

МФТИ, ФИВТ, 2-ой семестр, 2009.
Краткий конспект лекций по курсу
Математическая логика и теория алгоритмов.
Д. Мусатов, А. Ромащенко.

Лекция 1, 18 февраля. Обсуждение: зачем нужно строгое определение алгоритма. Машины Тьюринга, машины Поста, машины Минского, алгорифмы Маркова.

Соответствующие варианты определения вычислимых функций $\{0, 1\}^* \rightarrow \{0, 1\}^*$.

Обсуждение (без строгих доказательств) эквивалентности определений.

Лекция 2, 25 февраля.

Диагональная конструкция, теорема о существовании невычислимых функций.

Разрешимые множества. Существование неразрешимых множеств.

Перечислимые множества (5 определений, их эквивалентность).

Лекция 3, 4 марта

Окончание доказательства эквивалентности 5 определений перечислимых множеств.

Замкнутость разрешимых множеств относительно операций объединения, пересечения и дополнения. Теорема Поста.

Теорема Райса–Успенского.

Теорема о существовании универсальной функции.

Лекция 4, 11 марта

Теоремы об универсальной функции и о главной нумерации.

Теорема Клини о рекурсии и её применение.

Формулировка теоремы Клини о рекурсии: Будем называть номера n и m эквивалентными (*обознач.* $n \equiv m$), если программы с номерами n и m в стандартной нумерации вычисляют одну и ту же функцию (другими словами, вычислимые функции φ_n и φ_m из главной универсальной нумерации совпадают). Пусть $g(x)$ – вычислимая и всюду определённая функция. Тогда найдётся такой номер n_0 , что числа n_0 и $g(n_0)$ эквивалентны.

Одно из доказательств: Шаг 1. Обозначим $f : n \mapsto \varphi_n(n)$ вычислимую (но не всюду определённую) “диагональную” функцию (она вычисляет значение n -ой вычислимой функции из главной нумерации на её собственном номере). Построим вычислимую и всюду определённую функцию f' такую, что:

Если $f(n)$ определено, то $f'(n)$ эквивалентно $f(n)$ (*)

Функция f' действует следующим образом. Получив вход n , она выдаёт в качестве результата номер такой программы:

1. получаем на вход x
2. моделируем работу n -ой программы на её собственном номере и вычисляем значение $k = \varphi_n(n)$. /* для некоторых n на этом шаге происходит заикливание */
3. моделируем работу k -ой программы из стандартной нумерации на входе x . Если не произошло заикливания, выдаём полученный результат.

Нетрудно проверить, что функция f' всюду определена, и удовлетворяет требованию (*).

Шаг 2. Рассмотрим вычислимое всюду определённое отображение

$$h(n) = g(f'(n))$$

Обозначим m номер программы, вычисляющей h . Далее, применим к этому номеру функцию f' :

$$m' = f'(m)$$

Далее мы увидим, что номер m' и является искомой неподвижной точкой для g .

Нам нужно доказать, что m' и $g(m')$ эквивалентны. В самом деле,

$$m' = f'(m) \equiv \varphi_m(m) = h(m) = g(f'(m)) = g(m')$$

(первое равенство следует из определения m' ; эквивалентность следует из свойства (*); следующее равенство есть всего лишь переписывание определения номера m ; следующее равенство – определение функции h ; последнее равенство следует из определения m'). Теорема доказана.

Лекции 5, 18 марта

Вычисления с оракулом, сводимость по Тьюрингу. Сводимость на примере множеств $K = \{n : \varphi_n(n) \text{ определено}\}$, $H = \{\langle n, m \rangle : \varphi_n(m) \text{ определено}\}$, $K = \{n : \varphi_n \text{ всюду определено}\}$.

Арифметическая иерархия множеств: классы Σ_n и Π_n , их простейшие свойства. Теорема об иерархии без доказательства.

Лекции 6, 25 марта

Определение представимости множества в языке арифметики.

Теорема 1: Всякое представимое в арифметике множество лежит в некотором Σ_n .

Теорема 2: Всякое множество из Σ_n или Π_n представимо в арифметике.

Основная Лемма: Существует такая арифметическая формула $Sec(a, j, b)$, что для всякой конечной последовательности битов $\pi = \pi_1 \dots \pi_N$ найдётся такое число a , что $Sec(a, j, 1)$ истинно если и только если $\pi_j = 1$.

Лекции 7, 1 апреля

Лемма о возможности переставлять местами ограниченного и неограниченного кванторов.

Определим последовательность релятивизованных проблем остановки: $H_0 = \emptyset$, $H_{n+1} = \{ \langle k, m \rangle : \phi_k^{H_n}(m) \text{ определено} \}$

Теорема об иерархии: (а) Σ_{n+1} перечислимо с оракулом H_n ; (б) Σ_{n+1} разрешимо с оракулом H_{n+1} ; (в) $H_{n+1} \in \Sigma_{n+1}$; (г) $\Sigma_{n+1} \neq \Sigma_n$.

Следствие: (а) Множество замкнутых истинных арифметических множеств не является перечислимым. (б) Множество замкнутых истинных арифметических множеств не принадлежит ни одному из классов Σ_n (теорема Тарского).

Лекции 8, 8 апреля

Системой аксиом будем называть любое *разрешимое* (конечное или бесконечное) множество формул языка 1-го порядка.

Пример – аксиомы Пеано для формальной арифметики:

1. $\forall x(Sx \neq 0)$
2. $\forall x\forall y(Sx = Sy \rightarrow x = y)$
3. $\forall x(x \neq 0 \rightarrow \exists y(x = Sy))$
4. $\forall x(x + 0 = x)$
5. $\forall x\forall y(x + Sy = S(x + y))$
6. $\forall x(x \cdot 0 = 0)$
7. $\forall x\forall y(x \cdot Sy = x \cdot y + x)$
8. $(A(0) \& (\forall x(A(x) \rightarrow A(Sx)))) \rightarrow \forall x A(x)$

Последняя аксиома – на самом деле бесконечная серия аксиом, для всех формул A , в которых есть свободная переменная x (и, быть может, какие-то другие).

Система аксиом противоречива, если из неё можно вывести одновременно некоторую формулу A и её отрицание $\neg A$.

Для любой системы аксиом множество выводимых формул (теорем) перечислимо.

1-ая теорема Гёделя о неполноте: Для любого корректного множества аксиом формальной арифметики существует истинное, но недоказуемое утверждение (*корректность* означает, что все аксиомы должны быть истинны в стандартной модели арифметики).

Определение: функция $f : \mathbb{N}^k \rightarrow \mathbb{N}$ называется представимой в теории PA , если существует такая формула $\Phi(x_1, \dots, x_k, y)$, что для всех a_1, \dots, a_k , если $f(a_1, \dots, a_k) = b$, то

1. $PA \vdash \Phi(\bar{a}_1, \dots, \bar{a}_k, \bar{b})$

$$2. PA \vdash \forall y(\Phi(\bar{a}_1, \dots, \bar{a}_k, y) \rightarrow y = \bar{b})$$

(\bar{m} , как всегда, обозначает терм $SS \dots S0$, т.е. m -кратное прибавление единицы к нулю).

Теорема о представимости в PA всех вычислимых функций (без доказательства).

Теорема о диагонализации: для любой формулы с одной свободной переменной $A(x)$ найдётся такая замкнутая формула B , что $PA \vdash B \leftrightarrow A(\text{номер формулы } B \text{ в алфавитном порядке})$ (доказательство на следующей лекции).

Следствие: новое доказательство теоремы Тарского о неарифметичности множества истинных арифметических формул: если бы нашлась такая $T(x)$, которая истинно строго на номерах истинных формул, то мы построили бы такую B , что $PA \vdash B \leftrightarrow \neg T(\text{номер } B)$, что есть абсурд.

Лекции 9, 15 апреля

Доказательство теоремы о диагонализации. Теорема Лёба. Вторая теорема Гёделя о неполноте.

Лекции 10, 22 апреля

Краткий обзор изученных подходов к понятию алгоритма: машины Тьюринга, Поста, Минского, алгоритмы Маркова; представимость вычислимых функций в PA.

λ -обозначения функций в примерах. Сведение функций нескольких переменных к функциям одной переменной (например, функция двух переменных $F(x, y)$ представляется как отображение из x во множество функций одной переменной $G(y)$).

Формальное **определение** λ -терма: переменный и константы суть термы если A и B λ -термы, то (AB) тоже λ -терм; если A λ -терм, а $a = x$ переменная, то $(\lambda x.A)$ тоже терм.

Свободные и связанные (квантором λ) переменные определяются обычным образом. Замкнутые (без свободных переменных) λ -термы называются *комбинаторами*.

Соглашение о расстановке скобок: мы обычно опускаем внешнюю пару скобок формулы; пропущенные скобки внутри терма по умолчанию восстанавливаются с группированием 'справа'; например, $abcd$ обозначает на самом деле $((ab)c)d$; наконец, $\lambda xyz.F$ обозначает $\lambda x.(\lambda y.(\lambda z.F))$.

α -конверсия: переименование в терме одной из связанных квантором переменных (в определении нужно проявить аккуратность — переименование связанной x в y законно, если вхождение переменной нигде не попадает в область действия уже имеющихся кванторов λy по этой же самой переменной). В принципе, можно было бы потребовать, чтобы новая переменная вообще нигде не встречалась в старой записи формулы.

β -редукция: $(\lambda x.A)B$ превращается в $A(B/x)$ (B подставляется вместо всех свободных вхождений x). Снова нужно проявить аккуратность; потребуем, чтобы в A и B не встречались одинаковые переменные. Редукцию

можно применять к подформуле: если M редуцируется в M' , то MN редуцируется в $M'N$ и NM редуцируется в NM' .

В типичной ситуации мы будем пользоваться α конверсией, чтобы стало возможно применить β -редукцию.

λ -терм называется нормальной формой, если даже после переименования переменных (каких-либо α -преобразований), к нему нельзя применить β -редукцию.

Мы хотели бы приводить λ -термы к нормальной форме. Но есть несколько плохих новостей:

Пример 1: λ -терм $(\lambda x.xx)(\lambda x.xx)$ не приводится к нормальной форме.

Пример 2: λ -терм $(\lambda x.xxx)(\lambda x.xxx)$ не просто не приводится к нормальной форме; β -редукции только увеличивают его длину.

Пример 3: λ -терм $(\lambda xy.y)((\lambda x.xxx)(\lambda x.xxx))$ имеет нормальную форму $\lambda y.y$. Однако, если 'неудачно' применять β -редукции, размер терма неограниченно возрастает.

Определение λ -термы называются равными, если один переводится в другой цепочкой преобразований, каждое из которых есть либо α -конверсия, либо β -редукция, либо обратное к β -редукции преобразование.

Хорошая новость:

Теорема Чёрча–Россера: Если λ -теоремы A и B равны, то существует такой λ -терм C , что и A , и B можно редуцировать в C последовательностью α -конверсий и β -редукций. (Без доказательства)

Следствие: Если λ -терм редуцируется к нормальной форме, то эта нормальная форма единственна (с точностью до переименования переменных с помощью α -конверсий).

Лекции 11, 29 апреля

Комбинаторы **True** = $\lambda xy.x$, **False** = $\lambda xy.y$, **and** = $\lambda xy.(xy \text{ False})$, **or** = $\lambda xy.(x \text{ True } y)$.
Простейшие приёмы программирования в λ -исчислении: конструкция if-then-else.

Кодирование пары, операции с ними: пара $\langle A, B \rangle$ кодируется λ -термом $\lambda f.fAB$; комбинатор составления пары: **Pair** = $\lambda xyf.fxy$; комбинаторы извлечения элементов из пары: **Left** = $\lambda p.(p \text{ True})$ и **Right** = $\lambda p.(p \text{ False})$.

Нумералы Чёрча и комбинаторы прибавления единицы, сложения, умножения. комбинатор **DEC** вычитание единицы (трюк 'зуба мудрости' Клини).

Лекции 12, 6 мая

Теорема о неподвижной точке, комбинатор Y . Рекурсивное программирование в λ -исчислении. Вычисление функции $n!$; вычисление n -ого числа Фибоначчи.

Работа со списком (в виде упражнения).

Множества: Элементарные операции. Представление упорядоченной пары по Куратовскому. Декартово произведение множеств; отношения и функции. Равномощность множеств; отношение 'мощность A не больше мощности B '.

Лекции 13, 13 мая

Формулировка теоремы Кантора–Бернштейна (доказательство на семинарах). Теорема Кантора (мощность $\mathcal{P}(A)$ больше мощности A).

Три определения фундированного (частично упорядоченного) множества, доказательство их эквивалентности.

Определение вполне упорядоченного множества, примеры.

Операции сложения и умножения вполне упорядоченных множеств.

Лемма об определении функции по трансфинитной рекурсии.

Лекции 14, 20 мая

Аксиома выбора: Пусть S — некоторое семейство непустых множеств, и U — объединение всех этих множеств. Существует функция $\varphi : S \rightarrow U$ такая, что $\varphi(A) \in A$ для любого множества $A \in S$.

Интуитивный смысл аксиомы выбора таков: если есть какое-то семейство S (конечное или бесконечное) непустых множеств, то из каждого из этих множеств можно как-то выбрать по одному элементу. Формально мы говорим, что существует некоторое “правило”, которое каждому множеству из семейства S сопоставляет элемент этого множества. Это “правило” и есть функция φ в нашей формулировке аксиомы выбора.

Для некоторых семейств множеств S функцию φ можно описать явно. Например, пусть S — некоторое семейство множеств целых чисел (для каждого $A \in S$ имеем $A \subseteq \mathbb{N}$). Тогда можно определить φ как

$$\varphi(A) = \min\{a \in A\}$$

(из каждого множества мы выбираем минимальный элемент). Однако если S — семейство множеств вещественных чисел, то уже не ясно, как именно явно описать выбор элемента в каждом множестве. В общем случае (для произвольного семейства множеств произвольной природы) отображение φ не удаётся определить “конструктивно”.

Аксиома выбора является основным ингредиентом теоремы Цермело: всякое множество может быть вполне упорядочено.

Теорема (Цермело). Для всякого множества X существует такое отношение $<$ (на $X \times X$), что $(X, <)$ является вполне упорядоченным множеством.

Доказательство: В качестве семейства множеств S рассмотрим множества всех непустых подмножеств X . Согласно аксиоме выбора существует такое отображение $\varphi : S \rightarrow X$, что для любого $A \in S$ (т.е., для любого непустого подмножества $A \subseteq X$) $\varphi(A) \in A$.

В дальнейшем рассуждении нам будет удобно рассматривать следующую функцию ψ , которая определена на всех подмножествах X , кроме самого X :

$$\psi(A) = \varphi(X \setminus A)$$

Таким образом, отображение ψ сопоставляет каждому множеству $A \subset X$ (включая $A = \emptyset$) некоторый элемент $a \in X$ не принадлежащий A .

Теперь мы будем строить на X порядок, превращающий его во вполне упорядоченное множество. Это значит, что мы хотим “занумеровать” элементы X , т.е., представить его в виде $X = \{x_0, x_1, x_2, \dots\}$ (и положить $x_0 < x_1 < x_2 < \dots$).

Основная идея доказательства выглядит просто: мы положим

- $x_0 = \psi(\emptyset)$,
- $x_1 = \psi(\{x_0\})$ (по определению ψ элемент x_1 не может совпадать с x_0),
- $x_2 = \psi(\{x_0, x_1\})$ (по определению ψ элемент x_2 не может совпадать с x_0 или x_1),
- $x_3 = \psi(\{x_0, x_1, x_2\})$ (по определению ψ элемент x_3 будет отличаться от x_0, x_1 и x_2),

и так далее, пока не будут исчерпаны все элементы X . Таким образом, множестве X будет вполне упорядоченно. Конечно, в строгом доказательстве мы должны объяснить, что здесь означают слова *и так далее*. Это потребует некоторой подготовки.

Определение. Пусть $A \subset X$, и на множестве A есть некоторый порядок $<_A$ такой, что $(A, <_A)$ является вполне упорядоченным множеством. Будем говорить, что $(A, <_A)$ является *правильным* (для выбранного нами ψ), если для любого $a \in A$

$$a = \psi(\{b \in B : b < a\}).$$

Например, множество $\{x_0, x_1, x_2, x_3\}$, определённое выше, с порядком $x_0 < x_1 < x_2 < x_3$ является правильным вполне упорядоченным множеством.

Лемма. Если вполне упорядоченные множества $(A, <_A)$ и $(B, <_B)$ правильны, то одно множество является подмножеством другого, и на общих элементах A и B порядки $<_A$ и $<_B$ совпадают. Более того, одно из этих множеств является начальным отрезком другого.

Доказательство леммы:

На лекции мы доказали, что любые два вполне упорядоченные множества сравнимы между собой: одно из них изоморфно начальному отрезку другого. Пусть для определённости $(A, <_A)$ изоморфно начальному отрезку $(B, <_B)$. Обозначим этот изоморфизм f . Таким образом, существует такое отображение

$$f : A \rightarrow B,$$

что для всяких $a_1, a_2 \in A$, если $a_1 <_A a_2$, то $f(a_1) <_B f(a_2)$, и образ функции f является начальным отрезком в $(B, <_B)$. Для доказательства леммы достаточно доказать, что функция f является тождественной на своей области определения, т.е., для всякого $a \in A$ выполнено $f(a) = a$.

Пусть $f(a) = a$ выполнено не для всех a . Поскольку множество $(A, <_A)$ вполне упорядоченно, найдётся минимальный (в A) элемент x такой, что $f(x) \neq x$. Тогда множество

$$Z = \{a \in A : a <_A x\}$$

является начальным отрезком одновременно и в $(A, <_A)$, и в $(B, <_B)$.

Поскольку $(A, <_A)$ правильное, имеем $x = \psi(Z)$. Далее, обозначим x' минимальный элемент в $(B, <_B)$, больший всех элементов из Z . Поскольку $(B, <_B)$ тоже правильное, получаем $x' = \psi(Z)$. Таким образом, точки x и x' совпадают.

Из определения f следует, что минимальный элемент, больший Z в $(A, <_A)$, должен отобразиться в минимальный элемент, больший образа Z в $(B, <_B)$. Это значит, что $x' = f(x)$.

Мы получили противоречие с тем, что $f(x) \neq x$. Лемма доказана.

Рассмотрим семейство всех правильных вполне упорядоченных $(A, <_A)$. Доказанная лемма говорит, что порядки на всех этих вполне упорядоченных множествах согласованы друг с другом: порядок на одном множестве продолжает порядок на другом. Рассмотрим объединение всех этих множеств и назовём его D . На этом множестве можно ввести естественный линейный порядок: для всяких $x, y \in D$ мы считаем, что $x <_D y$, если x, y принадлежат некоторому правильному $(A, <_A)$, и $x <_A y$.

Контрольный вопрос: Почему для любых $x, y \in D$ найдётся такое правильное множество $(A, <_A)$, которое содержит сразу оба элемента x, y ?

Полученное множество $(D, <_D)$ является вполне упорядоченным. В самом деле, пусть в D есть бесконечная убывающая цепь $x_1 > x_2 > x_3 > \dots$. Элемент x_1 должен лежать в некотором правильном $(A, <_A)$. Но тогда и все меньшие элементы x_2, x_3, \dots тоже лежат в A , что противоречит тому, что $(A, <_A)$ вполне упорядоченное.

Покажем, что множество $(D, <_D)$ само является правильным. Для всякого $x \in D$ есть некоторое правильное $(A, <_A)$, которое содержит x . Тогда всё множество $\{y \in D : y <_D x\}$ содержится в A , и совпадает с $\{y \in D : y <_A x\}$. Из правильности $(A, <_A)$ следует, что $x = \psi(\{y \in D : y <_D x\})$, что и означает правильность $(D, <_D)$.

Нам остаётся показать, что $D = X$. Пусть это не так, пусть не все элементы X вошли в D . Тогда к D можно применить ψ . Назовём $d = \psi(D)$. Если добавить к D элемент d и объявить его большим всех остальных элементов D , мы получим некоторое правильное множество. И это правильное множество не является подмножеством D , что противоречит построению D .

Таким образом, мы получили вполне упорядоченное множество, носитель которого совпадает со всем X . Теорема доказана.

Следствие теоремы Цермело: мощности любых двух множеств сравнимы.

Теорема. Любое бесконечное множество A равномощно своему квадрату A^2 .

Доказательство: Введём на A некоторый полный порядок (это возможно по теореме Цермело). Нам будет удобно считать, что в полученном упорядоченном множестве (A, \leq) есть максимальный элемент (если такого элемента нет, добавим его искусственно; добавление одной точки не изменить мощности бесконечного множества).

Обозначим α_0 минимальный элемент A такой, что начальный отрезок $[0, \alpha_0)$ равномошен A . Теперь нам нужно доказать, что $[0, \alpha_0)$ равномощно $[0, \alpha_0) \times [0, \alpha_0)$.

Прежде всего введем полный порядок на квадрате $A \times A$. Для $(a, b), (a', b') \in A \times A$ будем считать, что (a, b) меньше (a', b') , если

- либо $\max\{a, b\} < \max\{a', b'\}$
- либо $a = \max\{a, b\} = a' = \max\{a', b'\}$ и $b < b'$
- либо $a = \max\{a, b\} = b' = \max\{a', b'\}$ и $a' < b'$
- либо $b = \max\{a, b\} = b' = \max\{a', b'\}$ и $a < a'$

Этот порядок легко представить себе наглядно. Разобьём $A \times A$ на ‘уголки’, состоящие из пары отрезков (‘вертикального’ и ‘горизонтального’):

$$\text{Уголок}_c = \{(x, c) : x \leq c\} \cup \{(c, x) : x \leq c\}$$

Пары (a, b) мы упорядочиваем так. Если (a, b) попадает в Уголок с меньшим значением c , нежели (a', b') , то считаем, что $(a, b) < (a', b')$. Если обе пары попадают в один и тот же уголок, то смотрим, лежат ли пары на вертикальной или горизонтальной линии; все точки вертикальной линии считаются меньше всех точек горизонтальной линии. А внутри вертикальной (соответственно, горизонтальной) линии точки упорядочены снизу вверх (соответственно, слева направо).

Нетрудно понять, что введённый является полным (проверьте!).

Теперь определим функцию, которая будет задавать биекцию между $[0, \alpha_0)$ и $[0, \alpha_0) \times [0, \alpha_0)$. Определим функцию $\varphi : [0, \alpha_0) \rightarrow A \times A$ рекурсивно:

$$\varphi(a) = \min\{(b, c) \in A \times A : (b, c) \text{ не встречалось среди } \varphi(a') \text{ для } a' < a\}$$

Лемма о трансфинитной рекурсии говорит, что такая функция φ существует.

Лемма 1. Образ $[0, \alpha_0)$ под действием φ лежит внутри $[0, \alpha_0) \times [0, \alpha_0)$.

Доказательство: Пусть образ $[0, \alpha_0)$ под действием φ покрывает больше, чем квадрат $[0, \alpha_0) \times [0, \alpha_0)$. Возьмем минимальное β ($\beta < \alpha_0$) такое, что среди φ -образов $[0, \beta)$ содержится весь квадрат $[0, \alpha_0) \times [0, \alpha_0)$. Заметим, что ‘диагональ’ этого квадрата (т.е. пары (x, x) для $x < \alpha_0$) равномощна $[0, \alpha_0)$. Получается, что $[0, \alpha_0)$ равномощно подмножеству $[0, \beta)$. Но это противоречит тому, что $[0, \alpha_0)$ – самый первый из начальных отрезков, равномощный всему A . Лемма доказана.

Определение. Будем называть $\beta \in A$ *кардинальным*, если ни для какого $\gamma < \beta$ начальные отрезки $[0, \beta)$ и $[0, \gamma)$ равномощны.

В частности, по определению, α_0 является кардинальным. Заметим, что только что доказанную лемму можно переформулировать в несколько более сильной форме:

Лемма 1'. Для каждого кардинального $\beta \in A$ образ $[0, \beta)$ под действием φ лежит внутри $[0, \beta) \times [0, \beta)$.

Доказательство: Годится рассуждение из Леммы 1 – в доказательстве мы не использовали никаких других свойств α_0 кроме кардинальности.

Лемма 2. Для каждого кардинального $\beta \in A$ образ $[0, \beta)$ под действием φ содержит $[0, \beta) \times [0, \beta)$.

Вместе с Леммой 1' это означает, что φ осуществляет биекцию между $[0, \beta)$ и $[0, \beta) \times [0, \beta)$

Доказательство: Предположим, что утверждение леммы неверно, и для некоторых кардинальных β отображение φ переводит $[0, \beta)$ в собственное подмножество $[0, \beta) \times [0, \beta)$. Пусть β_0 – минимальный элемент A с этим свойством.

Прежде всего заметим, что если $[0, \beta)$ счётно (а существует ровно одно β , для которого $[0, \beta)$ счётно – это первое β , у которого есть бесконечно много предшественников), то и $[0, \beta) \times [0, \beta)$ тоже счётно. Действительно, наша конструкция отображения φ для этого β всего лишь повторит стандартное доказательство равномощности \mathbb{N} и $\mathbb{N} \times \mathbb{N}$.

Итак, β_0 должно быть несчётным. Обозначим γ минимальный элемент, для которого $[0, \gamma) \times [0, \gamma)$ содержит целиком φ -образ $[0, \beta_0)$. По предположению $\gamma < \beta_0$. Таким образом, для $[0, \gamma)$ утверждение леммы не нарушается. Это значит, $[0, \gamma)$ равномошно $[0, \gamma) \times [0, \gamma)$ (β_0 является минимальной кардинальной точкой, для которой это свойство нарушено!). Объединяя эти факты, мы заключаем, что $[0, \beta_0)$ имеет мощность не больше, чем $[0, \gamma)$. Но это противоречит кардинальности β_0 . Лемма доказана.

Лемма 1 вместе с Леммой 2 показывают, что заданное отображение φ является биекцией между $[0, \alpha_0)$ и $[0, \alpha_0) \times [0, \alpha_0)$. Теорема доказана.