mathfrak{n}^{\mathfrak{m}})^M \leqslant (\mathfrak{n}^{\mathfrak{m}})^{M[G]}$. Следовательно, $\mathfrak{n}^{\mathfrak{m}} = \mathfrak{n}$ в M.

Поэтому предположим, что $\mathfrak{n}^{\mathfrak{m}} = \mathfrak{n}$ в M. Для того чтобы получить $2^{\mathfrak{m}} = \mathfrak{n}$, нам необходимо ввести $\mathfrak{n}$ подмножеств $\mathfrak{m}$. Фактически мы введем отображение F из $\mathfrak{n} \times \mathfrak{m}$ в 2 и возьмем $[\beta \mid F(\alpha, \beta) = 0]$ в качестве α-го подмножества из $\mathfrak{m}$. Пусть $C = H(\mathfrak{n} \times \mathfrak{m};\ 2)$. Положив $F = \bigcup_{p \in G} p$, видим, что F — отображение в $M[G]$ из $\mathfrak{n} \times \mathfrak{m}$ в 2. Для $\alpha < \mathfrak{n}$ положим $A_\alpha = [\beta \mid \beta < \mathfrak{m} \,\&\, F(\alpha, \beta) = 0]$. Тогда A_α — подмножество $\mathfrak{m}$ в $M[G]$. Кроме того, $\alpha \neq \alpha' \to A_\alpha \neq A_{\alpha'}$; это следует из того, что

$$[p \mid \exists\beta\, (p(\alpha, \beta) \,\&\, p(\alpha', \beta) \text{ определены и не равны})]$$

— плотное множество в M.

По лемме 10.3 и следствию к лемме 10.2 $\mathrm{cf}^M = \mathrm{cf}^{M[G]}$ и, кроме того, M и $M[G]$ имеют одинаковые кардиналы. В частности, $\mathfrak{m}$ и $\mathfrak{n}$ являются кардиналами в $M[G]$. Так как мы указали $\mathfrak{n}$ различных подмножеств $\mathfrak{m}$ в $M[G]$, то $2^{\mathfrak{m}} \geqslant \mathfrak{n}$ в $M[G]$. По лемме 11.1

$$(2^{\mathfrak{m}})^{M[G]} \leqslant ((|C|^{\aleph_0})^{\mathfrak{m}})^M.$$

Подсчитывая в M, имеем по (10.2)

$$|C| \leqslant (\mathfrak{m} \cdot \mathfrak{n})^{\aleph_0} = \mathfrak{n}$$

(так как из $\mathfrak{n}^{\mathfrak{m}} = \mathfrak{n}$ следует $\mathfrak{m} < \mathfrak{n}$); поэтому

$$(|C|^{\aleph_0})^{\mathfrak{m}} = |C|^{\mathfrak{m}} \leqslant \mathfrak{n}^{\mathfrak{m}} = \mathfrak{n}.$$

Отсюда $2^{\mathfrak{m}} = \mathfrak{n}$ в $M[G]$. Это доказывает следующую теорему.

Теорема 11.1. *Пусть $\mathfrak{m}$ и $\mathfrak{n}$ — бесконечные кардиналы в M такие, что $\mathfrak{n}^{\mathfrak{m}} = \mathfrak{n}$ в M. При подходящем выборе C*

имеем $\mathrm{cf}^M = \mathrm{cf}^{M[G]}$; *M и M[G] имеют одинаковые кардиналы и* $2^{\mathfrak{m}} = \mathfrak{n}$ *в M[G].*

Теперь предположим, что мы определили константу Γ в теории ZFC и доказали в теории ZFC, что Γ — кардинал. Мы хотели бы показать, что $2^{\aleph_0} = \Gamma$ совместно с теорией ZFC. В силу теоремы Кёнига мы требуем, чтобы $\mathrm{cf}(\Gamma) > \omega$ было доказуемым в теории ZFC. Допустим это и возьмем M удовлетворяющим аксиоме конструктивности, а значит, и GCH. Из GCH и $\mathrm{cf}(\Gamma) > \omega$ мы можем доказать $\Gamma^{\aleph_0} = \Gamma$, поэтому $(\Gamma^{\aleph_0})^M = \Gamma^M$. Выбирая C, как в теореме 11.1, имеем $2^{\aleph_0} = \Gamma^M$ в $M[G]$. Затем мы получим требуемый результат, если докажем, что $\Gamma^M = \Gamma^{M[G]}$. Вспоминая, что M и $M[G]$ имеют одинаковые кардиналы и одинаковые функции cf, мы видим, что равенство выполняется, если Γ, скажем, $\aleph_2$ или $\aleph_{\omega_1}$ или первый слабо недостижимый кардинал (при условии, что существует слабо недостижимый кардинал в M).

Предположим теперь, что GCH выполняется в M. Если $2^{\mathfrak{m}} = \mathfrak{n}$ в $M[G]$, то $2^{\mathfrak{p}} \geqslant \mathfrak{n}$ для $\mathfrak{p} \geqslant \mathfrak{m}$, поэтому GCH может быть ложной в $M[G]$ выше $\mathfrak{m}$. Покажем, что можно сохранить GCH ниже $\mathfrak{m}$, если $\mathfrak{m}$ регулярно в M.

Теорема 11.2. *Пусть* GCH *выполняется в M. Пусть* $\mathfrak{m}$ *и* $\mathfrak{n}$ — *бесконечные кардиналы из M такие, что* $\mathfrak{m}$ *регулярно в M и* $\mathrm{cf}(\mathfrak{n}) > \mathfrak{m}$ *в M. При подходящем выборе C имеем* $\mathrm{cf}^M = \mathrm{cf}^{M[G]}$, *M и M[G] имеют одинаковые кардиналы,* $2^{\mathfrak{m}} = \mathfrak{n}$ *в M[G] и* $\forall \mathfrak{p}\,(\mathfrak{p} < \mathfrak{m} \to 2^{\mathfrak{p}} = \mathfrak{p}^+)$ *выполняется в M[G].*

Доказательство. Возьмем $C = H^M_{\mathfrak{m}}(\mathfrak{m} \times \mathfrak{n}\,; 2)$. Условия теоремы показывают, что $\mathfrak{m}^{\mathfrak{m})} = \mathfrak{m}$ в M. Поэтому леммы 10.2 и 10.3 и следствие к лемме 10.6 показывают, что $\mathrm{cf}^M = \mathrm{cf}^{M[G]}$, а M и $M[G]$ имеют одинаковые кардиналы. Доказательство того, что $2^{\mathfrak{m}} = \mathfrak{n}$ в $M[G]$, по существу такое же, как раньше (отметим, что из $\mathrm{cf}(\mathfrak{n}) > \mathfrak{m}$ и GCH следует, что $\mathfrak{n}^{\mathfrak{m}} = \mathfrak{n}$). Если $\mathfrak{p} < \mathfrak{m}$, то $S^M(\mathfrak{p}) = S^{M[G]}(\mathfrak{p})$ по лемме 10.6. Так как M и $M[G]$ имеют одинаковые кардиналы и $2^{\mathfrak{p}} = \mathfrak{p}^+$ в M, то мы видим, что $2^{\mathfrak{p}} = \mathfrak{p}^+$ в $M[G]$.

Неизвестно, выполняется ли теорема 11.2, когда $\mathfrak{m}$ сингулярна в M. Простейшей нерешенной проблемой является следующая: будет ли совместным с теорией ZFC предположение, что $\forall n\,(n < \omega \to 2^{\aleph_n} = \aleph_{n+1})$ и $2^{\aleph_\omega} \neq \aleph_{\omega+1}$?

Историческая справка. Теорема 11.1 принадлежит Коэну, теорема 11.2 принадлежит Соловею.

12. Вынуждение с классами

До сих пор мы предполагали, что C — множество в M. Но иногда мы можем строить модели вынуждения и тогда, когда C — просто класс в M. Так как общая ситуация еще не исследована полностью, рассмотрим лишь одну частную проблему.

Эта проблема является обобщением результатов предыдущего параграфа. Предположим, что H — отображение множества бесконечных кардиналов из M в себя, которое является функционалом в M. Мы хотим выбрать C так, чтобы M и $M[G]$ имели одинаковые кардиналы и чтобы для каждого бесконечного кардинала $\mathfrak{m}$ в M было $2^{\mathfrak{m}} = H(\mathfrak{m})$ в $M[G]$.

Очевидно, мы должны иметь

$$\mathfrak{m} \leqslant \mathfrak{n} \to H(\mathfrak{m}) \leqslant H(\mathfrak{n}). \tag{12.1}$$

Кроме того,

$$\mathfrak{m} < \mathrm{cf}(H(\mathfrak{m})) \tag{12.2}$$

должно выполняться в M. Действительно, это выполняется в $M[G]$ по теореме Кёнига, а потому и в M по (10.1). Будем предполагать дополнительно, что M удовлетворяет аксиоме конструктивности *). В этом случае мы покажем, что M и $M[G]$ для подходящего C имеют одинаковые кардиналы, $\mathrm{cf}^M = \mathrm{cf}^{M[G]}$ и $2^{\mathfrak{m}} = H(\mathfrak{m})$ в $M(G)$ для каждого регулярного кардинала $\mathfrak{m}$ в M.

Замечание. Снова не очень много известно про сингулярные кардиналы. Ясно, что на H должны быть наложены дополнительные условия, если бы мы хотели включить в рассмотрение и этот случай. Например,

$$\forall n \in \omega\,(2^{\aleph_n} = \aleph_{\omega+1}) \to 2^{\aleph_\omega} = \aleph_{\omega+1}.$$

Действительно,

$$2^{\aleph_\omega} = 2^{\Sigma \aleph_n} = \Pi 2^{\aleph_n} = \aleph_{\omega+1}^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0} = \aleph_{\omega+1}.$$

*) Используется только GCH и вполне упорядоченность универсума, а можно обойтись и без последнего. Однако это не существенно для вопросов непротиворечивости.

Теперь опишем C. Пусть областью изменения $\mathfrak{m}$ и $\mathfrak{n}$ будут *регулярные* кардиналы из M. Положим

$$Q_{\mathfrak{m}}=[\langle\mathfrak{n},\ \alpha,\ \beta\rangle\mid\mathfrak{n}\leqslant\mathfrak{m}\ \&\ \alpha<H(\mathfrak{n})\ \&\ \beta<\mathfrak{n}].$$

Пусть C — множество всех функций p в M таких, что $\mathrm{Ra}(p)\subset 2$, $\mathrm{Do}(p)\subset\bigcup\limits_{\mathfrak{m}}Q_{\mathfrak{m}}$ и $|\mathrm{Do}(p)\cap Q_{\mathfrak{m}}|<\mathfrak{m}$ в M для каждого $\mathfrak{m}$.

Для $p,\ q\in C$ пусть $p\leqslant q$ означает $q\subset p$. Очевидно, что C — понятие вынуждения, которое является классом в M.

Естественно потребовать, чтобы генерическое множество пересекалось со всеми плотными классами в M. Поэтому мы выбираем G C-генерическим над M', где M' — множество всех классов в M. Так как M' счетно, то это может быть сделано по теореме существования.

Теперь определим $M[G]$, как раньше. Точно так же, как и раньше, мы доказываем, что $M[G]$ счетно и транзитивно и $M\subset M[G]$. При попытке обобщить результаты § 5 возникают трудности: индуктивное определение $p\Vdash^{*}a\neq\neq b$ уже не может быть дано в M. Поэтому мы будем действовать по-другому.

Пусть

$$C_{\mathfrak{m}}=[p\mid p\in C\ \&\ \mathrm{Do}(p)\subset Q_{\mathfrak{m}}],$$

$$C^{\mathfrak{m}}=[p\mid p\in C\ \&\ \mathrm{Do}(p)\cap Q_{\mathfrak{m}}=0].$$

Как $C_{\mathfrak{m}}$, так и $C^{\mathfrak{m}}$ содержат 1 и, следовательно, являются понятиями вынуждения. Кроме того, $C_{\mathfrak{m}}$ является множеством в M; функция, которая переводит $\mathfrak{m}$ в $C_{\mathfrak{m}}$, — функционал в M, а $C^{\mathfrak{m}}$ — класс в M.

Для $p\in C$ пусть $p_{\mathfrak{m}}$ будет ограничением p до $Q_{\mathfrak{m}}$ и пусть $p^{\mathfrak{m}}=p-p_{\mathfrak{m}}$. Легко проверить, что $p\to\langle p_{\mathfrak{m}},\ p^{\mathfrak{m}}\rangle$ — изоморфизм между C и $C_{\mathfrak{m}}\times C^{\mathfrak{m}}$, обращение которого переводит $\langle q,\ r\rangle$ в $q\cup r$. Пусть $G_{\mathfrak{m}}=[p_{\mathfrak{m}}\mid p\in G]$, $G^{\mathfrak{m}}=[p^{\mathfrak{m}}\mid p\in\in G]$. Тогда по теореме о произведении*) $G_{\mathfrak{m}}$ является $C_{\mathfrak{m}}$-генерическим над M, а $G^{\mathfrak{m}}$ — $C^{\mathfrak{m}}$-генерическим над $M[G^{\mathfrak{m}}]$.

*) Строго говоря, теорема о произведении здесь неприменима, но нужная часть доказательства переносится без затруднений.

Кроме того, G соответствует $G_{\mathfrak{m}}\times G^{\mathfrak{m}}$ при этом изоморфизме, т. е.

$$G=[p\cup q\mid p\in G_{\mathfrak{m}}\ \&\ q\in G^{\mathfrak{m}}].\tag{12.3}$$

Отсюда следует, что

$$G\cap C_{\mathfrak{m}}=G_{\mathfrak{m}}.\tag{12.4}$$

Заметим, что C — объединение всех $C_{\mathfrak{m}}$, тогда мы можем определить $\Delta(b)$ в M индукцией по $\mathrm{rk}(b)$ следующим образом: $\Delta(b)$ есть наименьшее $\mathfrak{m}$ такое, что $\Delta(a)\leqslant\mathfrak{m}$ для каждого $a\in\mathrm{Ra}(b)$ и $p\in C_{\mathfrak{m}}$ для каждого $p\in\mathrm{Do}(b)$. Докажем индукцией по $\mathrm{rk}(b)$, что

$$\Delta(b)\leqslant\mathfrak{m}\to K_G(b)=K_{G_{\mathfrak{m}}}(b).\tag{12.5}$$

Если $\langle a,\ p\rangle\in b$, то $\Delta(a)\leqslant\Delta(b)\leqslant\mathfrak{m}$, $\mathrm{rk}(a)<\mathrm{rk}(b)$, поэтому $K_G(a)=K_{G_{\mathfrak{m}}}(a)$ по индуктивному предположению. Кроме того, $p\in C_{\mathfrak{m}}$, поэтому $p\in G\leftrightarrow p\in G_{\mathfrak{m}}$ по (12.4). Отсюда $K_G(b)=K_{G_{\mathfrak{m}}}(b)$.

Теперь определим

$$a^{(\mathfrak{m})}=[\langle b^{(\mathfrak{m})},\ p\rangle\mid\langle b,\ p\rangle\in a\ \&\ p\in C_{\mathfrak{m}}].$$

Опять это есть функционал в M. Докажем

$$K_G(a^{(\mathfrak{m})})=K_{G_{\mathfrak{m}}}(a)\tag{12.6}$$

индукцией по $\mathrm{rk}(a)$. По индуктивному предположению и (12.4)

$$\begin{aligned}K_G(a^{(\mathfrak{m})})&=[K_G(b^{(\mathfrak{m})})\mid\exists p\in G(\langle b,\ p\rangle\in a\ \&\ p\in C_{\mathfrak{m}})]=\\&=[K_{G_{\mathfrak{m}}}(b)\mid\exists p\in G_{\mathfrak{m}}(\langle b,\ p\rangle\in a)]=\\&=K_{G_{\mathfrak{m}}}(a).\end{aligned}$$

Простая индукция показывает, что

$$\Delta(a^{(\mathfrak{m})})\leqslant\mathfrak{m}.\tag{12.7}$$

Из (12.5) и (12.6) получаем

$$M[G]=\bigcup_{\mathfrak{m}}M[G_{\mathfrak{m}}].\tag{12.8}$$

Кроме того,

$$\mathfrak{m}\leqslant\mathfrak{n}\to M[G_{\mathfrak{m}}]\subset M[G_{\mathfrak{n}}].\tag{12.9}$$

Действительно,

$$K_{G_{\mathfrak{m}}}(a)=K_G(a^{(\mathfrak{m})})=K_{G_{\mathfrak{n}}}(a^{(\mathfrak{m})})$$

по (12.6), (12.7) и (12.5).

Все $C_{\mathfrak{m}}$ имеют такой же язык вынуждения, как и C. Определим $p \Vdash^*_{\mathfrak{m}} \Phi$ для $C_{\mathfrak{m}}$, как раньше. Затем положим $\Delta(a, b)=\max(\Delta(a), \Delta(b))$ и определим

$$p \Vdash^* a \in b, \quad \text{если} \quad p_{\Delta(a,b)} \Vdash^*_{\Delta(a,b)} a \in b,$$
$$p \Vdash^* a \neq b, \quad \text{если} \quad p_{\Delta(a,b)} \Vdash^*_{\Delta(a,b)} a \neq b.$$

Лемма определимости и лемма о расширении тривиальны. Чтобы доказать лемму об истинности, скажем для $a \in b$, мы имеем для $\mathfrak{m}=\Delta(a, b)$:

$$\begin{aligned} \vdash_G a \in b &\leftrightarrow \vdash_{G_{\mathfrak{m}}} a \in b \text{ по } (12.5) \\ &\leftrightarrow \exists p \in G_{\mathfrak{m}} (p \Vdash^*_{\mathfrak{m}} a \in b) \\ &\leftrightarrow \exists p \in G (p_{\mathfrak{m}} \Vdash^*_{\mathfrak{m}} a \in b) \\ &\leftrightarrow \exists p \in G (p \Vdash^* a \in b). \end{aligned}$$

Теперь можно определить $p \Vdash^* \Phi$ для неатомных Φ и доказать все три леммы о вынуждении, как раньше.

Далее мы заметим, что $C_{\mathfrak{m}}$ удовлетворяет условию $\mathfrak{m}^+$-цепи (в M). Действительно, по лемме 10.3 $H_{\mathfrak{m}}(Q_{\mathfrak{m}}; 2)$ удовлетворяет условию $\mathfrak{m}^+$-цепи. Но $C_{\mathfrak{m}} \subset H_{\mathfrak{m}}(Q_{\mathfrak{m}}; 2)$ и элементы (из $C_{\mathfrak{m}}$), совместные в $H_{\mathfrak{m}}(Q_{\mathfrak{m}}; 2)$, являются совместными и в $C_{\mathfrak{m}}$, так как их объединение лежит в $C_{\mathfrak{m}}$. Это дает требуемый результат. Также отметим, что $C^{\mathfrak{m}}$ будет $\mathfrak{m}^+$-замкнутым в M.

Будем говорить, что $\{D_\beta\}_{\beta<\mathfrak{m}}$ есть *последовательность классов в* M, если множество пар $\langle p, \beta\rangle$ таких, что $p \in D_\beta$, является классом в M. Отметим, что лемма 10.4 обобщается на классы в M, а лемма 10.5 обобщается на последовательности классов в M.

Лемма 12.1. *Пусть $\{D_\beta\}_{\beta<\mathfrak{m}}$ — последовательность классов в M такая, что каждое D_β — плотное сечение в C. Тогда существует $q \in G^{\mathfrak{m}}$ такое, что*

$$\forall \alpha < \mathfrak{m} \exists p \in G_{\mathfrak{m}} (p \cup q \in D_\alpha).$$

Доказательство. Для $q \in C^{\mathfrak{m}}$ положим

$$D^q_\alpha=[p \mid p \in C_{\mathfrak{m}} \,\&\, p \cup q \in D_\alpha].$$

Достаточно выбрать $q \in G^{\mathfrak{m}}$ так, чтобы D^q_α было $C_{\mathfrak{m}}$-плотным для каждого $\alpha<\mathfrak{m}$. Поэтому, полагая

$$D'_\alpha=[q \mid q \in C^{\mathfrak{m}} \,\&\, D^q_\alpha \text{ является } C_{\mathfrak{m}}\text{-плотным}],$$

достаточно будет показать, что $\bigcap_{\alpha<\mathfrak{m}} D'_\alpha$ плотно. Ввиду вышеприведенных замечаний нам нужно лишь показать, что D'_α плотно.

Пусть $q' \in C^{\mathfrak{m}}$. Выберем r_β индуктивно в M так, чтобы $r_\beta \leqslant q'$, $r_\beta \in D_\alpha$ и для всех $\gamma<\beta$ имело место неравенство $(r_\beta)^{\mathfrak{m}} \leqslant (r_\gamma)^{\mathfrak{m}}$ и $(r_\beta)_{\mathfrak{m}}$ и $(r_\gamma)_{\mathfrak{m}}$ были несовместны.

Если существует много таких r_β, то используем определимое вполне упорядочение на D_α, имеющееся вследствие аксиомы конструктивности, для того чтобы выбрать одно такое r_β; если такого r_β не существует, то r_β не определено.

Так как $C_{\mathfrak{m}}$ удовлетворяет условию $\mathfrak{m}^+$-цепи в M, то мы видим, что наименьшее β такое, что r_β не определено, существует и удовлетворяет $|\beta| \leqslant \mathfrak{m}$ в M. Поэтому существует $q \in C^{\mathfrak{m}}$ такое, что $q \leqslant (r_\gamma)^{\mathfrak{m}}$ для всех $\gamma<\beta$ и $q \leqslant q'$. Мы должны показать, что $q \in D'_\alpha$, т. е. что D^q_α плотно.

Пусть $p \in C_{\mathfrak{m}}$. Тогда $p \cup q$ имеет расширение r в D_α. Так как r не является возможным значением для r_β, то $r_{\mathfrak{m}}$ совместно с некоторым $(r_\gamma)_{\mathfrak{m}}$. Пусть p' — общее расширение для $r_{\mathfrak{m}}$ и $(r_\gamma)_{\mathfrak{m}}$. Тогда $p' \leqslant r_{\mathfrak{m}} \leqslant p$ и $p' \cup q \leqslant \leqslant (r_\gamma)_{\mathfrak{m}} \cup (r_\gamma)^{\mathfrak{m}}=r_\gamma$, поэтому $p' \cup q \in D_\alpha$ и, следовательно, $p' \in D^q_\alpha$.

Лемма 12.2. *Пусть F — функционал в $M[G]$ такой, что $\mathfrak{m}$ содержится в области определения F. Тогда ограничение f функционала F до $\mathfrak{m}$ находится в $M[G]$. Если $[F(\alpha) \mid \alpha<\mathfrak{m}]$ содержится в некотором множестве из $M[G_{\mathfrak{m}}]$, то f находится в $M[G_{\mathfrak{m}}]$.*

Доказательство. Пусть $\Phi(x, y)$ — формула языка вынуждения такая, что

$$F(\bar{a})=\bar{b} \leftrightarrow \vdash_G \Phi(a, b). \tag{12.10}$$

Для каждого $\alpha < \mathfrak{m}$ положим

$$D_\alpha = [p \mid \exists b\,(p \Vdash \exists x \Phi(\hat{\alpha}, x) \to \Phi(\hat{\alpha}, b))].$$

Тогда $\{D_\alpha\}$ — последовательность классов в M. Применяя лемму 10.4, мы видим, что D_α — плотное сечение. Поэтому по лемме 12.1 существует $q \in G^{\mathfrak{m}}$ такое, что

$$\forall \alpha < \mathfrak{m} \exists p \in G_{\mathfrak{m}}\,(p \cup q \in D_\alpha). \tag{12.11}$$

Для $\alpha < \mathfrak{m}$ и $p \in C_{\mathfrak{m}}$ пусть $A_{\alpha, p}$ — множество всех таких b, что

$$p \cup q \Vdash \exists x \Phi(\hat{\alpha}, x) \to \Phi(\hat{\alpha}, b). \tag{12.12}$$

Пусть g — функция в M, область определения которой представляет собой множество пар $\langle \alpha, p \rangle$ из $\mathfrak{m} \times C_{\mathfrak{m}}$ таких, что $A_{\alpha, p} \neq 0$ и $g(\langle \alpha, p \rangle) \in A_{\alpha, p}$ для каждой такой пары $\langle \alpha, p \rangle$.

Покажем, что

$$f = [\langle K_G(b), \alpha \rangle \mid \exists p \in G_{\mathfrak{m}}\,(b = g(\langle \alpha, p \rangle))]. \tag{12.13}$$

По (12.11) для каждого $\alpha < \mathfrak{m}$ существует такое $p \in G_{\mathfrak{m}}$, что $A_{\alpha, p} \neq 0$, и, следовательно, такое, что $q(\langle \alpha, p \rangle)$ определено. Поэтому мы должны показать, что если $p \in G_{\mathfrak{m}}$ и $b = g(\langle \alpha, p \rangle)$, то $K_G(b) = f(\alpha)$. Так как (12.12) выполняется и $p \cup q \in G$ по (12.3), то $\vdash_G \exists x \Phi(\hat{\alpha}, x) \to \Phi(\bar{\alpha}, b)$. Отсюда и из (12.10) $F(\alpha) = K_G(b)$, поэтому $f(\alpha) = K_G(b)$.

Выберем $\mathfrak{n}$ так, чтобы $\mathfrak{m} \leqslant \mathfrak{n}$ и $\Delta(b) \leqslant \mathfrak{n}$ для $b \in \mathrm{Ra}(g)$. По (12.4) и (12.5) мы можем записать (12.13) следующим образом:

$$f = [\langle K_{G_{\mathfrak{n}}}(b), \alpha \rangle \mid \exists p \in G_{\mathfrak{n}}\,(b = g(\langle \alpha, p \rangle))].$$

Так как $G_{\mathfrak{n}} \in M[G_{\mathfrak{n}}]$ и существует функционал в $M[G_{\mathfrak{n}}]$, совпадающий с $K_{G_{\mathfrak{n}}}$ на аргументах в M, то отсюда следует, что $f \in M[G_{\mathfrak{n}}]$. Следовательно, $f \in M[G]$.

Теперь предположим, что $[F(\alpha) \mid \alpha < \mathfrak{m}] \subset K_{G_{\mathfrak{m}}}(a)$; мы хотим показать, что можно взять $\mathfrak{n} = \mathfrak{m}$. Переделаем D_α на множество таких p, что

$$\exists b \in \mathrm{Ra}(a^{(\mathfrak{m})})\,[p \Vdash \exists x\,(x \in a^{(\mathfrak{m})} \,\&\, \Phi(\hat{\alpha}, x)) \to \Phi(\hat{\alpha}, b)].$$

Для доказательства того, что оно плотно, мы должны отметить, что каждый элемент из $K_G(a^{(\mathfrak{m})})$ имеет имя в $\mathrm{Ra}(a^{(\mathfrak{m})})$ по (4.1).

Из того, что

$$\vdash_G \exists x\,(x \in a^{(\mathfrak{m})} \,\&\, \Phi(\alpha, x)) \to \Phi(\alpha, b),$$

получаем

$$F(\alpha) = K_G(b).$$

Далее используется (12.6).

Мы можем теперь предположить, что каждое b в $\mathrm{Ra}(g)$ содержится в $\mathrm{Ra}(a^{(\mathfrak{m})})$ и поэтому имеет вид $b'^{(\mathfrak{m})}$. Но $\Delta(b'^{(\mathfrak{m})}) \leqslant \mathfrak{m}$; таким образом, действительно можно взять $\mathfrak{n} = \mathfrak{m}$.

Лемма 12.3. *Если $\bar{a} \in M[G]$ и $\bar{a} \neq 0$, то существует $\mathfrak{m}$ такое, что $\bar{a} \in M[G_{\mathfrak{m}}]$, и отображение f из $\mathfrak{m}$ на $\bar{a}$, которое содержится в $M[G_{\mathfrak{m}}]$*

Доказательство. Выберем $\mathfrak{n}$ по (12.8) так, чтобы $\bar{a} \in M[G_{\mathfrak{n}}]$. Выберем $\mathfrak{m}$ так, чтобы $\mathfrak{n} \leqslant \mathfrak{m}$ и $|\bar{a}| \leqslant \mathfrak{m}$ в $M[G_{\mathfrak{n}}]$. Тогда существует f в $M[G_{\mathfrak{n}}]$, отображающая $\mathfrak{m}$ на $\bar{a}$, и $\bar{a}$, $f \in M[G_{\mathfrak{m}}]$ по (12.9).

Теперь проверим, что $M[G]$ удовлетворяет условиям леммы 2.1. Так как $\omega \in M \subset M[G]$, то (а) выполняется. Пусть теперь $\bar{a} \in M[G]$, $\bar{a} \neq 0$ и выберем $\mathfrak{m}$ и f, как в лемме 12.3. Предположим, что A — класс в $M[G]$ такой, что $A \subset \bar{a}$ и $A \neq 0$. Так как $f \in M[G]$, то легко определить функционал F в $M[G]$ с областью определения $\mathfrak{m}$ и областью значений A. По лемме 12.2 $F \in M[G_{\mathfrak{m}}]$; таким образом $A \in M[G_{\mathfrak{m}}] \subset M[G]$. Это доказывает (б). Это также показывает, что каждое подмножество из $\bar{a}$ в $M[G]$ содержится в $M[G_{\mathfrak{m}}]$ и, следовательно, в множестве степени для $\bar{a}$ в $M[G_{\mathfrak{m}}]$. Это доказывает (г).

Пусть теперь F — функционал в $M[G]$, и пусть $\bar{a}$ — непустое подмножество области определения F. Снова пусть $\mathfrak{m}$ и f таковы, как в лемме 12.3, и F_1 — функционал, определенный следующим образом: $F_1(\alpha) = F(f(\alpha))$. Тогда $F_1 \in M[G]$ по лемме 12.2. Поэтому для некоторого $\mathfrak{n}$ имеем $F_1 \in M[G_{\mathfrak{n}}]$, а также $U(\mathrm{Ra}(F_1)) \in M[G_{\mathfrak{n}}] \subset M[G]$. Но $U(\mathrm{Ra}(F_1)) = U([F(x) \mid x \in \bar{a}])$. Итак, мы доказали (в).

По лемме 2.1 $M[G]$ — модель теории ZF. Используя лемму 12.3, получаем, что $M[G]$ — модель теории ZFC.

Теперь покажем, что $\mathrm{cf}^M = \mathrm{cf}^{M[G]}$. Если это не так, то мы имели бы $\aleph_0 \leqslant \mathrm{cf}^{M[G]}(\alpha) < \mathrm{cf}^M(\alpha)$ для некоторого α. Положим $\mathfrak{m} = \mathrm{cf}^{M[G]}(\alpha)$. Это есть бесконечный кардинал в M, а так как $\mathfrak{m} = \mathrm{cf}^{M[G]}(\mathfrak{m}) \leqslant \mathrm{cf}^M(\mathfrak{m}) \leqslant \mathfrak{m}$, то он регулярен в M. Пусть f — отображение из $\mathfrak{m}$ на конфинальное подмножество из α такое, что $f \in M[G]$. По лемме 12.2 $f \in M[G_\mathfrak{m}]$. Следовательно, $\mathrm{cf}^{M[G_\mathfrak{m}]}(\alpha) \leqslant \mathfrak{m}$. С другой стороны, из $\mathfrak{m} < \mathrm{cf}^M(\alpha)$ следует $\mathfrak{m}^+ \leqslant \mathrm{cf}^M(\alpha)$, поэтому $\mathrm{cf}^M(\alpha) = \mathrm{cf}^{M[G_\mathfrak{m}]}(\alpha)$ по лемме 10.2. Таким образом, $\mathfrak{m} < \mathrm{cf}^M(\alpha) = \mathrm{cf}^{M[G_\mathfrak{m}]}(\alpha) \leqslant \mathfrak{m}$; получаем противоречие.

Из $\mathrm{cf}^M = \mathrm{cf}^{M[G]}$ следует, что M и $M[G]$ имеют одинаковые кардиналы; доказательство этого подобно доказательству леммы 10.2 (б).

Каждое непустое подмножество из $\mathfrak{m}$ в $M[G]$ есть образ $\mathfrak{m}$ относительно некоторого функционала в $M[G]$ и поэтому по лемме 12.2 содержится в $M[G_\mathfrak{m}]$. Тем самым $S^{M[G]}(\mathfrak{m}) = S^{M[G_\mathfrak{m}]}(\mathfrak{m})$, поэтому, чтобы доказать $2^\mathfrak{m} = H(\mathfrak{m})$ в $M[G]$, достаточно доказать это в $M[G_\mathfrak{m}]$. Полагая $F = U(G_\mathfrak{m})$ и

$$A_\alpha = [\beta \mid \beta < \mathfrak{m} \mathbin{\&} F(\mathfrak{m}, \alpha, \beta) = 0]$$

для $\alpha < H(\mathfrak{m})$, мы доказываем, как и раньше, что все A_α дают $H(\mathfrak{m})$ различных подмножеств $\mathfrak{m}$. Используя (12.1), имеем в M

$$|Q_\mathfrak{m}| \leqslant \mathfrak{m} \cdot H(\mathfrak{m}) \cdot \mathfrak{m} = H(\mathfrak{m})$$

(так как (12.2) дает $\mathfrak{m} < H(\mathfrak{m})$). Так как $C_\mathfrak{m} \subset H_\mathfrak{m}(Q_\mathfrak{m}; 2)$, получаем

$$|C_\mathfrak{m}| \leqslant H(\mathfrak{m})^{\mathfrak{m}} = H(\mathfrak{m})$$

по (10.2) и (12.2) *). Тогда по лемме 11.1

$$|S(\mathfrak{m})|^{M[G_\mathfrak{m}]} \leqslant (H(\mathfrak{m})^{\mathfrak{m} \cdot \mathfrak{m}})^M = H(\mathfrak{m}).$$

Таким образом, $2^\mathfrak{m} = H(\mathfrak{m})$ в $M[G_\mathfrak{m}]$.

Историческая справка. Все результаты этого параграфа принадлежат Истону [3].

*) И по (2.1), так как это можно вычислять в M, а в M выполнена GCH.— *Прим. ред.*

ЛИТЕРАТУРА К ПРИЛОЖЕНИЮ II

[1] P. J. Cohen, The independence of the continuum hypothesis, Parts I, II, Proc. Nat. Acad. Sci. U. S. A. **50** (1963), 1143—1148; **51** (1964), 105—110.

[2] P. J. Cohen, Set theory and the continuum hypothesis, Benjamin, New York, 1966. (Русский перевод: П. Дж. Коэн, Теория множеств и континуум-гипотеза, «Мир», 1969.)

[3] W. Easton, Powers of regular cardinals, Thesis, Princeton, University, 1964.

[4] S. Feferman, Some applications of the notion of forcing and generic sets, Fundam. Math. **56** (1965), 325—345.

[5] K. Gödel, The consistency of the axiom of choice and of the generalized continuum hypothesis with the axioms of set theory, Ann. of Math. Studies, No. 3, Princeton University Press, Princeton, N. J., 1940. (Русский перевод: К. Гёдель, Совместимость аксиомы выбора и обобщенной континуум-гипотезы с аксиомами теории множеств, УМН **3**, № 1 (1948), 96—149.)

[6] A. Lévy, Axiom schemata of strong infinity in axiomatic set theory, Pacific J. Math. **10** (1960), 223—238.

[7] A. Lévy, Definability in axiomatic set theory. I. (Proc. 1964 Internat. Congr.) Logic, Methodology and Philosophy of Science, North-Holland, Amsterdam, 1966.

[8] A. Mostowski, An undecidable arithmetical statement, Fundam. Math. **36** (1949), 143—164.

[9] J. C. Shepherdson, Inner models for set theory, Part I, J. Symbolic Logic **16** (1951), 161—190.