Конспект лекций

Аксиоматическая теория множеств — это список аксиом, из которых следуют все свойства множеств, используемые в математических рассуждениях.

Изучая этот список аксиом, мы сами используем некоторую “метатеорию”. У качестве метатеории можно выбрать наивную теорию множеств Кантора, или ту же самую аксиоматическую теорию множеств, или формальную арифметику Пеано. (В последнем случае мы не имеем права говорить об интерпретациях теории множеств.)

Мы будем использовать наивную теорию множеств в качестве метатеории, хотя все наши рассуждения можно провести и в аксиоматической теории множеств.

Объектами аксиоматической теории множеств являются множества без праэлементов, то есть элементами любого множества являются другие множества. Ничего, кроме множеств, в универсуме нет. (Примеры множеств без праэлементов: $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$.)

Поэтому в сигнатуру включаются только два нелогических символа: равенство и отношение принадлежности. Мы будем рассматривать только нормальные интерпретации этой сигнатуры: равенство интерпретируется как совпадение. Любую нормальную интерпретацию можно себе представлять, как ориентированный граф. Элементы носителя интерпретации (вершины графа) мы будем называть множествами.

0.1 Аксиомы теории множеств Цермело–Френкеля (ZF).

Все аксиомы ZF — замкнутые формулы сигнатуры $\langle =, \in \rangle$.

- Аксиома объемности: если два множества содержат одни и те же элементы, то они равны (то есть, совпадают). Эта аксиома используется для доказательства равенства двух множеств. (Ее не надо путать с определением равенства двух множеств. Равенство множеств в ZF определять не надо: равные множества — это совпадающие множества (одна и та же вершина графа).)

Из этой аксиомы следует, что пустое множество может быть только одно. (Но не следует его существование.)

- Аксиома существования пустого множества: существует множество, не содержащее элементов.

- Аксиома регулярности: в каждом непустом множестве есть элемент, не содержащий других элементов этого множества.

- Аксиома неупорядоченной пары: для любых двух множеств x, y существует множество, единственными элементами которых являются x и y. По аксиоме равенства такое множество единственно, поэтому мы имеем право использовать обозначения $\{x, y\}$ и $\{x\}$ для двух-элементных множеств и синглетона. Из этой аксиомы следует бесконечность количества множеств: все множества $\emptyset$, $\{\emptyset\}$, $\{\{\emptyset\}\}$, $\ldots$ попарно различны (это можно доказать внешней индукцией).

  Из аксиомы регулярности и этой аксиомы следует, что не существует множества, являющегося своим собственным элементом.

- Аксиома объединения. Для любого множества x существует множество, содержащее элементы элементов x и только их. Это множество будет обозначаться $\mathrm{Un}(x)$.

  Из этой аксиомы следует существование объединения двух множеств. В частности, она позволяет определить следующую важную операцию на множествах: $S(x) = x \cup \{x\}$. Забегая вперед, заметим, что многократно применяя эту операцию к пустому множеству, мы получим натуральные числа: $\emptyset$ (ноль), $\{\emptyset\}$ (один), $\{\emptyset, \{\emptyset\}\}$ (два), $\ldots$.

- Аксиома свертывания (точнее, схема аксиом). Пусть имеется формула $\varphi(x, y_1, \ldots, y_n)$ (под формулой мы всегда понимаем формулу языка первого порядка в сигнатуре $\langle \in, = \rangle$). Для любых множеств $y_1, \ldots, y_n$ и любого множества z существует множество v, которое содержит все $x \in z$, для которых выполнено $\varphi(x, y_1, \ldots, y_n)$, и не содержащая ничего другого.

В этой аксиоме важно, что заранее выбрано некоторое множество z, и мы выделяем из него множество элементов с некоторым свойством. Поэтому ее часто называют аксиомой выделения. Неограниченная аксиома свертывания, утверждающая, что для любых множеств $y_1, \ldots, y_n$ существует множество v, которое содержит все множества x, для которых выполнено $\varphi(x, y_1, \ldots, y_n)$, приводит к противоречию (парадокс Рассела). Этим объясняется, почему все предыдущие аксиомы (кроме аксиомы равенства и аксиомы регулярности), являющиеся частными случаями неограниченной аксиомы свертывания, нельзя заменить на нее саму.

Из этой аксиомы следует, что существование пустого множества следует из существования хотя бы одного множества. Из нее также следует существование пересечения и разности двух множеств.

- Аксиома степени: для любого множества x существует множество, содержащее все подмножества x и ничего другого. (Слова "и ничего другого" можно опустить, ведь у нас имеется аксиома выделения.) Это множество будет обозначаться через $\mathcal{P}(x)$.

- Аксиома замены (точнее, схема аксиом): пусть дана формула

$$\varphi(x, y, z_1, \ldots, z_n).$$

Для любых множеств $z_1, \ldots, z_n, u$ таких, что для всех $x \in u$ существует единственное y, для которого $\varphi(x, y, z_1, \ldots, z_n)$, существует множество v, содержащее все y такие, что для некоторого $x \in u$ выполнено $\varphi(x, y, z_1, \ldots, z_n)$. Иными словами, если $z_1, \ldots, z_n, u$ выбраны так, что формула φ задает всюду определенную на u функцию, то значения этой функции образуют некоторое множество.

Эта аксиома является вкладом Френкеля в аксиоматическую систему Цермело.

Осталась последняя аксиома. Прежде чем ее сформулировать, заметим, что система всех аксиом, приведенных выше, имеет счетную модель, в которой каждое множество конечно (счетный ориентированный граф, в котором входные степени всех вершин конечны). [Носитель — натуральные числа. Натуральное число n принадлежит натуральному числу m, если n-ый бит двоичной записи m равен 1.] Поэтому необходима аксиома, из которой следует существование бесконечных множеств.

- Аксиома бесконечности. Существует множество, которое содержит пустое множество, и которое для каждого своего элемента x содержит $S(x)$.

  Такое множество обязано быть бесконечным, поскольку оно содержит (попарно различные) множества $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, $\dots$. Этим объясняется ее название.

Перечисленное множество аксиом составляет аксиоматическую теорию множеств Цермело–Френкеля. Неизвестно, имеется ли модель у этой теории (то есть, существует ли ориентированный граф, удовлетворяющий всем аксиомам ZF). По знаменитой второй теореме Геделя о неполноте, если ZF имеет модель, то, используя в метатеории только аксиомы ZF, невозможно доказать существование модели ZF (= непротиворечивость ZF).

Теперь нам нужно убедиться, что можно дать определения обычных математических понятий (натурального числа, отношения, функции) таким образом, чтобы из аксиом ZF следовали те свойства этих понятий, которые мы используем в математических рассуждениях. (Мы говорим, что замкнутая формула φ следует из аксиом ZF, если φ истинна во всех моделях ZF. По теореме Геделя о полноте формула φ следует из аксиом ZF тогда и только тогда, когда φ выводится из аксиом ZF в исчислении предикатов с равенством.)

0.2 Отношения и функции

Проще всего с отношениями и функциями.

Сначала определим, что называется упорядоченной парой. Это понятие можно определить разными способами. Наиболее известный способ принадлежит Куратовскому: $\langle x, y\rangle = \{\{x\}, \{x, y\}\}$.

Лемма 1. *Упорядоченные пары совпадают тогда и только тогда, когда совпадают их первые и вторые компоненты.*

Из аксиомы степени следует существование декартова произведения любых двух множеств: декартово произведение x и y можно выделить из множества $\mathcal{P}(\mathcal{P}(x \cup y))$.

Бинарным отношением называется любое множество, состоящее только из упорядоченных пар. Функцией называется любое отношение, которое не содержит двух разных пар с одной первой компонентой.

Обычным образом определяются понятия области определения отношения и функции, понятие инъективной, сюръективной и биективной функции.

Лемма 2. *Для любого бинарного отношения существует область определения и множества значений. (В частности, это верно и для функций.)*

0.3 Ординалы.

Множество x называется транзитивным, если любой элемент любого элемента x снова является элементом x. Транзитивными являются множества $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, $\ldots$. Пример нетранзитивного множества — $\{\{\emptyset\}\}$.

Ординалом называется транзитивное множество, все элементы которого транзитивны. (Заметим, что транзитивность элементов не следует из транзитивности самого множества, контрпримером является транзитивное множество $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$, последний элемент которого нетранзитивен.)

Примеры ординалов: $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$.

Лемма 3. *Любой элемент любого ординала есть ординал.*

Мы говорим, что ординал α меньше ординала β, если α принадлежит β. Отношение принадлежности на ординалах транзитивно и иррефлексивно. Иными словами, отношение принадлежности задает частичный порядок на классе всех ординалов (мы не говорим “на множестве всех ординалов”, поскольку ординалы не образуют множества, как мы увидим ниже).

Лемма 4. *Пусть дана формула $\varphi(x, y_1, \ldots, y_n)$. Для любых множеств $y_1, \ldots, y_n$, для которых найдется ординал α такой, что $\varphi(\alpha, y_1, \ldots, y_n)$, найдется минимальный ординал β такой, что $\varphi(\beta, y_1, \ldots, y_n)$.*

Доказательство. Выберем ординал α такой, что $\varphi(\alpha, y_1, \ldots, y_n)$. Рассмотрим множество всех $\beta \in \alpha$, для которых $\varphi(\beta, y_1, \ldots, y_n)$. Такое множество существует по аксиоме выделения. Если оно пусто, то ординал α и есть искомый ординал. Иначе применим к нему аксиому регулярности. Элемент этого множества, не принадлежащий никаким другим его элементам, и есть искомый ординал. $\square$

Лемма 5. *Любые два ординала сравнимы (то есть, совпадают или один принадлежит другому).*

Доказательство. Допустим это не так. По предыдущей лемме существует минимальный ординал α, не сравнимый с некоторым ординалом. Еще раз применяя предыдущую лемму, заключаем, что существует минимальный ординал β, не сравнимый с α. Докажем, что α совпадает с β, получив тем самым противоречие.

Включение α в β. Любой элемент γ ординала α сравним со всеми ординалами, в частности, он сравним с β. Ординал γ не может ни содержать β, ни совпадать с ним (так как тогда α содержал бы β). Значит γ принадлежит β.

Включение β в α. По построению любой элемент γ ординала β сравним с α. Применив симметричные рассуждения, легко установить, что γ принадлежит α. □

Из доказанной леммы следует, что отношение принадлежности задает линейный порядок на классе всех ординалов. Более того, этот порядок полный. В частности, каждый ординал вполне упорядочен отношением принадлежности. Это объясняет употребление слова “ординал” (в наивной теории множеств Кантора ординальными числами называются классы подобия вполне упорядоченных множеств).

Поэтому для ординалов понятия “наименьший” и ”минимальный” совпадают. Наименьшим ординалом является пустое множество.

Ниже приводятся некоторые простые задачи про ординалы.

1. Если α ординал, то $S(\alpha)$ тоже ординал.

2. Ординал α меньше ординала β тогда и только тогда, когда α является собственным подмножеством β.

3. Для любого ординала α, ординал $S(\alpha)$ непосредственно следует за α в порядке на ординалах (следовательно, ординалов бесконечно много).

4. Объединение любого множества ординалов снова является ординалом, причем наименьшим из всех ординалов, больших или равных всех ординалов из этого множества.

5. Для любого множества ординалов существует ординал, больший всех ординалов этого множества (следовательно, не существует множества, содержащего все ординалы).

Классификация ординалов: ординалы делятся на три класса: 0 (пустое множество), последователи (ординалы вида $S(\alpha)$) и предельные ординалы (все остальные ординалы).

6. Докажите, что каждый предельный ординал равен объединению всех меньших ординалов.

Трансфинитная индукция. Пусть дана формула $\varphi(x, y_1, \ldots, y_n)$ и множества $y_1, \ldots, y_n$ такие, что одноместное отношение $\varphi(x, y_1, \ldots, y_n)$ обладает следующим свойством: для любого ординала α, если для всех ординалов β меньших α выполнено $\varphi(\beta, y_1, \ldots, y_n)$, то тогда выполнено и $\varphi(\alpha, y_1, \ldots, y_n)$. Тогда для всех ординалов α выполнено $\varphi(\alpha, y_1, \ldots, y_n)$.

0.4 Трансфинитная рекурсия

Пусть дана формула $\varphi(f, y)$ и вполне упорядоченное множество A, обладающие следующим свойством. Для любого $x \in A$ и любой функции f, определенной на всех элементах множества A, меньших x, существует единственное y, для которого $\varphi(f, y)$.

Мы хотим определить функцию f рекурсивно: пусть f уже определена на всех элементах A меньших x (и не определена на остальных), тогда мы полагаем $f(x)$ равным такому y, для которого $\varphi(f, y)$ (по условию такое y существует и единственно).

Теорема 1. *При этих условиях существует единственная функция f с областью определения A, для которой для всех $x \in A$ выполнено*

$$\varphi(f|\{z \in A \mid z < x\}, f(x)).$$

С помощью трансфинитной рекурсии можно показать, что каждое вполне упорядоченное множество A изоморфно некоторому ординалу. Действительно, трансфинитной индукцией мы определяем функцию f, которая сопоставляет каждому $x \in A$ наименьший ординал, отличный от всех $f(z)$ для $z < x$. Множество значений так определенной функции является искомым ординалом.

Поскольку любые два ординала сравнимы, отсюда следует, что из любых двух вполне упорядоченных множеств одно изоморфно начальному отрезку другого.

0.5 Внешние и внутренние множества

Пусть V — некоторая модель ZF (ориентированный граф, удовлетворяющий всем аксиомам ZF). В мета-теории мы будем часто рассматривать подмножества множества V, называя их внешними множествами. Чтобы отличить внешние множества от элементов V, которые мы также называем множествами, мы будем называть последние внутренними множествами. Мы говорим, что внешнее множество A соответствует внутреннему множеству $y \in V$, если для всех $x \in V$ выполнено $x \in y \Leftrightarrow x \in A$. (В левой части этой равносильности знак принадлежности понимается как наличие дуги в графе, а в правой части как обычная, внешняя, принадлежность.) В этом случае мы отождествляем внешнее множество с соответствующим ему внутренним множеством.

Например, само множество V является внешним множеством, ему не соответствует никакое внутреннее множество. То же самое относится и ко внешнему множеству всех ординалов.

Внешнее множество называется классом, если его элементы можно выделить из V формулой первого порядка с параметрами из V.

0.6 Натуральные числа

Внешней индукцией мы можем определить для каждого (внешнего) натурального числа i внутреннее множество $S^i(\emptyset)$. Таким образом, мы получаем внешнее множество $\{S^i(\emptyset) \mid i = 0, 1, \dots\}$. Оно может не быть ни внутренним множеством, ни классом. С этим связана трудность в определении натуральных чисел: мы хотели бы определить натуральные числа в V, как элементы V вида $S^i(\emptyset)$, но не можем этого сделать, поскольку получаемое так внешнее множество может не быть внутренним.

Определение. Множество x называется натуральным числом, если x является непредельным ординалом (то есть, нулем или последователем) и все элементы x являются непредельными ординалами.

Нетрудно проверить истинность всех аксиом Пеано:

(1) 0 является натуральным числом.

(2) Если x натуральное число, то и $S(x)$ — натуральное число.

(3) 0 не является последователем.

(4) Если последователи двух натуральных чисел равны, то и сами натуральные числа равны.

(5) Аксиома индукции. Если некоторое множество натуральных чисел содержит 0, и для каждого своего элемента содержит его последователь, то оно содержит все натуральные числа.

Обычным образом (рекурсивно) мы можем определить сложение и умножение, а также порядок (порядок получится тот же самый, что и порядок на ординалах):

$n+0=n$, $n+S(m)=S(n+m)$,
$n*0=0$, $n*S(m)=n*m+n$,
$n \le m$, если $n+k=m$ для некоторого натурального k.

Из аксиом Пеано выводятся обычные свойства этих операций.

Лемма 6. *Существует множество, содержащее все натуральные числа и только их. (Оно обозначается через ω или $\aleph_0$). Множество всех натуральных чисел является наименьшим предельным ординалом.*

Доказательство. В множестве, удовлетворяющем аксиоме бесконечности, выделим множество всех натуральных чисел. Оно удовлетворяет аксиоме индукции, следовательно, содержит все натуральные числа.

Множество ω транзитивно, поскольку любой элемент натурального числа снова является натуральным числом. Любой элемент множества ω транзитивен, поскольку является ординалом. Если бы множество натуральных чисел имело вид $S(x)$, то x было бы натуральным числом, а значит и $S(x)$ содержалось бы в ω, как натуральное число, а это невозможно по аксиоме регулярности. Наконец, любой предельный ординал содержит все натуральные числа, что доказывается по индукции, а значит включает ω. □

Определение 1. Множество называется конечным, если оно равномощно некоторому натуральному числу.

Замечание. Все множества вида $S^i(\emptyset)$ являются натуральными числами. Это доказывается внешней индукцией. Однако могут быть натуральные числа, не имеющие такого вида. Иногда их называют нестандартными натуральными числами.

0.7 Кумулятивная иерархия

Для каждого ординала α определим рекурсивно некоторое внутреннее множество V_α. Оно состоит из всех подмножеств объединения V_β по всем ординалам β меньшим α.

Например, V_0 содержит только пустое множество, V_1 содержит еще и 1.

Рангом множества x называется наименьшее α, для которого x принадлежит V_α. Обозначение $rk(x)$.

Лемма 7. *Для любого множества x найдется ординал α, для которого x принадлежит V_α, то есть любое множество имеет ранг.*

Доказательство. Нам понадобится понятие транзитивного замыкания множества. Пусть x произвольное множество. Определим индукцией по натуральным числам $x_0 = x$, $x_{n+1} = \mathrm{Un}(x_n)$ и положим $y = \bigcup_{n\in\omega} x_n$. Множество y транзитивно, включает x и является наименьшим по включению множеством, обладающим этими свойствами.

Если все элементы данного множества имеют ранг, то и само множество имеет ранг. Действительно, его рангом будет наименьший ординал, строго больший всех рангов его элементов.

Допустим, существует множество x, не имеющее ранга. Тогда и его транзитивное замыкание y не имеет ранга, а значит некоторый его элемент не имеет ранга. Применив аксиому регулярности к множеству всех элементов y, не имеющих ранга, мы найдем элемент z множества y, который не имеет ранга, но все его элементы имеют ранг. Противоречие. $\square$

Ранг множества равен наименьшему ординалу, строго большему рангов его элементов. Поэтому ранг любого ординала равен ему самому.

0.8 Кардиналы

Кардиналом называется ординал, который не равномощен никакому меньшему ординалу.

В аксиоматической теории множеств ZFC (так обозначается теория ZF с добавленной аксиомой выбора AC) можно определить понятие мощности множества. По теореме Цермело каждое множество из V равномощно некоторому ординалу α, а значит и некоторому кардиналу (наименьшему ординалу из равномощных α). Этот кардинал называется мощностью множества.

Кстати, теорему Цермело в ZFC можно доказать следующим образом: зафиксировав некоторую функцию выбора на непустых подмножествах множества A, которое нужно вполне упорядочить, мы определяем вложение A в класс всех ординалов. Образ A при этом вложении и будет ординалом, равномощным A.

Задачи.

1. Все натуральные числа являются кардиналами.

2. Множество натуральных чисел ω является кардиналом (часто этот кардинал обозначают $\aleph_0$).

3. Для любого кардинала $\aleph$ имеется наименьший кардинал, больший $\aleph$. Он обозначается через $\aleph^+$.

4. Для любого множества кардиналов имеется кардинал, больший всех кардиналов этого множества.

5. Постройте формулу, осуществляющую взаимно однозначное соответствие между классом всех ординалов и классом всех кардиналов.

6. Постройте формулу, осуществляющую взаимно однозначное соответствие между ординалами и предельными ординалами.

7. Постройте формулу, осуществляющую взаимно однозначное соответствие между ординалами и парами, первая компонента которых ординал, а вторая — натуральное число.

8. Постройте формулу, осуществляющую взаимно однозначное соответствие между парами ординалов и ординалами.

[Указание. Упорядочим пары ординалов следующим образом: пара $\langle\alpha_1, \beta_1\rangle$ меньше пары $\langle\alpha_2, \beta_2\rangle$, если выполнено одно из трех: (1) $\max\{\alpha_1, \beta_1\} < \max\{\alpha_2, \beta_2\}$, или (2) $\max\{\alpha_1, \beta_1\} = \max\{\alpha_2, \beta_2\}$ и $\alpha_1 < \alpha_2$ или (2) $\max\{\alpha_1, \beta_1\} = \max\{\alpha_2, \beta_2\}$, $\alpha_1 = \alpha_2$ и $\beta_1 < \beta_2$. Сопоставим ординалу τ наименьшую пару, не сопоставленную меньшим ординалам (рекурсивное определение).]

9. Докажите, что любой бесконечный кардинал равномощен своему декартову квадрату, причем взаимно однозначное соответствие можно задать формулой.

1 Совместимость аксиомы выбора и континуум-гипотезы с ZF

1.1 Абсолютные формулы

Пусть фиксированы (нормальные) интерпретации V и $M \subset V$, причем отношение принадлежности на M заимствовано из V. Мы говорим, что формула $\varphi(x)$ абсолютна для расширения $M \subset V$, если для любого $u \in M$ выполнено

$$V \models \varphi(u) \Leftrightarrow M \models \varphi(u).$$

Аналогично определяется абсолютность формул с несколькими параметрами.

Формула называется абсолютной, если она абсолютна для любых расширений $M \subset V$ таких, что M — транзитивное подмножество V.

Лемма 8. *Семейство абсолютных формул одержит все атомные формулы и замкнутое относительно связывания всеми логическими связками и навешивания кванторов вида $(\forall x \in y)$, $(\exists x \in y)$. (В частности, оно включает семейство всех формул с ограниченными кванторами — наименьшее семейство формул, содержащее все атомные формулы и замкнутое относительно связывания всеми логическими связками и навешивания кванторов вида $(\forall x \in y)$, $(\exists x \in y)$.)*

Из леммы следует абсолютность следующих формул.

1. Формула $x \subset y$ (то есть, стандартная формула, определяющая включение).

2. Формула "x транзитивно" (то есть, стандартная формула, определяющая это понятие).

3. Формула "x — ординал".

4. Формула $y = S(x)$.

5. Формула "x — предельный ординал".

6. Формула "x — натуральное число".

7. Свойство $x = \omega$ также можно записать формулой с ограниченными кванторами "x предельный ординал, и любой ненулевой элемент x является последователем некоторого другого элемента x".

Теперь сформулируем достаточное условие того, что в результате навешивания неограниченного квантора на абсолютную формулу получается абсолютная формула.

Лемма 9. *Пусть формула $\varphi(x, y)$ абсолютна для расширения $M \subset V$. Пусть для всех $y \in M$, если в V существует x, для которого в V истинно $\varphi(x, y)$, то и в M существует x, для которого в V истинно $\varphi(x, y)$. Тогда формулы $\exists x\ \varphi(x, y)$, $\forall x\ \varphi(x, y)$ абсолютны для расширения $M \subset V$. То же самое справедливо и для формул с любым числом параметров.*

Применим эту лемму для доказательства абсолютности формулы "x конечно" для любого расширения $M \subset V$, такого что M транзитивная модель ZF. Индукцией по натуральному числу $n \in V$ можно доказать, что если f является функцией из n в M, то f принадлежит M. Отсюда следует, что если $f \in V$ является биекцией между некоторым натуральным числом n и множеством $x \in M$, то f принадлежит M.

Примеры неабсолютных формул: "$x = \mathcal{P}(y)$", "x — кардинал", "x — счетно". Эти формулы могут быть неабсолютными даже для расширений

$M \subset V$ таких, что M и V — модели ZF и M транзитивно. Для первой формулы причина в том, что в V может быть больше подмножеств y, чем в M, для второй — в V может существовать биекция x и меньшего ординала, отсутствующая в M, для третьей — в V может быть биекция x и ω, которой нет в M.

1.2 Конструктивные множества

Теорема 2. *Если существует модель ZF, то существует и модель ZFC. (То есть, если ZF имеет модель, то отрицание аксиомы выбора не следует из ZF. Синтаксическая формулировка — если теория ZF непротиворечива, то отрицание аксиомы выбора не выводится из ZF в исчислении предикатов с равенством.)*

Эта теорема доказывается с помощью конструктивных множеств. Фиксируем V — модель ZF.

Модель, в которой будет истинна аксиома выбора, является подмножеством V, состоящим из всех “конструктивных” множеств. Отношение принадлежности на конструктивных множествах заимствуется из V.

Конструктивные множества составляют наименьшее по включению транзитивное внешнее подмножество $L \subset V$, которое является моделью ZF и содержит все ординалы. Существование такого подмножества можно можно доказать двумя способами: по Коэну и по Геделю. При первом способе используется внутреннее понятие определимости формулами с параметрами. При втором способе конструктивные множества определяются как наименьшее подмножество V, содержащее все ординалы и замкнутое относительно нескольких довольно простых операций.

1.2.1 Конструктивные множества по Коэну

Обычным образом определим внутреннее для V понятие формулы нашей сигнатуры. Например, формулами можно считать любые конечные последовательности натуральных чисел, отождествив каждый из символов алфавита формул с некоторым натуральным числом. Затем можно определить внутри V понятие истинности формул с параметрами (индукцией по длине формулы).

Каждой внешней формуле φ можно сопоставить внутреннюю формулу $\varphi' \in V$. Это соответствие сохраняет истинность: $V \models \varphi$ тогда и только тогда, когда в V истинно утверждение об истинности φ'. То же самое верно и любых формул с параметрами и доказывается внешней индукцией по длине формулы.

Поскольку не любое натуральное число является натуральным числом с внешней точки зрения, и не любая конечная последовательность натуральных чисел конечна с внешней точки зрения, не каждая внутренняя формула в V имеет вид φ'. Формулы, не имеющие такого вида, можно назвать нестандартными.

Пусть $M \in V$. Множество $A \in V$ называется определимым над M, если для некоторой внутренней формулы $\varphi(x, p)$ из V и некоторого $u \in M$ множество A состоит из всех $x \in M$ для которых в M истинно $\varphi(x, u)$. (Формула φ может иметь несколько параметров, а не только один, вместо каждого из них надо подставить элемент из M.)

В этом определении важно, что мы рассматриваем внутренние формулы. Эта дает возможность записать свойство определимости над M формулой с параметром M. Множества, определимые над M внешними формулами, являются определимыми над M (множество, определимое внешней формулой φ, определимо также соответствующей ей внутренней формулой φ'). Обратное может оказаться неверным.

По трансфинитной рекурсии сопоставим каждому ординалу из V некоторое внутреннее множество L_α в V. Для этого введем обозначение

$$L_{<\alpha} = \bigcup_{\beta<\alpha} L_\beta$$

и положим

$$L_\alpha = (\text{множество всех определимых над } L_{<\alpha} \text{ множеств}).$$

Если $\beta < \alpha$, то каждое множество y из L_β определимо над $L_{<\alpha}$ формулой $x \in y$, следовательно L_α включает L_β.

Множество называется конструктивным, если для некоторого ординала α оно принадлежит L_α. Класс конструктивных множеств обозначается через L, или L^V, если надо подчеркнуть зависимость от исходной модели V. Будем называть порядком конструктивного множества x наименьшее α, для которого x принадлежит L_α.

Определение конструктивного множества инвариантно в следующем смысле. Пусть U есть транзитивное внешнее подмножество V, содержащее все ординалы из V и являющееся моделью ZF (с отношением принадлежности, заимствованным из V). Поскольку понятие ординала абсолютно для расширения $U \subset V$, все ординалы из U являются ординалами и с точки зрения V и обратно. То есть можно говорить о том, что U и V имеют одинаковые ординалы.

Определим, как описано выше, конструктивные множества в U. Чтобы отличить их друг от друга, будем использовать обозначения $L^U(\alpha)$ и $L^V(\alpha)$. Тогда трансфинитной индукцией можно показать, что $L^U(\alpha) = L^V(\alpha)$ для всех α.

Действительно, поскольку множества натуральных чисел в U и V одинаковы, множества формул в них тоже одинаковы. Понятие истинности формулы при данных значениях параметров абсолютно для расширения $U \subset V$ (это доказывается индукцией по длине формулы). Поэтому из равенства $L^U(\beta) = L^V(\beta)$ для всех $\beta < \alpha$ следует равенство $L^U(\alpha) = L^V(\alpha)$.

В частности, мы доказали абсолютность формулы "$x = L_\alpha$" для расширения $U \subset V$.

Из доказанного следует, что $L^V = L^U \subset U$, а значит, L включено в любую транзитивную модель $U \subset V$ теории ZF.

Как мы объявили ранее, L является наименьшим по включению транзитивным подмножеством V, которое является моделью ZF и содержит все ординалы. Минимальность уже доказана. Транзитивность выполнена по построению (каждое из множеств L_α транзитивно). Осталось доказать, что L является моделью ZF и содержит все ординалы.

Лемма 10. *Для любого ординала α выполнено $\alpha \in L_\alpha$. Следовательно, все ординалы конструктивны.*

Доказательство. Докажем по трансфинитной индукции, что любой ординал конструктивен и его порядок равен ему самому.

Пусть это верно для всех ординалов, меньших α. Рассмотрим абсолютную формулу "x — ординал". По построению множество $L_{<\alpha}$ транзитивно, поэтому эта формула выделяет из $L_{<\alpha}$ все ординалы. По индуктивному предположению $L_{<\alpha}$ содержит все ординалы, меньшие α и никаких других. Это доказывает, что $\alpha \in L_\alpha$.

Осталось доказать, что α не принадлежит L_β для всех ординалов $\beta \in \alpha$. Допустим, что это не так для некоторого $\beta \in \alpha$. Тогда β, будучи элементом α, принадлежит $L_{<\beta}$, значит его порядок меньше β. Это противоречит индуктивному предположению. □

1.2.2 Принцип отражения

Пусть каждому ординалу $\alpha \in V$ сопоставлено некоторое множество $W_\alpha \in V$, причем соответствие $\alpha \mapsto W_\alpha$ задается некоторой формулой. Положим W равным объединению W_α по всем ординалам из V и положим

$$W_{<\alpha} = \bigcup_{\beta<\alpha} W_\beta.$$

Теорема 3. *Для любого ординала $\beta \in V$ и любой формулы $\varphi(x)$ найдется такой ординал $\alpha > \beta$, что*

$$W \models \varphi(u) \Leftrightarrow W_{<\alpha} \models \varphi(u)$$

для всех $u \in W_{<\alpha}$.

Все то же самое справедливо и для формул с любым количеством параметров и для любого конечного числа формул. Последнее означает, что для любого (внешнего) конечного множества формул Φ для любого ординала β найдется такой ординал $\alpha > \beta$, что для любой формулы φ из Φ с параметрами из $W_{<\alpha}$ истинность φ в W равносильна ее истинности в $W_{<\alpha}$.

Утверждение теоремы можно записать в виде схемы аксиом, Пусть φ — формула с параметром x. Обозначим через φ^B формулу, полученную из φ релятивизацией всех кванторов к B. Это означает, что каждое вхождение квантора всеобщности $\forall z$ в φ заменяется на ограниченный квантор $(\forall z \in B)$ и аналогично для кванторов существования. Тогда утверждение теоремы означает истинность в V формулы

$$\forall\beta(\exists\alpha > \beta)(\forall x \in W_{<\alpha})(\varphi^{W_{<\alpha}} \leftrightarrow \varphi).$$

Это объясняет употребление слова "принцип" (принципами обычно называют схемы аксиом). Употребление слова "отражение" объясняется так. Пусть V — модель ZF. Говорят, что множество $M \in V$ отражает формулу φ (относительно V), если для всех $u \in M$ выполнено

$$V \models \varphi(u) \Leftrightarrow M \models \varphi(u)$$

(иными словами, формула φ абсолютна для расширения $M \subset V$). Из теоремы 3 следует, что для любой формулы φ существуют сколь угодно большие ординалы α, для которых V_α отражает φ. (Это — одна из стандартных формулировок принципа отражения.)

Доказательство. Без ограничения общности мы можем считать, что формула φ содержит только кванторы существования (формула $\forall y\psi$ эквивалентна формуле $\neg\exists y\neg\psi$). Обозначим через Ψ список всех подформул формулы φ, которые начинаются с квантора существования.

Определим (внутреннюю, то есть, принадлежащую V) последовательность ординалов $\beta_0 < \beta_1 < \beta_2 < \dots$ по индукции. Положим $\beta_0 = \beta$. Если β_i уже определено, то β_{i+1} получается так. Для каждой истинной (в V) формулы $\exists y\psi(y, a_1, \dots, a_k)$ из Ψ с параметрами из $W_{<\beta_i}$ рассмотрим наименьший ранг b, для которого формула $\psi(b, a_1, \dots, a_k)$ истинна. По аксиоме замены ординалы, сопоставленные всем таким парам (формула, значения ее параметров) образуют множество. В качестве β_{i+1} возьмем объединение всех ординалов этого множества.

Положим α равным объединению всех ординалов $\beta_0, \beta_1, \beta_2, \dots$.

Докажем, что $W_{<\alpha}$ отражает (относительно W) все подформулы формулы φ индукцией по длине подформулы.

Для атомных формул это очевидно. Ясно также, что семейство отражаемых $W_{<\alpha}$ формул замкнуто относительно связывания логическими связками. Осталось рассмотреть случай, когда подформула имеет вид $\exists y\psi(y, a_1, \dots, a_k)$. Если эта формула истинна в $W_{<\alpha}$, то существует b из $W_{<\alpha}$, для которого утверждение $\psi(b, a_1, \dots, a_k)$ истинно в $W_{<\alpha}$. По индуктивному предположению, она истинна и в W, а значит и формула $\exists y\psi(y, a_1, \dots, a_k)$ истинна W.

В обратную сторону: допустим формула $\exists y\psi(y, a_1, \dots, a_k)$ истинна в W. Рассмотрим такое i, что все $a_1, \dots, a_k$ принадлежат $W_{<\beta_i}$. По построению в $W_{<\beta_{i+1}}$ (а значит и в $W_{<\alpha}$) найдется b, для которого $\psi(b, a_1, \dots, a_k)$ истинно в W. По индуктивному предположению $\psi(b, a_1, \dots, a_k)$ истинно в $W_{<\alpha}$. □

Замечания.

1. Почему доказательство принципа отражения не проходит для бесконечного числа формул? Скажем, почему аналогичным образом не удается доказать, что существует $B \in V$, отражающее все вообще формулы? Ответ таков: при доказательстве существования множества A_{i+1}, содержащего свидетелей для данной формулы вида $\exists x\psi$ мы используем аксиому замены для некоторой формулы, в состав которой входит ψ. Если количество формул, которые нам надо обслужить, было бы бесконечным, то нам пришлось бы использовать бесконечные формулы.

2. Пусть Φ некоторое конечное множество аксиом ZF. По первому

принципу отражения в любой модели V теории ZF имеется множество B, в котором истинны все аксиомы из Φ. На синтаксическом уровне это означает, что из аксиом ZF можно вывести формулу

$$\exists B \bigwedge_{\varphi\in\Phi} \varphi^B.$$

(Можно доказать этот факт и чисто синтаксически, переведя доказательство принципа отражения на синтаксический язык.)

Более того, каждой внешней формуле φ в любой модели V теории ZF соответствует внутренняя формула $\varphi'_V \in V$. Это соответствие сохраняет истинность: φ истинна в $B \in V$ тогда и только тогда, когда φ'_V истинна в B во внутреннем смысле. Таким образом, в любой модели V имеется множество B, в котором истинны все формулы вида φ'_V для $\varphi \in \Phi$. На синтаксическом уровне это означает, что из аксиом ZF можно вывести формулы

$$(\Phi \text{ имеет модель}), \qquad (\Phi \text{ непротиворечиво}).$$

Не противоречит ли это второй теореме Геделя о неполноте, гласящей в частности, что в ZF нельзя доказать непротиворечивость ZF? Ведь если каждое конечное подмножество ZF непротиворечиво, то и все множество аксиом ZF непротиворечиво.

Дело тут в том, что для каждого подмножества Φ мы получаем свое доказательство непротиворечивости Φ безо всякой равномерности по Φ. Чтобы этим способом доказать в ZF непротиворечивость ZF, нам нужно вывести в ZF формулу "любое конечное множество $\Phi \subset ZF$ имеет модель". Заметим еще, что внутренняя теория ZF может быть шире внешней теории ZF (за счет нестандартных формул).

1.2.3 Продолжение доказательства.

Теорема 4. *Класс конструктивных множеств является моделью ZF.*

Доказательство. Аксиомы *регулярности* и *объемности* верны в любом транзитивном подмножестве множества V, а L транзитивно по построению.

Аксиома *пары*: формула "$x = \{y, z\}$" абсолютна. Поэтому достаточно доказать, что если y, z конструктивны, то и множество $\{y, z\}$ конструктивно. Если y принадлежит L_α, а z принадлежит L_β, то $\{y, z\}$ определимо формулой с параметрами y, z в L_γ при $\gamma = S(\max\{\alpha, \beta\})$.

Аксиома *объединения*: если A принадлежит L_α, то $\mathrm{Un}(A)$ принадлежит $L_{<S(\alpha)}$, поскольку определимо над L_α формулой

$$\exists y(y \in A \wedge x \in y).$$

Осталось заметить, что формула $u = \mathrm{Un}(v)$ абсолютна.

Аксиома *степени*. Свойство "быть подмножеством" абсолютно, поэтому нам достаточно доказать, что множество всех конструктивных подмножеств любого конструктивного множества A конструктивно. Пусть $A \in L_\beta$. Каждому конструктивному подмножеству A сопоставим его порядок. По аксиоме замены мы получим некоторое множество ординалов. Пусть α любой ординал, больший всех ординалов этого множества и больший β.

Тогда $L_{<\alpha}$ содержит все конструктивные подмножества A и их множество выделяется из $L_{<\alpha}$ абсолютной формулой $x \subset A$, а значит принадлежит L_α.

Аксиома *выделения*. Пусть $\varphi(x,p)$ (внешняя) формула, и $A, B \in L_\beta$. Нам нужно показать, что в L истинна формула

$$\exists y \forall x(x \in y \leftrightarrow x \in A \wedge \varphi(x,B)).$$

Истинность этой формулы в L означает, что множество

$$\{x \in A \mid L \models \varphi(x,B)\}$$

конструктивно. По принципу отражения (теорема 3), примененному к отображению $\alpha \mapsto L_\alpha$ и формуле φ, найдется ординал $\alpha > \beta$, для которого это множество совпадает с множеством

$$\{x \in A \mid L_{<\alpha} \models \varphi(x,B)\}.$$

Значит, оно определяется над $L_{<\alpha}$ внешней формулой

$$x \in A \wedge \varphi(x,B),$$

а следовательно принадлежит L_α.

Аксиома *замены* доказывается аналогично аксиоме выделения: пусть имеется формула $\varphi(x,y,u)$ и конструктивные множества A, B такие, что в L истинна формула

$$(\forall x \in A)\ \exists! y\ \varphi(x,y,B).$$

Нам нужно доказать, что множество

$$C = \{y \in L \mid L \models (\exists x \in A)\varphi(x, y, B)\}$$

(это множество существует, поскольку в V истинна аксиома замены) конструктивно. Применим принцип отражения к формуле $\varphi(x, y, z)$ и любому ординалу, большему порядка B и порядков всех элементов $A \cup C$. Для полученного ординала α для всех $x \in A$ и $y \in C$ выполнено

$$L \models \varphi(x, y, B) \Leftrightarrow L_{<\alpha} \models \varphi(x, y, B),$$

следовательно

$$C = \{y \in L_{<\alpha} \mid L_{<\alpha} \models (\exists x \in A)\varphi(x, y, B)\}.$$

Значит множество C может быть определено над $L_{<\alpha}$ формулой

$$(\exists x \in A)\varphi(x, y, B).$$

(Можно рассуждать и по-другому — применить уже доказанную аксиому выделения к множеству $L_{<\alpha}$ и этой формуле, где α — любой ординал больший порядков всех множеств из C.)

Аксиома *бесконечности*. Множество ω конструктивно, как любой ординал. Нетрудно убедиться, что формула

$$\emptyset \in x \wedge (\forall y \in x)\ S(y) \in x$$

абсолютна. Поэтому ординал ω удовлетворяет этой формуле и в L, а значит аксиома бесконечности истинна в L. □

Закончим доказательство теоремы 2. Рассмотрим утверждение "любое множество конструктивно". Это утверждение записывается формулой первого порядка и называется аксиомой конструктивности. Аксиома конструктивности обозначается через $V = L$. Докажем, что во-первых аксиома конструктивности истинна в L, а во-вторых из аксиом ZF и аксиомы конструктивности следует аксиома выбора, то есть, аксиома выбора истинна в любой модели теории ZFL = ZF + $(V = L)$.

1.2.4 Истинность аксиомы конструктивности в L.

Как мы уже отмечали формула $x \in L_\alpha$ абсолютна для любого расширения $U \subset V$ такого, что U транзитивная модель ZF, содержащая все ординалы из V. В частности, это верно и для $U = L$. Поэтому для любого конструктивного множества x найдется ординал α, для которого формула $x \in L_\alpha$ истинна в L. Поскольку свойство быть ординалом тоже абсолютно, и множества ординалов V и L совпадают, аксиома конструктивности верна в L.

1.2.5 Истинность аксиомы выбора в любой модели ZFL

Осталось доказать, что из аксиомы конструктивности следует аксиома выбора. Для этого мы напишем формулу с двумя параметрами, которая нумерует ординалами все конструктивные множества (а значит, все множества, если $V = L$). Это несложно сделать по трансфинитной рекурсии. Сначала зафиксируем формульное взаимно-однозначное соответствие между ординалами и кортежами из ординалов любой конечной длины. Ординал, соответствующий кортежу будем называть его номером. Каждое множество x из L_α можно задать тройкой $\langle\alpha$; номер формулы, задающей x; номер кортежа, состоящего из номеров параметров этой формулы$\rangle$. Первая и последняя компонента — ординалы, а вторая — натуральное число. Занумеруем все тройки такого вида ординалами так, чтобы третья компонента любой тройки не превосходила его номера. Теперь мы можем рекурсивно определить $K(\tau)$ (конструктивное множество с номером τ), как множество выделяемое в $L_{<\alpha}$ формулой номер i с со значениями параметров $K(\beta_1), \ldots, K(\beta_n)$, где $\langle\alpha, i, \text{номер } \langle\beta_1, \ldots, \beta_n\rangle\rangle$ — это тройка номер α. Если n не равно количеству параметров i-ой формулы, положим $K(\tau)$ равным пустому множеству. Чтобы это определение было корректным нам нужно, чтобы для всех j было $\beta_j < \tau$. Этого легко добиться, если выбрать нумерацию кортежей ординалов ординалами так, чтобы все компоненты любого кортежа ординалов, не превосходили его номера, а для всех компонент, кроме первой компоненты, были строго меньше его номера (номер 0 при этом использоваться не будет, а конструктивное множество с номером 0 определяется как пустое множество).

1.2.6 Конструктивные множества по Геделю

k-местным функционалом на V называется внешнее отображение из V^k в V, задаваемое некоторой формулой с $k+1$ параметром. Функционал называется абсолютным, если он может быть задан абсолютной формулой.

Мы зафиксируем некоторый конечный список абсолютных функционалов $F_1, \ldots, F_N$. Зафиксируем также формульное взаимно однозначное соответствие между ординалами и парами вида (натуральное число, кортеж ординалов произвольной конечной длины) такое, что все ординалы из кортежа, составляющего вторую компоненту пары, меньше номера пары (если первый компонент не равен нулю).

Затем для каждого ординала α рекурсивно определим $C(\alpha)$ (конструктивное множество с номером α), как результат применения функционала F_i к кортежу конструктивных множеств $\langle C(\beta_1), \ldots, C(\beta_k)\rangle$, где α — номер пары $\langle i, \langle \beta_1, \ldots, \beta_k\rangle\rangle$. Если i отлично от $1, \ldots, N$ или k не равно валентности F_i, то положим $C(\alpha) = \{C(\beta) \mid \beta < \alpha\}$.

Положим $L = \{C(\alpha) \mid \alpha - \text{ординал}\}$. По построению множество L замкнуто относительно применения всех функционалов $F_1, \ldots, F_N$. Кроме того, оно обладает следующие свойством: если все элементы некоторого множества $x \in V$ конструктивны, то x можно расширить до конструктивного множества.

Мы подберем функционалы $F_1, \ldots, F_N$ так, чтобы L стало транзитивной моделью ZF, содержащей все ординалы. Докажем сначала, что этого достаточно.

Как и раньше доказывается, что в L истинна аксиома конструктивности $\forall x\ \exists \alpha\ x = C(\alpha)$. Действительно, пусть U любое транзитивное подмножество V, в котором истинны все аксиомы ZF. Из абсолютности функционалов $F_1, \ldots, F_N$ следует абсолютность формулы $x = C(\alpha)$ для расширения $U \subset V$. Если дополнительно известно, что U содержит все ординалы из V, то и формула

$$\exists \alpha\ (\alpha - \text{ординал и } x = C(\alpha))$$

абсолютна. В частности эта формула абсолютна для расширения $L \subset V$. Для любого конструктивного множества x эта формула истинна в V, а значит и в L.

Из абсолютности формулы $x = C(\alpha)$ относительно расширения $L \subset$

V следует, что L включено в любую транзитивную модель ZF, содержащую все ординалы.

Как и раньше, из аксиомы конструктивности следует аксиома выбора.

Осталось доказать следующее утверждение.

Теорема 5. *Существует конечный набор абсолютных функционалов $F_1, \ldots, F_N$ такой, что множество L является транзитивной моделью ZF, содержащей все ординалы.*

Доказательство. Во-первых, положим $F_1(x, y) = \{x, y\}$. Все остальные функционалы будут обладать следующим свойством: любой элемент множества $F_i(x_1, \ldots, x_k)$ может быть получен из элементов транзитивного замыкания $x_1 \cup \cdots \cup x_k$ конечным числом применения функционала спаривания. (Будем говорить, что функционалы, обладающие этим свойством, имеют конечную глубину.) Отсюда следует

Лемма 11. *Множество L транзитивно.*

Доказательство. Докажем индукцией по α, что транзитивное замыкание $C(\alpha)$ включено в L. Пусть нам известно, что транзитивные замыкания каждого из множеств $x_1, \ldots, x_k$ включены в L, а функционал F имеет конечную глубину. Требуется доказать, что транзитивное замыкание $F(x_1, \ldots, x_k)$ включено в L. Рассмотрим множество A, которое получится, если замкнуть транзитивное замыкание множества $x_1 \cup \cdots \cup x_k$ относительно операции спаривания. Поскольку L замкнуто относительно спаривания, множество A включено в L. Поскольку добавление к транзитивному множеству неупорядоченной пары любых его элементов, не нарушает транзитивности, множество A транзитивно. Поэтому транзитивное замыкание множества $F(x_1, \ldots, x_k)$ включено в A, а значит и в L. □

Из леммы следует, что в L истинны аксиомы объемности, регулярности и взятия неупорядоченной пары.

Теперь посмотрим, какие функционалы понадобится включить, чтобы была истинна аксиома выделения. Мы хотим, чтобы была истинна следующая

Лемма 12. *Пусть дана формула φ, все параметры которой включены в список $x_1, \ldots, x_n$, и дано конструктивное множество B. Тогда множество кортежей $\langle a_1, \ldots, a_n \rangle \in B$, удовлетворяющих в L формуле φ, конструктивно.*

По определению $\langle a_1, \ldots, a_n \rangle = \langle a_1, \langle a_2, \ldots, \langle a_{n-1}, a_n \rangle \ldots \rangle \rangle$. Будем доказывать эту лемму индукцией по построению формулы φ, увеличивая по ходу список функционалов.

Доказательство. Пусть φ имеет вид $x_i \in x_j$. Без ограничения общности мы можем считать, что $i \neq j$. Нам нужны функционалы, которые позволяют выделить из B все кортежи $\langle a_1, \ldots, a_n \rangle$, для которых $a_i \in a_j$. Ясно, что нам нужен функционал

$$B \mapsto \{\langle a_1, a_2 \rangle \in B \mid a_1 \in a_2\}.$$

Если $n = 2$, $i = 1$, $j = 2$, то этого функционала достаточно. Если $n > 2$, $i = 1$, $j = 2$, то нужен еще функционал

$$B \mapsto \{\langle a_1, \langle a_2, a_3 \rangle \rangle \in B \mid a_1 \in a_2\}.$$

При других значениях i, j, n нам нужны функционалы, которые позволяют переставлять члены кортежа произвольным образом. Нетрудно убедиться, что для этого достаточно иметь функционалы

$$B \mapsto \{\langle \langle a, b \rangle, c \rangle \mid \langle a, \langle b, c \rangle \rangle \in B\},$$

$$B \mapsto \{\langle a, \langle b, c \rangle \rangle \mid \langle \langle a, b \rangle, c \rangle \in B\},$$

$$B \mapsto \{\langle a, \langle c, \langle b, d \rangle \rangle \rangle \mid \langle a, \langle b, \langle c, d \rangle \rangle \rangle \in B\}$$

(любая перестановка есть композиция транспозиций соседних элементов).

Пусть φ имеет вид $x_i = x_j$. Чтобы доказать лемму для этой формулы, нам нужны функционалы

$$B \mapsto \{\langle a_1, a_2 \rangle \in B \mid a_1 = a_2\}, \qquad B \mapsto \{\langle a_1, \langle a_2, a_3 \rangle \rangle \in B \mid a_1 = a_2\}.$$

Для формул вида $\psi \wedge \eta$ и $\neg\psi$ нам нужны операции пересечения и взятия разности.

Пусть дана формула $\psi = \exists y \varphi(y, x_1, \ldots, x_n)$ и конструктивное множество B. Каждому кортежу $\langle a_1, \ldots, a_n \rangle$ из B, для которого в L истинно утверждение $\exists y\ \varphi(y, a_1, \ldots, a_n)$, сопоставим конструктивное множество y с наименьшим номером, для которого в L истинно $\varphi(y, a_1, \ldots, a_n)$. По аксиоме все такие y образуют некоторое множество. Расширим это множество до некоторого конструктивного множества C.

По индуктивному предположению для множества $C \times B$ (в число функционалов надо включить декартово произведение) и формулы φ множество

$$\{\langle y, a_1, \ldots, a_n\rangle \in C \times B \mid L \models \varphi(y, a_1, \ldots, a_n)\}$$

конструктивно. Искомое множество равно проекции этого (включим в список функционалов проекцию).

Нетрудно проверить, что все функционалы, использованные нами в доказательстве, абсолютны и имеют конечную глубину. □

Теперь мы можем доказать аксиому выделения. Пусть имеется формула $\varphi(x, y)$ и конструктивные множество A, C. (Мы разбираем случай двух параметров, общий случай аналогичен.) Нам нужно доказать конструктивность множества

$$\{x \in A \mid L \models \varphi(x, C)\}.$$

Применим лемму ко множеству $B = A \times \{C\}$, а затем возьмем проекцию полученного множества.

Аксиомы объединения, степени и замены следуют из аксиомы выделения и того, что любое множество из V, все элементы которого конструктивны, может быть расширено до некоторого конструктивного множества. Действительно, множество, существование которого утверждают эти аксиомы, выделяется формулой из последнего.

Аксиома бесконечности следует из того, что все ординалы (а значит и ω) конструктивны. Докажем это трансфинитной индукцией. Пусть все ординалы меньшие α конструктивны. Тогда α можно расширить до некоторого конструктивного множества A. Формула “x — ординал” выделяет из C некоторый ординал β, который не меньше α. Поскольку мы уже доказали, что аксиома выделения истинна в L, ординал β принадлежит L, а значит и α принадлежит L по транзитивности. □

1.3 Совместимость континуум-гипотезы с ZF

Нам понадобится следующая форма принципа отражения.

Теорема 6. *Пусть V модель ZFC. Для любой формулы $\varphi(x)$ и любого счетного и транзитивного $A \in V$ найдется счетное транзитивное множество $M \in V$ такое, что для всех $u \in A$ выполнено*

$$V \models \varphi(u) \Leftrightarrow M \models \varphi(u)$$

Заметим, что не утверждается, что M отражает φ, поскольку в качестве u можно брать только элементы A (а не более широкого множества M, как в обычном принципе отражения).

Но если формула φ замкнута, то M отражает φ, а мы будем применять эту теорему только для замкнутых формул. Все то же самое справедливо и для формул с любым количеством параметров и для любого конечного числа формул (найдется множество M, для которого истинность в M равносильна истинности в V для всех формул).

Доказательство. Сначала построим счетное нетранзитивное множество B, включающее A и отражающее φ (в обычном смысле). Без ограничения общности мы можем считать, что формула φ содержит только кванторы существования (формула $\forall y\psi$ эквивалентна формуле $\neg\exists y\neg\psi$). Обозначим через Ψ список всех подформул формулы φ, которые начинаются с квантора существования.

Определим (внутреннюю, то есть, принадлежащую V) последовательность подмножеств $A_0 \subset A_1 \subset A_2 \subset \dots$ по индукции. Положим $A_0 = A$. Если A_i уже определено, то A_{i+1} получается добавлением к A_i для каждой истинной (в V) формулы $\exists y\psi(y, a_1, \dots, a_k)$ из Ψ с параметрами из A_i, некоторого одного такого b, для которого формула $\psi(b, a_1, \dots, a_k)$ истинна.

Для того, чтобы выбрать такое b нам требуется аксиома выбора. Положим B равным объединению всех A_i. Индукцией по длине подформулы нетрудно доказать, что B отражает все подформулы формулы φ

Все множества A_i счетны, а значит и множество B счетно. Однако B может быть нетранзитивным. Можно было бы попытаться сделать B транзитивным, переходя к транзитивному замыканию на четных шагах. Однако, построенное множество B может оказаться несчетным, потому что добавляемые множества b могли быть несчетными.

Поэтому мы поступим по-другому: мы выбросим из каждого $x \in B$, все его элементы, не принадлежащие B, и то же самое сделаем для всех оставшихся элементов x, элементов его элементов и т.д. В результате, некоторые элементы B могут стать равными, и B “сожмется”. Чтобы определить эту операцию аккуратно, надо использовать индукцию по рангу. А именно, рекурсией по рангу $x \in B$ определим

$$\bar{x} = \{\bar{y} \mid y \in x \cap B\}.$$

(Аксиома замены гарантирует, что такое множество есть в V.) Далее, положим

$$\bar{B} = \{\bar{x} \mid x \in B\}.$$

По построению множество $\bar{B}$ транзитивно.

Докажем, что отображение $x \mapsto \bar{x}$ является изоморфизмом B и $\bar{B}$. Это означает, что для всех x, y из B выполнено

$$x \in y \Leftrightarrow \bar{x} \in \bar{y}, \qquad x = y \Leftrightarrow \bar{x} = \bar{y}.$$

Первая из импликаций слева направо верна по построению, а вторая очевидна. Импликации справа налево мы докажем совместной трансфинитной индукцией. Упорядочим неупорядоченные пары ординалов $\{\alpha, \beta\}$ следующим образом: сначала сравниваем наименьшие члены пары и объявляем тот ординал меньшим, у которого наименьший из членов пары меньше. Если наименьшие члены пар равны, то сравниваем наибольшие члены. Этот порядок полный и обладает следующим свойством: при уменьшении любого члена пары, сама пара тоже уменьшается.

Мы будем доказывать утверждение трансфинитной индукцией по неупорядоченной паре, состоящей из рангов x и y. Сначала докажем первую импликацию. Пусть $\bar{x} \in \bar{y}$. Это означает, что найдется $z \in y \cap B$, для которого $\bar{x} = \bar{z}$. Поскольку $z \in y$, ранг z меньше ранга y, а значит к паре $\{x, z\}$ можно применить индуктивное предположение. Следовательно, для нее выполнена вторая равносильность, а значит $x = z$, следовательно, $x \in y$.

Докажем вторую импликацию. Пусть x не равно y. Без ограничения общности мы можем считать, что в B выполнена аксиома объемности (для этого при построении B надо включить ее и ее подформулы в множество Ψ). Поэтому в B найдется элемент z, который принадлежит симметрической разности x и y. Пусть, скажем, z принадлежит x и не принадлежит y. Тогда по построению $\bar{z} \in \bar{x}$. К паре $\{z, y\}$ можно применить предположение индукции и заключить, что $\bar{z}$ не принадлежит $\bar{y}$.

Докажем теперь, что отображение $x \mapsto \bar{x}$ тождественно на A, то есть, для всех $x \in A$ выполнено $\bar{x} = x$. Это доказывается индукцией по рангу x. Если $x \in A$, то $x \subset A \subset B$ в силу транзитивности A. Поэтому

$$\bar{x} = \{\bar{y} \mid y \in x \cap B\} = \{y \mid y \in x\} = x.$$

В частности, отсюда следует, что $\bar{B}$ включает A.

Итак, интерпретации B и $\bar{B}$ изоморфны над A, а значит элементарно эквивалентны над A. Последнее означает, что для всех $a \in A$ выполнено

$$B \models \varphi(a) \Leftrightarrow \bar{B} \models \varphi(a).$$

Поскольку B отражает φ, левая часть равносильности эквивалентна тому, что $\varphi(a)$ истинно в V.

Осталось заметить, что $\bar{B}$ счетно, поскольку отображение $x \mapsto \bar{x}$ осуществляет биекцию B и $\bar{B}$, и B по построению счетно. □

Теорема 7. *Континуум-гипотеза верна в любой модели ZFL.*

Доказательство. Пусть V любая модель ZFL. Нам достаточно доказать, что для любого подмножества D натурального ряда существует счетный ординал α, для которого $x = C(\alpha)$. Действительно, отсюда следует, что множество всех подмножеств натурального ряда можно вложить в множество счетных ординалов, мощность которого равна $\aleph_1$ (первый несчетный ординал).

Напомним, что если в транзитивном подмножестве U множества V истинны все аксиомы ZF, то формула $x = C(\alpha)$ абсолютна для расширения $U \subset V$. В доказательстве этого факта используется лишь то, что в U истинно лишь некоторое конечное число аксиом ZF, а не все аксиомы, которых бесконечно много, Можно и не копаться в доказательстве, а воспользоваться теоремой Мальцева о компактности. А именно, добавим в сигнатуру теории множеств константу U, а к аксиомам ZF добавим аксиомы φ^U для каждой аксиомы φ теории ZF. Тогда из аксиом полученной теории следует утверждение об абсолютности формулы $x = C(\alpha)$ относительно расширения $U \subset V$. По теореме компактности оно следует из некоторого конечного подмножества этой теории.

Итак, существует конечное множество Φ аксиом ZF такое, что любое транзитивное подножество V, в котором истинны все формулы из Φ, отражает формулу $x = C(\alpha)$. Добавим в Φ еще и аксиому конструктивности

$$\forall x \exists \alpha\ (\alpha - \text{ординал } \wedge x = C(\alpha)).$$

Применим теорему 6 к конъюнкции всех формул из Φ и множеству $A = \omega \cup \{D\}$. По теореме найдется счетное транзитивное множество $B \supset A$, в котором истинны все формулы из Φ. В частности, формула $x = C(\alpha)$ абсолютна для расширения $B \subset V$ и в B истинна аксиома конструктивности.

Последнее означает, что для каждого $x \in B$ в B имеется ординал α, для которого $x = C(\alpha)$. По условию D принадлежит A, а значит и B. Значит, такой ординал α есть и для $x = D$. Поскольку B транзитивно, множество α включено в B, следовательно, счетно. Это и требовалось доказать. □

Замечание. В доказательстве можно использовать и иерархию конструктивных множеств L_α. Аналогичным образом можно доказать, что для любого $D \subset \omega$ существует счетный ординал α, для которого $D \in L_\alpha$. Поскольку для счетных ординалов α множество L_α счетно, множество $L_{<\aleph_1}$ имеет мощность не более $\aleph_1$.

2 Генерические расширения и вынуждение

2.1 Генерические расширения

Для генерических расширений нам понадобится модель ZFC, содержащая счетное транзитивное множество M, также являющееся моделью ZFC. Сначала объясним, почему существует такая модель.

Теорема 8. *Допустим теория ZFC имеет модель. Тогда существует модель ZFC, содержащая счетное транзитивное множество, также являющееся моделью ZFC.*

Доказательство. Добавим в сигнатуру языка теории множеств константу c, а к аксиомам все аксиомы ZFC, релятивизованные множеством c, а также утверждения о счетности и транзитивности c. Нам нужно доказать, что получившаяся теория
$S = \mathrm{ZFC} + \mathrm{ZFC}^c + (c \text{ счетно}) + (c \text{ транзитивно})$
имеет модель. По теореме компактности Мальцева нам достаточно доказать, что любое конечное подмножество S имеет модель. Пусть R состоит из всех формул из ZFC^c, попавших в R и пусть V — любая модель ZFC. По принципу отражения в V имеется транзитивное счетное множество M, отражающее конъюнкцию всех формул из R. Поскольку все эти формулы истинны в V, они истинны и в M. Множество M поэтому годится в качестве интерпретации константы c. □

Итак, пусть V модель ZFC, а M — транзитивное множество в V, также являющееся моделью ZFC. Пусть T — произвольное непустое множество из M, а g функция из T в $\{0, 1\}$, принадлежащая V (но не M). Мы собираемся определить некоторое транзитивное множество из V, обозначаемое $M[g]$. Если g генерическая функция (что неформально означает, что g является функцией общего положения, то есть не обладает никакими особыми свойствами), то $M[g]$ будет моделью ZFC, причем наименьшей по включению моделью, расширяющей M и содержащей g. Модель $M[g]$ будет называться генерическим расширением M.

Перейдем к определению $M[g]$. Обозначим через P множество всех конечных частичных функций из T в $\{0,1\}$. Конечными множествами считаются те, для которых есть биекция между некоторым натуральным числом и множеством. Поскольку понятие натурального числа абсолютно и все натуральные числа из V принадлежат M, любое внешнее конечное подножество M принадлежит M, понятие конечного множества тоже абсолютно.

На множестве M определим двуместное отношение обозначаемое

$$a \in_g b \leftrightharpoons (\exists p \in P)\ p \subset g,\ \langle p, a\rangle \in b$$

С этим отношением множество M можно рассматривать как интерпретацию сигнатуры $\{=, \in\}$, однако эта интерпретация не удовлетворяет аксиоме объемности.

Поэтому мы преобразуем ее в транзитивное множество с помощью сжатия (уже использованного нами однажды при доказательстве второго принципа отражения). А именно, для каждого множества $a \in M$ определим $a[g]$ трансфинитной индукцией по рангу a:

$$a[g] = \{b[g] \mid b \in M, b \in_g a\}.$$

Положим

$$M[g] = \{a[g] \mid a \in M\}.$$

Множество a называется именем множества $a[g]$, у каждого множества из $M[g]$ есть много имен. По построению множество $M[g]$ транзитивно, а значит в нем истинны аксиомы объемности и регулярности (какой бы ни была функция g).

Докажем, что $M[g]$ включает M и содержит g. Именем множества $a \in M$ будет множество $\hat{a}$, которое определяется рекурсивно

$$\hat{a} = \{\langle \emptyset, \hat{b}\rangle \mid b \in a\}.$$

Действительно, для любого g выполнено $x \in \hat{a}[g] \Leftrightarrow (x = \hat{b}[g]$ для некоторого $b \in a)$, поэтому трансфинитной индукцией можно доказать, что $\hat{a}[g] = a$ для всех $a \in M$.

Именем множества g будет множество

$$\{\langle \{p\}, \hat{p} \rangle \mid p \in T \times \{0,1\}\}.$$

В множестве $M[g]$ истинна аксиома пары, поскольку, если a, b являются именами, соответственно, x, y из $M[g]$, то именем $\{x, y\}$ будет, например, множество $\{\langle \emptyset, a \rangle, \langle \emptyset, b \rangle\}$.

В $M[g]$ также истинна аксиома бесконечности: $M[g]$ включает все ординалы из M, в частности ω, которое и удовлетворяет в $M[g]$ аксиоме бесконечности (поскольку $M[g]$ транзитивно, свойство, требуемое в аксиоме бесконечности, абсолютно).

С аксиомой объединения уже не все так просто: очевидно, что

$$\mathrm{Un}(a[g]) = \{c[g] \mid (\exists b \in M)\ c \in_g b \in_g a\}.$$

Однако в M может не быть такого d, для которого

$$c \in_g d \Leftrightarrow (\exists b \in M)\ c \in_g b \in_g a.$$

Заметим, что объединение любых двух множеств из $M[g]$ также принадлежит $M[g]$, поскольку именем $a[g] \cup b[g]$ будет $a \cup b$.

С остальными аксиомами также возникают проблемы. С аксиомой множества всех подмножеств проблема такая: хотелось бы сказать, что именем множества всех подмножеств $a[g]$ является множество

$$c = \{\langle \emptyset, \hat{b} \rangle \mid b \subset a\}.$$

Для этого множества выполнено

$$c[g] = \{b[g] \mid b \subset a\} \subset \mathcal{P}(a[g]).$$

Обратное, однако, может быть неверным, поскольку из $b[g] \subset a[g]$ не следует $b \subset a$.

С аксиомами выделения и замены трудность в том, что у нас нет возможности определять в M истинность в $M[g]$. Все эти трудности можно преодолеть, если наложить на g дополнительные требования.

Перейдем к определению. Будем обозначать через Ω множество всех функций из T в $\{0,1\}$, принадлежащих в V. Для $p \in P$ через Ω_p мы обозначаем подножество Ω, состоящее из тех функций, которые продолжают p. Множества такого вида называются интервалами.

Объединения множеств вида Ω_p называются открытыми. Множество $B \subset P$ будем называть базой открытого множества $\bigcup_{p \in B} \Omega_p$. (Открытое множество может иметь много разных баз.)

Подмножество Ω называется плотным, если оно пересекается с любым открытым множеством (достаточно потребовать, чтобы оно пересекалось с любым интервалом).

Будем называть большим любое открытое всюду плотное множество. Малыми будем называть множества, которые можно покрыть счетным объединением дополнений к большим.

Нас будут интересовать открытые всюду плотные множества, которые имеют базу, принадлежащую M. Будем называть их большими над M. Малыми над M будем называть множества, которые можно покрыть объединением дополнений к большим над M множествам.

Пусть множество T бесконечно. Тогда примером большого множества является множество всех функций отличных от некоторой фиксированной функции f. Если функция f принадлежит M, то это множество большое над M. Малым над M является множество всех функций, принадлежащих M.

Определение 2. Функция g называется генерической над M, если g принадлежит всем большим над M множествам.

Теорема 9. *Генерические функции существуют. Более того, множество генерических функций всюду плотно.*

Доказательство. Докажем сначала существование. По предположению M счетно, а значит и множество больших над M множеств счетно. Перенумеруем их все $A_1, A_2, \ldots$. Построим последовательность вынуждающих условий $\alpha_1 \subset \alpha_2 \subset \ldots$ такую, что Ω_{p_i} включено в A_i для всех i. Это легко сделать по индукции пользуясь открытостью и плотностью A_i. Пересечение всех Ω_{p_i} непусто и любая функция из этого пересечения генерическая.

Для доказательства всюду плотности семейства генерических функций достаточно заметить, что мы можем начать цепь $\alpha_1 \subset \alpha_2 \subset \ldots$ с любого вынуждающего условия α_0. $\square$

Теорема 10. *Если g генерическая функция, то $M[g]$ является моделью ZFC, причем наименьшей из моделей, содержащей g и включающей M.*

Для доказательства этой теоремы нам понадобится понятие вынуждения.

2.2 Вынуждение

Множество $A \subset \Omega$ называется измеримым по Бэру, если существует открытое множество $B \subset \Omega$ такое, что симметрическая разность A и B мала. Мы говорим в этом случае, что B приближает A.

Множество $A \subset \Omega$ называется измеримым по Бэру над M, если существует открытое множество $B \subset \Omega$, имеющее базу в M и такое, что симметрическая разность A и B мала над M. Мы говорим в этом случае, что B приближает A над M.

Лемма 13. *Семейство измеримых по Бэру множеств замкнуто относительно счетных объединений и дополнения.*

Доказательство. Пусть $\mathcal{A}$ счетное семейство измеримых по Бэру множеств. Пользуясь аксиомой выбора, выберем для каждого из множеств $A \in \mathcal{A}$ приближающее его открытое множество $\tilde{A}$. Тогда симметрическая разность $\mathrm{Un}\, A$ и $\bigcap_{A\in\mathcal{A}} \tilde{A}$ покрывается объединением симметрических разностей множеств A и $\tilde{A}$, а значит мала над M.

Пусть A измеримо по Бэру и приближается множеством $\tilde{A}$, а B есть дополнение до A. Обозначим через C дополнение до $\tilde{A}$ и определим $\tilde{B}$, как внутренность C. Докажем, что симметрическая разность $\tilde{B}$ и B мала. Она покрывается объединением $B \triangle C$ и $C \triangle \tilde{B} = C \setminus \tilde{B}$. Первая симметрическая разность мала, поскольку совпадает с $A \triangle \tilde{A}$. Докажем малость второй разности. Более того, мы докажем, что дополнение к ней $\tilde{A} \cup \tilde{B}$ является большим множеством. Это множество открыто, как объединение двух открытых. Оно всюду плотно, поскольку если базовое множество Ω_p не пересекается с $\tilde{A}$, то оно включено в $\tilde{B}$. □

Аналогичная лемма справедлива и для измеримости над M.

Лемма 14. *Пусть имеется семейство $\mathcal{A}$ измеримых над M множеств такое, что некоторые базы множеств, приближающих элементы $\mathcal{A}$, образуют множество из M. Тогда объединение всех множеств из $\mathcal{A}$ измеримо над M.*

Дополнение любого измеримого над M множества измеримо над M.

Доказательство. Первое очевидно: если некоторые базы множеств, приближающих элементы $\mathcal{A}$, образуют множество $\mathcal{B} \in M$, то базой приближающего $\mathrm{Un}(\mathcal{A})$ множества будет $\mathrm{Un}(\mathcal{B})$.

Замкнутость относительно дополнения. Пусть множество $\tilde{A}$, приближающее множество A над M, имеет базу $C \in M$. Определим D, как семейство всех вынуждающих условий p таких, что Ω_p включено в $\tilde{B}$ (внутренность дополнения до $\tilde{A}$). Очевидно, что $D \cup C$ является базой $\tilde{A} \cup \tilde{B}$. Так же как в предыдущей лемме доказывается, что $\tilde{B}$ приближает дополнение к A над M. Осталось доказать, что D принадлежит M. Без ограничения общности мы можем считать, что если $p \in C$ и $q \supset p$, то $q \in C$ (замыкание относительно взятия продолжения не изменяет задаваемое множество и не выводит из M). Нетрудно убедиться, что при этом условии

$$D = \{p \mid (\forall q \supset p)\ q \notin C\},$$

следовательно D принадлежит M. □

Пусть формула φ имеет параметры $x_1, \dots, x_n$. Будем называть оцененной формулой выражение $\varphi(a_1, \dots, a_n)$, где a_i — произвольные элементы M. Для каждой оцененной формулы рассмотрим множество

$$\{g \mid M[g] \models \varphi(a_1[g], \dots, a_n[g])\},$$

которое мы будем обозначать через

$$[\varphi(a_1, \dots, a_n)].$$

Теорема 11. *Для любой оцененной формулы $\varphi(a_1, \dots, a_n)$ множество $[\varphi(a_1, \dots, a_n)]$ измеримо по Бэру над M. Более того, это верно равномерно по параметрам формулы. Точнее, найдется формула φ', у которой на один параметр больше и которая обладает следующим свойством. Для всех значений параметров $a_1, \dots, a_n \in M$ формулы φ множество тех $p \in P$, для которых*

$$M \models \varphi'(p, a_1, \dots, a_n)$$

является базой открытого множества, приближающего над M множество $[\varphi(a_1, \dots, a_n)]$.

Если в M истинно $\varphi'(p, a_1, \dots, a_n)$, то мы говорим, что p вынуждает $\varphi(a_1, \dots, a_n)$ и записываем это $p \Vdash \varphi(a_1, \dots, a_n)$.

Доказательство. Докажем сначала индукцией по длине формулы измеримость множества $[\varphi(a_1, \dots, a_n)]$. Можно считать, что формула φ не содержит кванторов всеобщности, импликации и конъюнкции.

База индукции: нам нужно доказать измеримость множеств вида $[a \in b]$, $[a = b]$, где $a, b \in M$. Докажем это индукцией по неупорядоченной паре $\{rk(a), rk(b)\}$. Утверждение $a[g] \in b[g]$ означает, что для некоторого $c \in_g b$ выполнено $a[g] = c[g]$. Для всех $c \in_g b$ к неупорядоченной паре $\{a, c\}$ можно применить индуктивное предположение и заключить измеримость множества $[a = c]$. Множество $[a \in b]$ получается из множеств $[a = c]$ и открытых множеств вида

$$\{g \mid c \in_g b\}$$

с помощью операций счетного объединения, дополнения, пересечения, и поэтому измеримо.

Утверждение $a[g] = b[g]$ означает, что не существует $c \in_g a$, для которого $c[g] \notin b[g]$, а также не существует $c \in_g b$, для которого $c[g] \notin a[g]$. Для всех $c \in_g a$ и $c \in_g b$ к неупорядоченным парам $\{a, c\}$, $\{b, c\}$ можно применить индуктивное предположение и заключить измеримость множеств $[c \in b]$ и $[c \in a]$. Множество $[a = b]$ получается из множеств $[c \in a]$ и $[c \in b]$ и открытых множеств вида

$$\{g \mid u \in_g v\}$$

с помощью операций счетного объединения, дополнения, пересечения, и поэтому измеримо.

Индуктивный переход: множество $[\varphi \vee \psi]$ есть объединение множеств $[\varphi], [\psi]$, множество $[\neg\varphi]$ есть дополнение множества $[\varphi]$, и множество $[\exists x \varphi(x)]$ есть объединение множеств $[\varphi(a)]$ по всем $a \in M$. Поэтому достаточно сослаться на лемму 13.

Для доказательства равномерной измеримости над M множеств вида $[\varphi]$ нам понадобится лемма 14, и более того, конструкция из ее доказательства. Формулу $p \Vdash \varphi(a_1, \ldots, a_n)$ можно строить разными способами. Например, годится такое рекурсивное определение $p \Vdash \varphi(a_1, \ldots, a_n)$:

$$\begin{aligned}
&p \Vdash \varphi \vee \psi \leftrightarrow (p \Vdash \varphi) \vee (p \Vdash \psi),\\
&p \Vdash \exists \varphi(x) \leftrightarrow (\exists a \in M)\ p \Vdash \varphi(a),\\
&p \Vdash \neg\varphi \leftrightarrow (\forall q \supset p)\ \neg(q \Vdash \varphi),\\
&p \Vdash a \in b \leftrightarrow (\exists c \in M)\ (\exists q \subset p)\ \langle q, c\rangle \in a,\ p \Vdash c = a,\\
&p \Vdash a = b \leftrightarrow p \Vdash \neg(a \not\subset b \vee b \not\subset a)\\
&p \Vdash b \not\subset a \leftrightarrow (\exists c \in M)\ (\exists q \subset p)\ \langle q, c\rangle \in b,\ p \Vdash \neg c \in a.
\end{aligned}$$

Формула $b \not\subset a$ в последних двух строчках носит вспомогательный характер, и нужна только для сокращения длинного определения формулы $p \Vdash a = b$.

Это определение примерно соответствует построению открытого множества, приближающего $[\varphi(a_1, \ldots, a_n)]$, примененного в доказательстве измеримости этого множества. Чтобы доказать его корректность, заметим, что в первых трех строчках уменьшается длина формулы, а в последних двух строчках (рассматриваемых как единое определение для $p \Vdash a \in b$) уменьшается неупорядоченная пара $\{rk(a), rk(b)\}$.

Нетрудно доказать трансфинитной индукцией (по длине формулы, а для атомарных формул $a \in b$ индукцией по паре $\{rk(a), rk(b)\}$) следующие два утверждения:
(1) если $p \Vdash \varphi$ и $q \supset p$, то $q \Vdash \varphi$;
(2) множество тех p, для которых в M истинно $p \Vdash \varphi$, является базой открытого множества, приближающего над M множество $[\varphi]$. □

Из определения вынуждения следует *основное свойство вынуждения*: для любой генерической функции g выполена эквивалентость

$$M[g] \models \varphi(a_1[g], \ldots, a_n[g]) \Leftrightarrow (\exists p \subset g)\ p \Vdash \varphi(a_1, \ldots, a_n).$$

Действительно, правая часть означает, что g принадлежит открытому множеству, приближающему над M множество $[\varphi(a_1, \ldots, a_n)]$. Поскольку функция g не принадлежит ни одному малому над M множеству, она не может попасть в симметрическую разность множества $[\varphi(a_1, \ldots, a_n)]$ и приближающего его множества.

2.3 Доказательство теоремы 10

Нам осталось доказать, что если g генерическая фунция, то в $M[g]$ истинны аксиомы объединения, степени, выделения и замены.

Вынуждение дает следующий мощный метод построения имен элементов из $M[g]$.

Лемма 15. *Пусть $a, b \in M$, а $\varphi(x, y)$ произвольная формула с параметрами x, y. Тогда множество*

$$D = \{c[g] \mid c \in a,\ M[g] \models \varphi(c[g], b[g])\}$$

принадлежит $M[g]$, причем имеет имя включенное в множество $P \times a$. То же самое справедливо для формул с любым количеством параметров.

Доказательство. Именем D является множество

$$d = \{\langle p, c\rangle \mid c \in a,\ p \Vdash \varphi(c[g], b[g])\}.$$

Действительно, d является именем множества

$$d[g] = \{c[g] \mid c \in a,\ (\exists p \subset g)\ p \Vdash \varphi(c, b)\},$$

которое совпадает с D по основному свойству вынуждения. $\square$

Этим методом нетрудно доказать аксиому *свертывания*. Пусть скажем нам нужно доказать аксиому

$$\forall u \forall y \exists z \forall x\ (x \in z \leftrightarrow x \in u \wedge \varphi(x, y)).$$

Иными словами, для любых $b, c \in M$ нам нужно найти имя для множества

$$D = \{a[g] \mid a \in M,\ M[g] \models a[g] \in c[g] \wedge \varphi(a[g], b[g])\}.$$

Будем называть проекцией c множество вторых компонент всех упорядоченных пар из c. Область изменения a здесь можно ограничить проекцией множества c, а потом применить лемму.

Точно так же доказывается аксиома объединения: нам нужно доказать, что множество

$$D = \{a[g] \mid a \in M,\ M[g] \models \exists x\ (a[g] \in x \wedge x \in b[g])\}$$

принадлежит $M[g]$. Область изменения a здесь можно ограничить второй проекцией второй проекции b и затем применить лемму.

Аксиома *степени*: нам нужно доказать, что для всех $b \in M$ множество $M[g]$ содержит множество

$$D = \{a[g] \mid a \in M,\ M[g] \models a[g] \subset b[g]\}.$$

На этот раз ограничить область изменения a позволяет следующая лемма (в доказательстве которой мы опять используем вынуждение).

Лемма 16. *Если $a[g] \subset b[g]$, то $a[g]$ имеет имя, включенное в множество $P \times$ (проекция b).*

Доказательство. Поскольку $a[g] \subset b[g]$, все элементы $a[g]$ принадлежат $b[g]$, а значит имеют имена, принадлежащие второй проекции b. Следовательно,

$$a[g] = \{c[g] \mid c \in (\text{проекция } b) \; c[g] \in a[g]\}.$$

По лемме 15 множество $a[g]$ имеет имя, включенное в $P \times (\text{проекция } b)$. $\square$

Осталось доказать аксиому *замены.* Докажем ее для формул $\varphi(x, y)$ с двумя параметрами (доказательство легко обобщается на случай любого числа параметров). Пусть дано $c \in M$ такое, что

$$M[g] \models (\forall x \in c[g])(\exists! y) \; \varphi(x, y).$$

Нам нужно доказать, что множество, состоящее из всех $b[g]$, для которых найдется $a \in M$ со свойством

$$M[g] \models a[g] \in c[g] \wedge \varphi(a[g], b[g]),$$

принадлежит $M[g]$. Для этого нам достаточно ограничить каким-то множеством из M область изменения b. Сначала ограничим область изменения a проекцией c. По основному свойству вынуждения

$$M[g] \models a[g] \in c[g] \wedge \varphi(a[g], b[g])$$

тогда и только тогда, когда некоторое $p \subset g$ вынуждает формулу

$$a \in c \wedge \varphi(a, b).$$

В M есть множество d с таким свойством: для всех a из проекции c и всех $p \in P$, если в M существует b такое, что $p \Vdash (a \in c \wedge \varphi(a, b))$, то такое b есть и в d. Действительно, для каждой пары a, p для которых такое b существует, рассмотрим наименьший ранг такого b. Выберем ординал α, больший всех ординалов, полученных таким образом, а затем возьмем в качестве d семейство всех множеств из M, ранг которых меньше α.

Докажем, что если a принадлежит проекции c и

$$M[g] \models a[g] \in c[g] \wedge \varphi(a[g], b[g]),$$

то $b[g]$ имеет имя в d. По основному свойству вынуждения некоторое $p \subset g$ вынуждает формулу $(a \in c \wedge \varphi(a, b))$, а значит найдется $b' \in d$, для которого $p \Vdash (a \in c \wedge \varphi(a, b'))$. Опять применяя основной принцип вынуждения, заключаем что

$$M[g] \models a[g] \in c[g] \wedge \varphi(a[g], b'[g]).$$

В силу единственности $b'[g] = b[g]$, что и требовалось доказать.

Итак, мы доказали, что для любой генерической функции g множество $M[g]$ является моделью ZF.

Лемма 17. *$M[g]$ включено в любую транзитивную модель ZF, содержащую g и включающую M.*

Доказательство. Пусть U — такая модель. Нетрудно проверить, что формула $x = a[g]$ с двумя параметрами a, x абсолютна для расширения $U \subset V$. Поэтому все множества вида $a[g]$ при $a \in U$ принадлежат U. В частности, это верно и для всех $a \in M$. □

Лемма 18. *В $M[g]$ истинна аксиома выбора.*

Доказательство. Как отмечалось, формула с $x = a[g]$ абсолютна для расширения $U \subset V$, где U — любая транзитивная модель ZF, содержащая g и включающая M. В частности, это верно и для $U = M[g]$.

Пусть $a[g]$ любое множество из $M[g]$. Достаточно доказать, что $M[g]$ содержит наложение некоторого ординала из M на $a[g]$. Напомним, что мы предполагаем, что в M истинна аксиома выбора, а значит в M имеется биекция f некоторого ординала α и проекции множества a. Формула $x = f(\beta)[g]$ (с параметрами β, x) абсолютна относительно расширения $M[g] \subset V$, следовательно, для каждого $\beta \in \alpha$ существует единственное $x \in a[g]$, для которого $M[g] \models x = f(\beta)[g]$. По аксиоме выделения в $M[g]$ есть наложение α на $a[g]$. □

3 Независимость аксиомы конструктивности от ZFC

Лемма 19. *Множества $M[g]$ и M имеют одинаковые ординалы.*

Доказательство. Прежде всего заметим, что поскольку M и $M[g]$ транзитивны, понятие ординала абсолютно для расширений $M \subset M[g] \subset V$.

Нам надо доказать, что $M[g]$ не содержит никаких ординалов из V, кроме тех, которые принадлежат M.

Вспомним, что ранг любого ординала равен ему самому. Поэтому нам достаточно доказать, что ранг любого множества из $M[g]$ принадлежит M.

Индукцией по α нетрудно установить, что для всех $a \in M$ из $a \in V_\alpha$ следует $a[g] \in V_\alpha$ (то есть, ранг $a[g]$ не превосходит ранга a). (Через V_α кумулятивную иерархию в V.)

Формула $x \in V_\alpha$ абсолютна для расширения $M \subset V$, что доказывается индукцией по α. Можно записать это равенством $V_\alpha \cap M = M_\alpha$, где M_α обозначает кумулятивную иерархию в M.

Поскольку M является моделью ZF, для всех a из M существует ординал $\alpha \in M$ такой, что $a \in M_\alpha \subset V_\alpha$, и следовательно $a[g] \in V_\alpha$. Таким образом, ранг любого множества из $M[g]$ принадлежит M. □

Теорема 12. *Если ZFC имеет модель, то и теория ZFC +* $(V \neq L)$ *имеет модель.*

Доказательство. По теореме 8 существует модель V теории ZFC, содержащая счетное транзитивное множество M, являющееся моделью ZFC. Возьмем в качестве множества T натуральный ряд из M, и рассмотрим любую генерическую над M функцию из T в $\{0, 1\}$. Мы утверждаем, что аксиома конструктивности ложна в $M[g]$.

Любое конструктивное в $M[g]$ множество принадлежит M. Действительно, M является транзитивным подмножеством $M[g]$, в M истинны все аксиомы ZF и M содержащит все ординалы из $M[g]$.

С другой стороны, g не принадлежит M, поскольку семейство всех функций из T в $\{0, 1\}$, принадлежащих M, мало. Таким образом, g не конструктивно в $M[g]$. □

4 Независимость континуум гипотезы от ZFC

Мы уже выяснили, что M и $M[g]$ имеют одни и те же ординалы. Для кардиналов это могло бы быть не так по следующей причине. Напомним, что понятие кардинала не абсолютно: может так случиться, что некоторый ординал является кардиналом в M, но не является таковым в $M[g]$, поскольку в $M[g] \setminus M$ имеется биекция между этим ординалом и некоторым меньшим. В V все бесконечные ординалы из M равномощны, поскольку все множество M счетно. Поэтому существование такой биекции в $M[g]$ не представляется невероятным. Тем не менее, M и $M[g]$ имеют одни и те же кардиналы.

Теорема 13. *Любой кардинал из M является кардиналом и в $M[g]$.*

Доказательство. Для конечных кардиналов и для $\aleph_0$ это очевидно. Пусть $\aleph > \aleph_0$ — бесконечный кардинал в M. Допустим, что некоторая функция $a[g]$ из $M[g]$ является наложением некоторого меньшего кардинала $\aleph'$ из M на $\aleph$.

Скажем, что ординал β есть возможное значение a на $\alpha \in \aleph'$, если некоторое вынуждающее условие вынуждает формулу $a(\hat{\alpha}) = \hat{\beta}$. Эта формула является сокращением для утверждения о том, что a функция, содержащая пару $\langle \hat{\alpha}, \hat{\beta} \rangle$. Напомним, что $\hat{\alpha}$ обозначает такое множество из M, которое является именем α для любой функции g.

Лемма 20. *Для любого ординала α множество возможных значений a на α счетно или конечно в M.*

Доказательство. Пусть β, γ — два разных возможных значения, и p, q — соотвествующие вынуждающие условия. Тогда p и q не согласованы (не имеют общего продолжения). Действительно, иначе существовала бы генерическая функция g', продолжающая, как p, так и q. В $M[g']$ тогда были бы истинны обе формулы $a[g'](\alpha) = \beta$ и $a[g'](\alpha) = \gamma$, что невозможно.

Поэтому нам достаточно доказать, что любое семейство $F \in M$ попарно несогласованных вынуждающих условий конечно или счетно в M. Расслоим F в соответствии с мощностями областей определения функций: к F_i отнесем все функции из F_i, область определения которых содержит не более i элементов.

Очевидно, что мощности F_0 и F_1 не превосходят единицы. Поэтому нам достаточно показать, что $|F_i| \leq 1 + ia_{i-1}$, где a_{i-1} обозначает наибольшую мощность семейства попарно несогласованных вынуждающих условий, определенных на не более, чем $(i-1)$-элементном множестве.

Выберем любую фунциию p_0 из F_i и обозначим ее область определения через D_0. Для каждой из оставшихся функций p из F_i найдется $x \in D_0$ для которого $p(x) \neq p_0(x)$. При фиксированном x таких функций не больше a_{i-1}, поскольку их сужения на $T \setminus \{x\}$ попарно не согласованы (на x они принимают одно и то же значение, поскольку возможных значений всего два). □

По основному свойству вынуждения для всех $\alpha \in \aleph'$ ординал $a[g](\alpha)$ принадлежит множеству возможных значений a на α. Поэтому множество значений фунции $a[g]$ включено в объединение по $\alpha \in \aleph'$ множеств возможных значений a на α, мощность которого в M не превосходит мощности $\aleph' \times \aleph_0$, что меньше $\aleph$. $\square$

Теорема 14. *Если теория ZFC имеет модель, то она имеет модель, в которой ложна континуум-гипотеза.*

Доказательство. Пусть V — любая модель теории ZFC. Допустим сначала, что у нас имеется счетное транзитивное множество M из V, являющееся моделью ZFC. Положим T равным $\aleph_2^M \times \aleph_0$, где $\aleph_2^M$ обозначает второй бесконечный кардинал в M (в M он является вторым несчетным кардиналом, а в V он счетен, и стало быть не является кардиналом). Рассмотрим произвольное генерическое расширение $M[g]$. Докажем, что в $M[g]$ существует не менее $\aleph_2^M$ подмножеств натурального ряда.

Такими подмножествами являются множества вида

$$W_\alpha[g] = \{n \mid g(\alpha, n) = 1\}.$$

Все они различны, поскольку для любых двух различных ординалов α и β из $\aleph_2^M$ множество тех функций $f \in \Omega$, для которых $W_\alpha[f] \neq W_\beta[f]$ является большим над M множеством.

Осталось заметить, что $\aleph_2^M$ является вторым несчетным кардиналом не только в M, но и в $M[g]$ по теореме 13.

От предположении о существовании счетной транзитивно модели ZFC можно избавиться точно так же, как в доказательстве теоремы 12. $\square$

5 Независимость аксиомы выбора от ZF

Теорема 15. *Если теория ZFC имеет модель, то и теория ZF + $\neg AC$ имеет модель.*

План доказательства этой теоремы таков. Как обычно предположим, что имеется модель V теории ZFC и в ней имеется счетное транзитивное множество M, являющееся моделью ZFC.

Положим $T = \omega \times \omega$, выберем генерическую фунцию g из T в $\{0, 1\}$ и построим генерическое расширение $G = M[g]$. Обозначим через W_i множество $\{n \in \omega \mid g(i, n) = 1\}$ и положим $W = \{W_i \mid i \in \omega\}$.

Затем рассмотрим подмножество H множества G, которое состоит из всех наследственно определимых над G множеств. Множество $u \in G$ называется определимым, если существует формула $\varphi(x, a_1, \ldots, a_n)$ с одним параметром x, где каждое из $a_1, \ldots, a_n$ — это либо ординал из G, либо W_i, либо W, такая, что

$$u = \{x \in G \mid G \models \varphi(x, a_1, \ldots, a_n)\}.$$

Множество $x \in G$ называется наследственно определимым, если оно определимо и все элементы его транзитивного замыкания определимы.

Мы докажем, что H является искомой моделью, при этом в качестве множества из H, которое нельзя вполне упорядочить, мы возьмем множество W. Его конечно можно вполне упорядочить в G, более того, оно счетно в G. Однако биекция $i \mapsto W_i$ не является определимой, поскольку g не является таковой.

5.1 Наследственно ординально определимые множества

Начнем с доказательства того, что H является моделью ZF.

Теорема 16. *Семейство всех наследственно определимых множеств является моделью ZF.*

Доказательство. По построению H транзитивно, поэтому выполнены аксиомы *регулярности* и *объемности*. Поскольку H еще и содержит все ординалы из G, в H выполнена также аксиома *бесконечности*.

Проверим аксиому *пары*: пусть наследственно определимые множества a и b определяются формулами $\varphi(x)$ и $\psi(x)$, соответственно. Надо доказать, что множество наследственно определимо. Все элементы транзитивного замыкания $\{a, b\}$ по условию определимы. Поэтому надо доказать только определимость самого этого множества.

Рассмотрим формулу $\varphi'(x) = \forall y(y \in x \leftrightarrow \varphi(y))$ и аналогично определим $\psi'(x)$. Тогда $\{a, b\}$ определяется формулой $\varphi'(x) \vee \psi'(x)$.

Точно также доказывается истинность в H аксиомы *объединения*: Пусть наследственно определимое множество a определяется формулой $\varphi(x)$. Транзитивное замыкания $\mathrm{Un}(a)$ включено в транзитивное замыкание a, поэтому достаточно доказать определимость самого множества $\mathrm{Un}(a)$. Оно определяется формулой $\exists y\ (\varphi(y) \wedge x \in y)$.

Для остальных аксиом нам понадобится следующая

Лемма 21. *Понятие наследственно определимого множества определимо в G формулой с параметром W.*

Доказательство. Очевидно достаточно построить формулу с параметром W, задающую понятие определимости. Для этого рассмотрим трехместный предикат истинности $U \models \varphi(z)$, переменными которого являются $U \in G$, формула φ из G и кортеж z элементов U. Его можно записать формулой $T(U, \varphi, z)$", которая истинна в G тогда и только тогда, когда $U \models \varphi(z)$.

Рассмотрим кумулятивную иерархию G_α в G. По первому принципу отражения для любой формулы $\varphi(x)$ с разрешенными параметрами (разрешенные параметры — это ординалы, множества W_i и W), найдутся сколь угодно большие ординалы α такие, что

$$G \models \varphi(x) \leftrightarrow G_\alpha \models \varphi(x)$$

для всех $x \in G_\alpha$. Поэтому без ограничения общности в качестве определяющих формул можно рассматривать формулы вида "$G_\alpha \models \varphi(x)$". Следовательно, определимость задается формулой "существует формула $\varphi(x, y_1, \ldots, y_n)$, ординал α и значения $a_1, \ldots, a_n$ переменных $y_1, \ldots, y_n$, каждое из которых является ординалом или принадлежит W или равно W, такие, что "$G_\alpha \models \varphi(y, a_1, \ldots, a_n)$" тогда и только тогда, когда $y \in x$". □

Теперь мы можем доказать истинность в H аксиомы *степени*. Пусть наследственно определимое множество a определяются формулой $\varphi(x)$. Нам нужно доказать наследственную определимость множества

$$B = \{b \in H \mid b \subset a\}$$

Транзитивное замыкание множества B включено в транзитивное замыкание a, поэтому достаточно доказать определимость самого B. Оно определяется формулой "x определимо и $(\forall y \in x)\ \varphi(y)$".

Аксиома *выделения*. Разберем для простоты случай формулы $\varphi(x)$ с одним параметром. Нам требуется доказать наследственную определимость множества

$$B = \{b \in a \mid H \models \varphi(b)\},$$

где a — некоторое наследственно определимое множество.

Все элементы транзитивного замыкания этого множества определимы, поэтому достаточно доказать определимость самого множества. Пусть $\psi(y)$ определяющая a формула. Тогда B определяется формулой $\varphi^H(x) \wedge \psi(x)$. Релятивизовать кванторы φ множеством H можно по лемме.

Аксиома *замены.* Разберем для простоты случай формулы $\varphi(x, y)$ с двумя параметрами. Нам требуется доказать наследственную определимость множества

$$B = \{b \in H \mid H \models (\exists x \in a)\varphi(x, b)\},$$

где a — некоторое наследственно определимое множество. Существование в G этого множества гарантируется тем, что для каждого $x \in a$ существует единственное наследственно определимое множество y, для которого $H \models \varphi(x, b)$.

Все элементы транзитивного замыкания этого множества определимы, поэтому достаточно доказать определимость самого множества. Пусть $\psi(x)$ определяющая a формула. Тогда B определяется формулой

$$y \in H \wedge \exists x\ (\psi(x) \wedge \varphi^H(x, y)).$$

Релятивизовать кванторы φ множеством H и записать утверждение $y \in H$ можно по лемме. $\square$

Для доказательства того, что аксиома выбора ложна в H, нам понадобятся следующие два приема.

5.2 Повторные генерические расширения

Пусть T произвольным образом разбито в объединение двух непустых множеств T_1, T_2, а g любая генерическая функция из T в $\{0, 1\}$. Обозначим через g_1 и g_2 ограничения g на T_1 и T_2. Через P_1 и P_2 будем обозначать множества конечных частичных функций из T_1 и T_2 в $\{0, 1\}$.

Лемма 22. *Функция g_1 является генерической над M, а функция g_2 является генерической над $N = M[g_1]$ и при этом $M[g] = N[g_2]$.*

Доказательство. Докажем генеричность g_1 над M. Пусть A открытое всюду плотное множество функций из T_1 в $\{0, 1\}$ с базой из M. Тогда множество

$$\{f : T \to \{0, 1\} \mid f_1 \in A\}$$

является открытым всюду плотным множеством функций из T в $\{0, 1\}$ с базой из M, а значит содержит g. Поэтому g_1 принадлежит A.

Докажем генеричность g_2 над $M[g_1]$. Пусть дано открытое всюду плотное множество X функций из T_2 в $\{0, 1\}$, имеющее базу x в $M[g_1]$. Нам нужно доказать, что g_2 принадлежит X.

Обозначим через $D(x)$ формулу, которая утверждает, что $x \subset P_1$ и открытое множество с базой x всюду плотно. Зафиксируем имя a множества x в $M[g_1]$ и рассмотрим открытое множество в Ω с базой

$$B = \{p \in P \mid p_1 \Vdash (D(a) \rightarrow \ \widehat{p_2} \in a)\}.$$

Докажем, что это множество всюду плотно. Пусть $q \in P$ произвольное вынуждающее условие. Найдем его конечное продолжение p, принадлежащее B. Для этого рассмотрим любое генерическое продолжение f функции q. Рассмотрим два случая.

1) Пусть в $M[f]$ выполнено $D(a[f_1])$. Тогда некоторое продолждение $r \in P_2$ функции q_2 принадлежит $a[f_1]$. Поэтому, некоторое вынуждающее условие $s \subset f$, $s \in P_1$, вынуждает формулу

$$D(a) \rightarrow \widehat{r} \in a.$$

Взяв в качестве p объединение r, s и q, мы получим условие из B, продолжающее q.

2) Пусть в $M[f_1]$ ложно $D(a[f_1])$. Тогда в $M[f_1]$ истинно утверждение

$$D(a[f_1]) \rightarrow \widehat{q_2} \in a[f_1].$$

По основному свойству вынуждения, оно вынуждается некоторым условием $r \subset f_1$, $r \in P_1$. Тогда условие $p = r \cup q$ принадлежит B.

Поскольку открытое множество с базой B всюду плотно, оно содержит g. Отсюда следует, что для некоторого $p \subset g$ в $M[g]$ истинно

$$D(a[g_1]) \rightarrow p_2 \in a[g_1].$$

По условию, в $M[g]$ истинно $D(a[g_1])$, а значит $p_2 \in a[g_1]$, что и требовалось доказать.

Осталось доказать, что $M[g] = (M[g_1])[g_2]$.

Чтобы доказать включение слева направо, достаточно проверить, что множество $(M[g_1])[g_2]$ включает M и содержит g. Первое следует из того, что оно включает $M[g_1]$, а значит и M. Второе — из того, что оно содержит функции g_1, g_2, а значит и функцию g, равную их объединению.

Чтобы доказать включение справа налево, достаточно проверить, что множество $M[g]$ включает $M[g_1]$ и содержит g_2. Первое следует из того, что оно включает M и содержит функцию g_1, как сужение g на T_1. Второе — из того, что g_2 есть ограничение g на T_2. $\square$

Задача. Докажите, что если g_1 генерична над M, а g_2 генерична над $M[g_1]$, то функция $g_1 \cup g_2$ генерична над M.

5.3 Формулы с именами, устойчивыми относительно перестановок

Пусть π любая перестановка множества ω, принадлежащая M. Для любой функции $f \in \Omega$ обозначим через πf функцию определенную как $\pi f(i,j) = f(\pi i, j)$. Очевидно, что свойство быть генерической функцией устойчиво относительно применения любой перестановки из M и при этом $M[f] = M[\pi f]$ для любой генерической функции $f : T \to \{0,1\}$.

Скажем, что множество $a \in M$ устойчиво относительно применения перестановок, если для любой конечной перестановки π и любой генерической f выполнено $a[f] = a[\pi f]$.

Лемма 23. *Пусть $\varphi(y_1, \dots, y_k)$ формула, а $a_1, \dots, a_k$ элементы M, устойчивые относительно перестановок. Тогда для любой генерической функции g в $M[g]$ выполнено $\varphi(a_1[g], \dots, a_k[g])$, тогда и только тогда, когда пустая функция вынуждает формулу $\neg\neg\varphi(a_1, \dots, a_k)$ (то есть, любое условие p имеет продолжение q, вынуждающее $\varphi(a_1, \dots, a_k)$).*

Доказательство. В одну сторону это очевидно: если пустая функция вынуждает формулу $\neg\neg\varphi(i, a_1, \dots, a_k]$, то для любой генерической функции g в $M[g]$ выполнено двойное отрицание формулы $\varphi(a_1[g], \dots, a_k[g])$, а значит и сама эта формула.

Докажем обратное: если в $M[g]$ выполнено $\varphi(a_1[g], \dots, a_k[g]$, то любое условие p имеет продолжение q, вынуждающее $\varphi(a_1, \dots, a_k)$. Фиксируем p и возьмем любое его генерическое продолжение f. Если в в $N[f]$ истинно $\varphi(a_1[f], \dots, a_k[f]$, то формула $\varphi(a_1, \dots, a_k)$ вынуждается некоторым $r \subset f$ и в качестве q можно взять объединение p и r.

Докажем теперь, что формула $\varphi(a_1[f],\dots,a_k[f]$, не может быть ложной в $M[f]$. Допустим, что она ложна, а значит ее отрицание вынуждается некоторым условием r. Пусть $s \subset g$ любое условие, вынуждающее $\varphi(a_1,\dots,a_k)$. Пусть π любая конечная перестановка такая, что $\pi^{-1}r$ и s имеют неперекающиеся области определения, а h любое генерическое продолжение объединения $\pi^{-1}r$ и p. Тогда с одной стороны в в $M[h]$ истинно $\varphi(i[h],a_1[h],\dots,a_k[h]$ (поскольку h продолжает s). С другой стороны, πh продолжает r, следовательно в $M[\pi h]$ истинно $\neg\varphi(i[\pi h],a_1[\pi h],\dots,a_k[\pi h]$. Осталось вспомнить, что $M[h]=M[\pi h]$ все имена $a_1,\dots,a_k$ устойчивы относительно перестановок из M, а значит в $M[h]$ истинно $\neg\varphi(a_1[h],\dots,a_k[h]$. □

5.4 Завершение доказательства теоремы 15

Теорема 17. *Аксиома выбора ложна в H.*

Доказательство. Нам нужно доказать, что ни для одного ординала α в H не существует наложения f на α. Допустим, противное. Тогда это наложение определимо в $M[g]$ некоторой формулой. Параметры этой формулы могут содержать лишь конечное число множеств W_i. Пусть n любое такое число, что все W_i, начиная с $i=n$, не являются ее параметрами. Тогда множество W_i определимо в $M[g]$ некоторой формулой, параметрами которой являются ординалы и множества $W, W_0,\dots,W_{n-1}$. Чтобы получить противоречие, нам надо доказать, что такой формулы нет.

Для этого мы представим генерическое расширение $M \subset M[g]$ как композицию двух генерических расширений $M \subset M[g_1] \subset (M[g_1])[g_2]$. А именно, представим T как объединение двух множеств $T_1 = \{\langle i,j\rangle \mid i < n,\ j\in\omega\}$ и $T_2 = T\setminus T_1$. Обозначим через g_1 и g_2 сужения генерической функции g на T_1 и T_2.

По лемме 22 g_1 является генерической над M функцией, а g_2 генерична над $N=M[g_1]$. Из последнего следует, что W_n не принадлежит N. Действительно, допустим, что $W_n = a[g_1]$. Множество всех функций $f : T_2 \to \{0,1\}$, для которых $\{i\in\omega \mid f(i,n)=1] \neq a[g_1]$ является открытым над M и при этом всюду плотным, поэтому содержит генерическую функцию g_2. Поэтому, чтобы получить противоречие, нам достаточно доказать, что $W_n \in N$.

А для этого мы применим лемму 23 к генерическому расширению $N \subset N[g_2]$. Пусть $\varphi(x,y_1,\dots,y_k)$ — формула, определяющая W_n в $G=$

$N[g_2]$ и пусть $i \in \omega$. Каждое из множества $i, y_1, \ldots, y_k$ является либо ординалом, либо принадлежит N, либо равно W. Все элементы N (в частности, все ординалы) очевидно имеют имена, устойчивые относительно любых перестановок множества $\{n, n+1, \ldots\}$. Любое естественно построенное имя множества W также является устойчивым относительно любых перестановок $\{n, n+1, \ldots\}$. По лемме 23 натуральное число i принадлежит W_n тогда и только тогда, когда пустая функция вынуждает формулу $\varphi(\hat{i}, a_1, \ldots, a_k)$, где $a_1, \ldots, a_k$ — устойчивые относительно перестановок имена $y_1, \ldots, y_k$. Поскольку вынуждение выразимо формулой, множество W_n принадлежит N по аксиоме выделения. $\square$