Дискретная математика. Модуль 3. Лекция 4

Лекторий ПМИ ФКН 2015-2016
Гринберг Вадим
Жижин Пётр
Пузырев Дмитрий

1 февраля 2016

1 Равномощность некоторых множеств

Множество двоичных слов. Множество пар натуральных чисел. Множество конечных последовательностей натуральных чисел

Рассмотрим следующие множества:

- $\{0, 1\}^*$ – множество двоичных слов.
- $\mathbb{N}$ – множество натуральных чисел (целые положительные и 0).
- $\mathbb{N} \times \mathbb{N}$ – множество пар натуральных чисел.
- $\mathbb{N}^*$ – множество конечных последовательностей натуральных чисел.

Докажем, что между ними есть эффективная биекция (то есть задаваемая простым алгоритмом).

Утверждение: $\{0, 1\}^* \sim \mathbb{N}$.

Доказательство. Рассмотрим такую функцию $f : W \to \overline{1W_2} - 1$, действующую из множества двоичных чисел в множество чисел, полученных путём вычитания единицы из значения двоичной записи исходного числа с приписанной вначале единицей. Тогда мы сопоставим каждому двоичному числу некоторое натуральное.

- $\{\ \} \to \overline{1_2} - 1 = 0$
- $0 \to \overline{10_2} - 1 = 1$
- $1 \to \overline{11_2} - 1 = 2$

Докажем, что это отображение – биекция.

Инъективность

Пусть у двух двоичных слов совпали образы, то есть им соответствует одно и то же натуральное число. Прибавим к этому числу единицу, получив тем самым число вида $\overline{1W_2}$. Но тогда по числу W_2 мы однозначно восстановим исходное слово, следовательно, изначальные двоичные слова равны.

Сюръективность

Возьмём любое число $P \in Z_+$, тогда P представимо в виде $\overline{1W_2}$ для некоторого W. У получившегося числа $\overline{1W_2}$ старшая цифра обязательно единица, тогда само число W есть единственный прообраз числа $P = \overline{1W_2}$ по построению.

Q.E.D.

Утверждение: $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$.

Доказательство. Есть 2 варианта построить биекцию между этими двумя множествами: первый – диагональный метод, рассмотренный ранее. Тогда: $(x, y) \to \binom{x+y-1}{2} + y$.

Рассмотрим второй вариант:

Построим биекцию $\mathbb{N}\times\mathbb{N} \to \mathbb{Z}_+$, а так как $\mathbb{Z}_+ \sim \mathbb{N}$, то мы тем самым докажем треубемое.

Пусть $f : (x, y) \to 2^x(2y + 1)$ – функция из множества пар в множество целых чисел, представленных в следующем виде. Покажем, что это – биекция.

Сюръективность

По Основной Теореме Арифметики, любое целое положительное число представимо в виде произведения степеней его простых множителей:

$\mathbb{Z}_+ = 2^{\alpha_2} \cdot 3^{\alpha_3} \cdot \ldots \cdot p^{\alpha_p} \Rightarrow$ вынесем степень двойки. Оставшееся число $3^{\alpha_3} \cdot \ldots \cdot p^{\alpha_p}$ – нечётное, значит, представимо в виде $2y + 1$ для некоего числа y.

Тогда этому значению нашей функции будет соответствовать пара чисел α_2 и y: $f(\alpha_2, y) = 2^{\alpha_2}(2y + 1) = z$, где $z \in \mathbb{Z}_+$.

Следовательно, для любой пары чисел (x, y) существует число вида $2^x(2y + 1)$.

Инъективность

По Основной Теореме Арифметики разложение целого положительного числа является единственным.

Отсюда следует, что разложение вида $\mathbb{Z}_+ = 2^{\alpha_2}\cdot3^{\alpha_3}\cdot\ldots\cdot p^{\alpha_p}$, определяется единственным образом $\Rightarrow$ соответствующее этому разложению число $2^x(2y+1)$ определяется единственным образом $\Rightarrow$ любой паре (x, y) будет соответствовать только одно число вида $2^x(2y+1)$ и инъективность выполнена. **Q.E.D.**

Утверждение: $\mathbb{N}^* \sim \mathbb{N}$.

Доказательство. Построим биекцию $\mathbb{N}^* \to \mathbb{Z}_+$, а так как $\mathbb{Z}_+ \sim \mathbb{N}$, то мы тем самым докажем треубемое.

Пусть $f : (x_1, x_2, \ldots, x_n) \to p_1^{x_1} \cdot p_2^{x_2} \cdot \ldots \cdot p_n^{x_n+1}$ – функция из множества последовательностей натуральных чисел в целые положительные числа, представленные в виде произведения степеней некоторых различных простых чисел. Покажем, что это – биекция.

Инъективность

Предположим, что две последовательности задают одно и то же число. Тогда, выписывая показатели степеней числа, восстанавливаем две исходные последовательности. По ОТА любое натуральное число однозначно представимо в виде произведения степеней простых сомножителей, значит, получившиеся последовательности равны.

Здесь же приведём ответ, почему степень числа p_n равна $x_n + 1$. Если бы показатель степени был равен x_n, то, к примеру, последовательности $\{1, 0\}$ и $\{1, 0, 0\}$ задавали бы одно и то же число: $2^1 \cdot 3^0 = 2^1 \cdot 3^0 \cdot 4^0$ – инъективность бы не соблюдалась.

Сюръективность

Основная Теорема Арифметики гарантирует существование для любого натурального числа разложения в виде произведения степеней простых сомножитилей. Значит, любому набору $f : (x_1, x_2, \ldots, x_n)$ можно сопоставить такое разложение, поэтому сюръекция установлена.

Q.E.D.

Множество всех подмножеств $\mathbb{N}$. Множество последовательностей натуральных чисел. Множество действительных чисел

Рассмотрим следующие множества:

- $\Phi(\mathbb{N})$ – множество всех подмножеств $\mathbb{N}$.

- $2^{\mathbb{N}}$ – множество последовательностей натуральных чисел.

- $\mathbb{R}$ – множество действительных чисел.

Определим действительные числа следующим образом: сопоставим каждому $x \in \mathbb{R}$ двоичное число: $\pm\underbrace{10110\ldots1011}_{\text{целая часть}}.\overbrace{110001\ldots00110}^{\text{дробная часть}}$. Считаем известным, что ряд из каких-то степеней двоек сходится, причём запрещаем в числах данного вида "хвосты из единиц".

Утверждение: $\Phi(\mathbb{N}) \sim 2^{\mathbb{N}}$.

Доказательство. Введём функцию $f : \mathbb{N} \to \chi(x)$ – индикаторная функция $= \begin{cases} 1, & x \in \mathbb{N} \\ 0, & x \notin \mathbb{N} \end{cases}$

То есть, для каждого подмножества множества $\phi(\mathbb{N})$ выписываем в ряд все натуральные числа, затем записываем для каждого натурального числа 1, если оно входит в это подмножество, и 0 иначе. Покажем, что это – биекция.

Инъективность

Пусть у двух элементов $\mathbb{N}$ совпали образы. Тогда возьмём такое подмножество $\mathbb{N}'$, в котором значение $f(\mathbb{N}') = 1$. Но тогда для каких-то $x_i,\ x_j \in f(\mathbb{N}') \mid x_i \neq x_j$ либо $x_i = 1,\ x_j = 0$, либо $x_i = 0,\ x_j = 1$. Следовательно, образы у этих двух элементов различны.

Сюръективность

Берём множество $\chi(x)$ и построим по нему элементы последовательности. Пусть мы получили 2 разных последовательности из одного двоичного числа. Но это означает, что в каком-то разряде двоичного числа не совпали цифры (в одном 0, в другом 1). Но тогда по построению это 2 разных числа.

Q.E.D.

Утверждение: $\mathbb{R} \sim 2^{\mathbb{N}}$.

Доказательство. Из курса математического анализа был известнен факт, что $\mathbb{R} \sim (0, 1)$. Пусть X – множество последовательностей из 0 и 1 без хвостов из единиц. Тогда по определению существует биекция $X \leftrightarrow [0, 1)$.

По определению $\mathbb{R}$: $[0, 1) \sim \pm 101\ldots001.1100\ldots01110$, тогда $X = 2^{\mathbb{N}} \backslash Y$, где Y – последовательность нулей и единиц с одиними единицами в конце.

Из семинарских занятий нам известна теорема: если множество A – бесконечно, множество B – счётно, то $A \cup B \sim A$.

Докажем, что множество Y счётно. Пусть у нас есть какое-то число с одними единицами в конце: $w_2.1100110111111$ (w_2 – целая часть числа). Если его инвертировать, то после точки получим двоичное число с бесконечным числом нулей в конце, единиц же будет счётное количество: $w_2.0011001000000$. Значит, эта новая последовательность нулей и единиц представляет какое-то натуральное число. Таким образом, мы построили биекцию $Y \leftrightarrow N$, значит по определению Y счётно.

Но тогда по теореме выше $2^{\mathbb{N}} = X \cup Y \sim X$, а так как $X \sim [0, 1)$, то $2^{\mathbb{N}} \sim [0, 1)$.

Очевидно, что множество $[0, 1] \sim [0, 1)$ – то же множество без одной точки. Но тогда аналогично $[0, 1) \sim (0, 1) \sim \mathbb{R}$.

Q.E.D.

Определение: Вышеперечисленные множества принято называть *континуальными.* Будем говорить, что множество X имеет мощность континуум, если $X \sim \mathbb{R}$.

Теорема Кантора для натуральных чисел. Полная теорема Кантора. Теорема Кантора-Бернштейна

Теорема Кантора. $\mathbb{N} \nsim \mathbb{R}$

Доказательство. Если вспомнить лекции по математическому анализу, мы доказывали неравномощность $\mathbb{N}$ и $(0,1)$, воспользовавшись тем, что $\mathbb{R} \sim (0,1)$.

В этот раз воспользуемся $\mathbb{R} \sim 2^{\mathbb{N}}$, и докажем $\mathbb{N} \nsim 2^{\mathbb{N}}$ для получения требуемого.

Докажем при помощи диагонального рассудения:

Пусть $F = \{f_0, f_1, \ldots, f_n, \ldots\}$ – множество последовательностей $f \in 2^{\mathbb{N}}$. Покажем, что $\exists x \in 2^{\mathbb{N}} : x \notin F$, тем самым доказав, что отображение $\mathbb{N} \to 2^{\mathbb{N}}$ не сюръективно.

Запишем элементы F в квадратную таблицу по правилу $f_i = \{f_{i0}\ f_{i1} \ldots f_{in}\}$:

$$\begin{array}{lllll} f_0 = & f_{00} & f_{01} & \ldots & f_{0n} \\ f_1 = & f_{10} & f_{11} & \ldots & f_{1n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ f_n = & f_{n0} & f_{n1} & \ldots & f_{nn} \end{array}$$

Выпишем последовательность по диагонали: $f_* = \{f_{00}\ f_{11}\ f_{22} \ldots f_{nn}\}$. Тогда пусть $x = \{\overline{f_{00}}\ \overline{f_{11}} \ldots \overline{f_{nn}}\}$. Тогда $x \neq f_i\ \forall i \in [0,n]$, так как $x_j = \overline{f_{jj}} \neq f_{jj}\ \forall j$. Значит, отображение не сюръективно.

Таким образом, $\mathbb{N} \nsim 2^{\mathbb{N}}$, и так как $\mathbb{R} \sim 2^{\mathbb{N}}$, то $\mathbb{N} \nsim \mathbb{R}$.

Q.E.D.

Полная теорема Кантора. $X \nsim 2^X\ \forall$ *множества X. Иначе говоря, любое множество не равномощно множеству своих подмножеств: $X \nsim \phi(x)$.*

Доказательство. Пусть имеется функция $f : X \to \Phi(x)$, сопоставляющая каждому множеству x его подмножество. Докажем, что эта фунция не является биекцией. Для этого достаточно показать, что не соблюдается сюръективность.

Возьмём множество $F = \{x \mid x \notin f(x)\} \in X$ – множество элементов, точно не принадлежащих образу функции f. Докажем, что нет такого y, что $f(y) = F$.

Пусть $y \in F \Rightarrow f(y) = F$, но тогда по определению $y \notin f(y) = F$ – противоречие.

Пусть теперь $y \notin F \Rightarrow X \backslash F = \{x \mid x \in f(x)\}$, но тогда $y \in f(y) = F$ – противоречие.

В итоге получаем, что $F \notin f(x)$, значит, отображение не сюръективно. Следовательно, биекции $f : X \leftrightarrow \phi(x)$ нет, и $X \nsim 2^X\ \forall$ множества X.

Q.E.D.

Определение: Будем говорить, что множество A не больше множества B $(A \leq B)$ тогда и только тогда, когда $\exists f : A \to B$ – инъекция.

Определение: Будем говорить, что множество A не меньше множества B $(A \geq B)$ тогда и только тогда, когда $\exists f : A \to B$ – сюръекция.

Замечание: $A \leq B \iff B \geq A$.

Утверждение: Пусть $A, B \neq \oslash$. Тогда если $\exists f : A \to B$ – инъекция, то $\exists g : B \to A$ – сюръекция, и наоборот.

Доказательство. Пусть $f : A \to B$ – инъекция. Возьмём функцию $y(x)$, такую, что

$$y(x) = \begin{cases} f^{-1}(x), \ x \in f(A) \\ a_0 \in A, \ x \notin f(A) \end{cases}$$

– мы получили сюръекцию из инъекции.

Обратно: пусть $f : B \to A$ – сюръекция. Возьмём некий элемент $a \in A$, тогда $f^{-1}(a) \neq \emptyset$. Но тогда, взяв нашу функцию $y(x)$, получаем: $y(a) \in f^{-1}(a)$. А так как множества из разных a не пересекаются, то получаем инъективность.

Q.E.D.

Теорема Кантора-Бернштейна. *Если множество A равномощно некоторому подмножеству множества B, а B равномощно некоторому подмножеству множества A, то множества A и B равномощны.*

Доказательство. Пусть A равномощно подмножеству B_1 множества B, а B равномощно подмножеству A_1 множества A (см. рис. 1). При взаимно однозначном соответствии между B и A_1 подмножество $B_1 \subset B$ переходит в некоторое подмножество $A_2 \subset A_1$. При этом все три множества A, B_1 и A_2 равномощны, — и нужно доказать, что они равномощны множеству B, или, что то же самое, A_1.

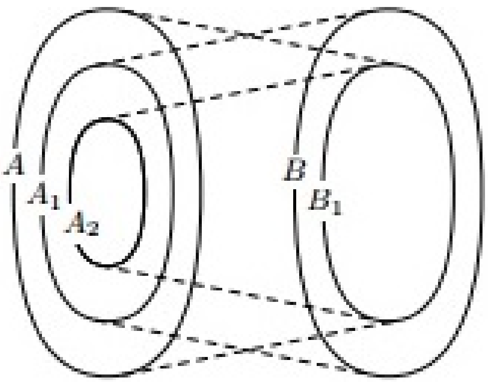

Рис. 1: Взаимные соответсвия между множествами

Теперь мы можем забыть про множество B и его подмножества и доказывать такой факт:

Если $A_2 \subset A_1 \subset A_0$ и $A_2 \sim A_0$, то все три множества равномощны.

(Для единообразия мы пишем A0 вместо A.)

Пусть f — функция, осуществляющая взаимно однозначное соответствие $A_0 \to A_2$ (элемент $x \in A_0$ соответствует элементу $f(x) \in A_2$). Когда A_0 переходит в A_2, меньшее множество A_1 переходит в какое-то множество $A_3 \subset A_2$ (см. рис. 2). Аналогичным образом само A_2 переходит в некоторое множество $A_4 \subset A_2$. При этом $A_4 \subset A3$, так как $A_1 \subset A_2$.

Рис. 2: Последовательные вхождения множеств

Продолжая эту конструкцию, мы получаем убывающую последовательность множеств

$$A_0 \supset A_1 \supset A_2 \supset A_3 \supset A_4 \supset \dots$$

и взаимно однозначное соответствие $f : A_0 \to A_2$, при котором A_i соответствует A_{i+2} (иногда это записывают так: $f(A_i) = A_{i+2}$). Формально можно описать A_{2n} как множество тех элементов, которые получаются из какого-то элемента множества A_0 после n-кратного применения функции f. Аналогичным образом A_{2n+1} состоит из тех и только тех элементов, которые получаются из какого-то элемента множества A_1 после n-кратного применения функции f.

Заметим, что пересечение всех множеств A_i вполне может быть непусто: оно состоит из тех элементов, у которых можно сколько угодно раз брать f-прообраз. Теперь можно сказать так: множество A_0 мы разбили на непересекающиеся слои $C_i = A_i/A_{i+1}$ и на сердцевину $C = \cap_i A_i$.

Слои $C_0, C_2, C_4, \dots$ равномощны (функция f осуществляет взаимно однозначное соответствие между C_0 и C_2, между C_2 и C_4 и т.д.):

$$C_0 \xrightarrow{f} C_2 \xrightarrow{f} C_4 \xrightarrow{f} \dots$$

То же самое можно сказать про слои с нечётными номерами:

$$C_1 \xrightarrow{f} C_3 \xrightarrow{f} C_5 \xrightarrow{f} \dots$$

Можно ещё отметить (что, впрочем, не понадобится), что функция f на множестве C осуществляет его перестановку.

Теперь легко понять, как построить взаимно однозначное соответствие g между A_0 и A_1. Пусть $x \in A_0$. Тогда соответствующий ему элемент $g(x)$ строится так: $g(x) = f(x)$ при $x \in C_{2k}$ и $g(x) = x$ при $x \in C_{2k+1}$ или $x \in C$ (см. рис. 3)

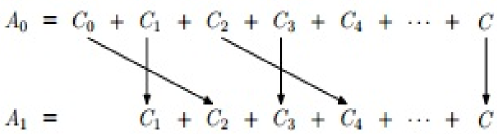

Рис. 3: Построение взаимно-однозначного соответствия

Q.E.D.