МАТЕМАТИЧЕСКАЯ ЛОГИКА

А. В. Яковлев

1. Исчисление высказываний

1.1.Арифметика высказываний. В этом пункте мы не заботимся о строгости изложения. Основным понятием является понятие *высказывания*. Высказыванием мы называем любое утверждение, про которое можно сказать, истинно оно или ложно. Конечно, эту фразу нельзя принять за строгое определение понятия высказывания; мы просто свели его к другому термину *утверждение*. Впрочем, вряд ли возможно дать ни на что не опирающееся строгое определение какого-либо первоначального понятия. Подобную же ситуацию мы имели для множеств: никакого точного определения множества мы дать не могли, и было возможно привести лишь несколько синонимов этого понятия (совокупность, коллекция и т.п.), позволяющих составить о нем представление.

Приведем несколько примеров высказываний.

(1) $2 \times 2 = 4$.
(2) Волга впадает в Каспийское море.
(3) Наполеон умер 5 мая 1821 года.
(4) Третье тысячелетие начнется 1 января 2000 года.
(5) Медианы невырожденного треугольника делятся их точкой пересечения пополам.
(6) Среди первых 10^{100} цифр десятичного разложения числа $e + \pi$ встретятся подряд 10^{89} нулей.

Высказывания (1)-(3) истинны, высказывания (4) и (5) ложны. Что касается высказывания (6), то мы не знаем, и вряд ли когда сможем узнать, истинно оно или ложно; однако, это тем не менее является высказыванием, потому что оно или выполняется, или нет, независимо от того, знаем ли мы правильный ответ.

Будем обозначать высказывания большими латинскими буквами, возможно, с индексами: A, B, C, D_i, $\bar{A}'$ и т.д. Пусть нам дан некоторый набор высказываний, которые мы будем называть *простыми* высказываниями. Из них можно составлять новые высказывания при помощи нескольких элементарных конструкций. Например, если A и B — простые высказывания, то мы можем составить высказывания "A **и** B", "A **или** B", "**или** A, **или** B", "**из** A **следует** B", "A, B **эквивалентны**", "**не** B". Хотя смысл этих новых высказываний представляется ясным, необходимо внести некоторые уточнения и разъяснения: ведь наш разговорный язык зачастую допускает неоднозначное толкование, а в математике такое положение недопустимо.

Высказывание "A **и** B" называется *конъюнкцией* высказываний A и B; оно означает, что одновременно выполняются и A, и B. Для конъюнкции высказываний A и B используется обозначение $A\&B$. Высказывание $A\&B$ истинно тогда и только тогда, когда истинны оба высказывания A и B; если хотя бы одно из высказываний A, B ложно, то и их конъюнкция $A\&B$ ложна.

Высказывание "A **или** B" означает, что выполняется хотя бы одно из высказываний A, B. Подчеркнем, что могут выполняться и оба высказывания; в разговорном русском языке слово "или" иногда понимается в том смысле, что должно выполняться в точности одно из высказываний. Обозначается высказывание "A **или** B" через $A\vee B$ и называется *дизъюнкцией* A и B. Дизъюнкция $A\vee B$ истинна, если истинно хотя бы одно из высказываний A, B; она является ложной только в том случае, когда ложны оба высказывания A, B. Еще раз подчеркнем разницу между дизъюнкцией и так называемой *разделительной дизъюнкцией* "**или** A, **или** B", которая является истинной тогда, когда истинно в точности одно из высказываний A, B.

Точный смысл высказывания "*не* А" совпадает с общепринятым: оно истинно, если A ложно, и оно ложно, если A истинно. Это высказывание называется отрицанием высказывания A и обозначается $\neg A$.

Высказывание "A, B **эквивалентны**" тоже имеет общепринятый смысл: оно истинно, если оба высказывания A, B одновременно истинны или одновременно ложны, и оно ложно, если одно из высказываний A, B истинно, а другое ложно. Это высказывание называется эквивалентностью и обозначается $A\leftrightarrow B$.

Наконец, высказывание "**из** A **следует** B", называемое *импликацией* и записываемое в виде $A\to B$, считается ложным только если A истинно, а B ложно. Таким образом, из ложной посылки следует все, что угодно, а из истинной посылки следуют только истинные высказывания. В обыденной речи мы не всегда понимаем следование именно в таком смысле, поэтому приведенное выше уточнение понятия импликации было необходимым. Отметим классический пример истинной импликации, приведенный Хаусдорфом в его "Теории множеств": если $1=0$, то все ведьмы зеленые.

Применяя несколько раз эти операции, мы можем составить новые, более сложные высказывания. Укажем несколько примеров таких составных высказываний: $\neg((A\&B)\to C)\leftrightarrow(B\&C)$, $((A\to B)\to C)\leftrightarrow(A\to(B\to C))$, $(\neg(A\vee B))\to(\neg A\&\neg B)$. Если нам известно, истинны или ложны простые высказывания A, B, C, то мы легко можем вычислить значение истинности для любого составного высказывания. В качестве примера проделаем это для высказывания $\neg((A\&B)\to C)\leftrightarrow(B\&C)$, предположив, что A ложно, а B и C истинны. Высказывание $A\&B$ ложно, так как ложной является одна из компонент конъюнкции; поэтому импликация $(A\&B)\to C$ истинна, Значит, отрицание этой импликации $\neg((A\&B)\to C)$ ложно. Далее, конъюнкция двух истинных высказываний $B\&C$ истинна, и потому эквивалентность $\neg((A\&B)\to C)\leftrightarrow(B\&C)$ истинного и ложного высказываний ложна.

Тот факт, что высказывание истинно, будем обозначать буквой "и", а ложным высказываниям будем сопоставлять букву "л". Значение истинности высказывания A будем обозначать $|A|$.

1.2. Алгебра высказываний. Так же, как при переходе от арифметики к алгебре мы вместо конкретных натуральных чисел начинаем рассматривать произвольные числа, обозначаемые буквами x, y и т.д., будем обозначать буквами X_1, X_2, ... произвольные высказывания. Из них можно составлять новые высказывания. Точнее говоря, высказывания определяются следующим образом.

Определение.

(1) "и" *и* "л" — *высказывания;*
(2) X_n — *высказывание для всякого натурального числа* $n \geq 1$;
(3) *если* A, B — *высказывания, то* $(A\&B)$, $(A \vee B)$, $(A \to B)$, $(A \leftrightarrow B)$, $(\neg A)$ — *тоже высказывания.*

Никакое выражение, которое не может быть получено по указанным правилам, не является высказыванием.

Таким образом, всякое высказывание — это слово в алфавите, состоящем из букв "(", ")", "&", " $\vee$ ", " $\to$ ", " $\leftrightarrow$ ", "и", "л", "X_n" (но не все слова являются высказываниями). Обычно бывает неудобно использовать бесконечный алфавит; этого можно избежать, если вместо бесконечного числа букв X_n оставить всего две буквы — X и $'$, и ввести обозначения: $X_1 = X$, $X_2 = X'$, $X_3 = X''$ и т.д.

В определении высказывания важную роль играют скобки; они дают возможность однозначно восстановить построение высказывания из простейших высказываний "и", "л", "X_n". Однако, в дальнейшем мы будем опускать для сокращения записи часть скобок, считая, что операция $\neg$ предшествует операциям $\&$, $\vee$, а эти две операции предшествуют операциям $\to$, $\leftrightarrow$, так же, как в алгебре возведение в степень предшествует умножению и делению, а они предшествуют сложению и вычитанию. Любое высказывание, кроме "и", "л", "X_n", заключено в скобки; эти наружные скобки мы будем, как правило, опускать. Наконец, мы будем опускать скобки в конъюнкциях и дизъюнкциях более чем двух высказываний, считая, что сначала действие производится над первыми двумя высказываниями, затем над полученным высказыванием и третьим высказыванием и т.д. Например, полной записью высказывания $X_1\&X_2\&X_3\&X_4$ будет $(((X_1\&X_2)\&X_3)\&X_4)$.

Высказывания X_i называются элементарными высказываниями. Всякое отображение множества элементарных высказываний $\{X_i \mid i = 1, 2, \dots\}$ в множество из двух элементов $\{\text{и}, \text{л}\}$ естественным образом продолжается по описанным выше правилам до отображения в $\{\text{и}, \text{л}\}$ всего множества высказываний. Таким образом, каждому высказыванию A отвечает его функция истинности, сопоставляющая каждому набору значений истинности элементарных высказываний значение истинности высказывания A. Например, функция истинности рассмотренного выше высказывания $A = \neg((X_1\&X_2) \to X_3) \leftrightarrow (X_2\&X_3)$ описывается следующей таблицей значений:

X_1	и	и	и	и	л	л	л	л
X_2	и	и	л	л	и	и	л	л
X_3	и	л	и	л	и	л	и	л
—	—	—	—	—	—	—	—	—
A	л	л	и	и	л	и	и	и

Пусть I — некоторое конечное множество индексов; мы будем обозначать через $\bigvee\limits_{i\in I} A_i$ и $\bigwedge\limits_{i\in I} A_i$ дизъюнкцию и конъюнкцию высказываний A_i, $i \in I$, взятых в произвольном порядке (все утверждения, в формулировке которых будут участвовать эти обозначения, выполняются при любом порядке высказываний). Конъюнкция пустого множества высказываний считается равной высказыванию "и", а дизъюнкция пустого множества высказываний — высказыванию "л".

Теорема. *Пусть* $\{\text{и},\text{л}\}^n$ *— n-я декартова степень множества* $\{\text{и},\text{л}\}$, *т.е. множество всех наборов* $(\varepsilon_1,\dots,\varepsilon_n)$, *таких что* $\varepsilon_i =$ и *или* $\varepsilon_i =$ л *для любого* i, $1 \le i \le n$. *Далее, пусть* I *— подмножество* $\{\text{и},\text{л}\}^n$. *Суждение*

$$X_I = \bigvee_{(\varepsilon_1,\dots,\varepsilon_n)\in I} ((\bigwedge_{i,\varepsilon_i=\text{и}} X_i)\&(\bigwedge_{j,\varepsilon_j=\text{л}} \neg X_j))$$

истинно тогда и только тогда, когда $(|X_1|,\dots,|X_n|) \in I$.

Доказательство. Конъюнкция $(\bigwedge\limits_{i,\varepsilon_i=\text{и}} X_i)\&(\bigwedge\limits_{j,\varepsilon_j=\text{л}} \neg X_j)$ истинна тогда и только тогда, когда элементарное высказывание X_i истинно при условии, что ε_i=и и ложно при условии ε_i=л; иными словами, эта конъюнкция истинна, если и только если $(|X_1|,\dots,|X_n|) = (\varepsilon_1,\dots,\varepsilon_n)$. Высказывание X_I является дизъюнкцией тех из этих конъюнкций, которые отвечают наборам $(\varepsilon_1,\dots,\varepsilon_n)$, принадлежащим I; она истинна тогда и только тогда, когда истинна одна из этих конъюнкций, т.е. когда $(|X_1|,\dots,|X_n|) \in I$.

Следствие 1. *Если подмножества* I, J *множества* $\{\text{и},\text{л}\}^n$ *не совпадают, то и функции истинности, отвечающие высказываниям* X_I, X_J *не совпадают.*

Следствие 2. *Пусть* $f(\xi_1,\dots,\xi_n) : \{\text{и},\text{л}\}^n \to \{\text{и},\text{л}\}$ *— функция, сопоставляющая каждому набору значений истинности элементарных высказываний один из символов* "и", "л". *Существует высказывание* X, *функция истинности для которого совпадает с* $f(\xi_1,\dots,\xi_n)$, *т.е. такое высказывание, что* $|X| = f(|X_1|,\dots,|X_n|)$.

Доказательство. Пусть $I \subseteq \{\text{и},\text{л}\}^n$ — множество всех тех наборов $(\varepsilon_1,\dots,\varepsilon_n)$, для которых $f(\varepsilon_1,\dots,\varepsilon_n) =$ и. Тогда высказывание X_I истинно тогда и только тогда, когда $(\varepsilon_1,\dots,\varepsilon_n) \in I$, т.е. когда $f(\varepsilon_1,\dots,\varepsilon_n) =$ и.

Бывают такие высказывания, которые являются истинными при любых значениях истинности основных высказываний $X_1, X_2, \dots$; такие высказывания называются *тождественно истинными* или *тавтологиями*. Приведем несколько примеров тавтологий:

$$X_1\&X_2 \to X_1, \quad X_1 \to (\neg X_1 \vee X_1), \quad ((X_2\&\neg X_1) \to (\text{л})) \to (X_2 \to X_1).$$

1.3. Булевы алгебры. Рассмотрим один тип алгебраических структур, который очень хорошо приспособлен для описания алгебры высказываний.

Определение. *Булевой алгеброй называется множество B, на котором заданы две бинарных операции — сложение "$+$" и умножение "$\cdot$", одна унарная операция — дополнение $x \to x'$ и в котором выделены две константы — 0 и 1, причем для любых элементов $x, y, z \in B$ выполняются следующие соотношения:*

(1) *(законы поглощения)* $x + x = x$, $x \cdot x = x$;
(2) *(коммутативность)* $x + y = y + x$, $x \cdot y = y \cdot x$;
(3) *(ассоциативность)* $x + (y + z) = (x + y) + z$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$;
(4) *(дистрибутивность)* $x \cdot (y+z) = (x \cdot y) + (x \cdot z)$, $(x \cdot y) + z = (x+z) \cdot (y+z)$;
(5) *(свойства 0 и 1)* $x \cdot 0 = 0$, $x \cdot 1 = x$, $x + 0 = x$, $x + 1 = 1$;
(6) *(свойства дополнения)* $x \cdot x' = 0$, $x + x' = 1$, $(x+y)' = x' \cdot y'$, $(x \cdot y)' = x' + y'$, $(x')' = x$.

Важнейшим примером булевой алгебры является множество $P(A)$ всех подмножеств некоторого множества A; действия над подмножествами определены следующим образом: для любых $X, Y \subseteq A$

$$X + Y = X \cup Y,\ X \cdot Y = X \cap Y,\ X' = A \setminus X = \{a \in X \mid a \notin X\}.$$

Единицей булевой алгебры $P(A)$ является все множество A, а нулем — пустое подмножество.

В дальнейшем мы часто будем опускать знак умножения $\cdot$ и часть скобок, пользуясь привычными соглашениями о том, что умножение предшествует сложению. Например, выражение $xy + ztu$ в развернутом виде выглядит так: $(x \cdot y) + (z \cdot (t \cdot u))$.

Все обычные алгебраические понятия — подалгебра, гомоморфизм, изоморфизм и т.п., естественным образом могут быть определены и для булевых алгебр; мы опускаем все эти определения, поскольку они ничем не отличаются от соответствующих определений для групп, векторных пространств, модулей и др.

В последующих рассуждениях нам будет удобно применять следующее обозначение. Пусть b — элемент некоторой булевой алгебры, и пусть ε равно 1 или -1; через b^ε мы будем обозначать элемент b, если $\varepsilon = 1$, и элемент b', если $\varepsilon = -1$.

Пусть B — произвольная булева алгебра, и пусть $b_1, \ldots, b_n$ — какие-то элементы из B. Если I — подмножество n-й декартовой степени $\{1, -1\}^n$ множества $\{1, -1\}$, то обозначим $b_I = \sum\limits_{(\varepsilon_1, \ldots, \varepsilon_n) \in I} (\prod\limits_{i=1}^{n} b_i^{\varepsilon_i})$. В частности, $b_\emptyset = 0$, $b_{\{1,-1\}^n} = \sum\limits_{(\varepsilon_1, \ldots, \varepsilon_n)} (\prod\limits_{i=1}^{n} b_i^{\varepsilon_i}) = \prod\limits_{i=1}^{n} (b_i + b_i') = 1$.

Лемма. *Для любых подмножеств $I, J \subseteq \{1, -1\}^n$*

$$b_I + b_J = b_{I \cup J}, \quad b_I \cdot b_J = b_{I \cap J}, \quad b_I' = b_{P(n) \setminus I}.$$

Кроме того, для любого s, $1 \le s \le n$, элемент b_s совпадает с $b_{I(s)}$, где $I(s)$ — множество всех тех наборов $(\varepsilon_1, \ldots, \varepsilon_n)$, в которых $\varepsilon_s = 1$. Таким образом,

множество $S(b_1,\dots,b_n)$ всех элементов b_I является подалгеброй булевой алгебры B; она содержит элементы $b_1,\dots,b_n$ и содержится в любой подалгебре булевой алгебры B, обладающей этим свойством.

Доказательство. Утверждение $b_I + b_J = b_{I\cup J}$ сразу следует из закона поглощения для суммы. Заметим теперь, что если $(\varepsilon_1,\dots,\varepsilon_n) \neq (\delta_1,\dots,\delta_n)$ существует номер s, такой что $\varepsilon_s \neq \delta_s$; поэтому произведение $(\prod\limits_{i=1}^{n} b_i^{\varepsilon_i}) \cdot (\prod\limits_{i=1}^{n} b_i^{\delta_i})$ содержит сомножители b_s, b'_s и потому равно 0. Из дистрибутивности и законов поглощения для умножения и сложения следует, что произведение

$$b_I \cdot b_J = (\sum_{(\varepsilon_1,\dots,\varepsilon_n)\in I} (\prod_{i=1}^{n} b_i^{\varepsilon_i})) \cdot (\sum_{(\delta_1,\dots,\delta_n)\in J} (\prod_{i=1}^{n} b_i^{\varepsilon_i}))$$

состоит только из таких слагаемых $\prod\limits_{i=1}^{n} b_i^{\varepsilon_i}$, которые входят и в b_I, и в b_J, и потому $b_I \cdot b_J = b_{I\cap J}$.

Пусть теперь $J = \{1,-1\}^n \setminus I$; из уже доказанного следует, что $b_I + b_J = b_{I\cup J} = 1$, $b_I \cdot b_J = b_\emptyset = 0$. Поэтому $b'_I = b'_I(b_I + b_J) = b'_I b_i + b'_I b_J = 0 + b'_I b_J = b_I b_J + b'_I b_J = (b_I + b'_I)b_J = 1 \cdot b_J = b_J$.

Наконец, $b_s = b_s \prod\limits_{i\neq s}(b_i + b'_i) = \sum\limits_{\substack{(\varepsilon_1,\dots,\varepsilon_n)\\ \varepsilon_s=1}} \prod\limits_{i=1}^{n} b_i^{\varepsilon_i} = b_{I_s}$.

Будем говорить, что построенная в только что доказанной лемме подалгебра $S(b_1,\dots,b_n)$ порождена элементами $b_1,\dots,b_n$. Если $S(b_1,\dots,b_n) = B$, то говорим, что $b_1,\dots,b_n$ — порождающая система булевой алгебры B; если к тому же все элементы b_I, $I \subseteq \{1,-1\}^n$, различны, то говорим, что B — свободная булева алгебра со свободными образующими $b_1,\dots,b_n$. Из этого определения следует, что свободная булева алгебра с n свободными образующими состоит из 2^{2^n} элементов.

Пусть теперь $\{b_i \,|\, i \in I\}$ — какое-то, вообще говоря, бесконечное семейство элементов из B. Будем говорить, что булева алгебра B порождена этим семейством, если для любого элемента $x \in B$ существует его конечное подсемейство $\{b_{i_1},\dots,b_{i_n}\}$, такое что $x \in S(b_{i_1},\dots,b_{i_n})$. Далее, если булева алгебра B порождена семейством $\{b_i \,|\, i \in I\}$ и если для каждого конечного подсемейства $\{b_{i_1},\dots,b_{i_n}\}$ множество $S(b_{i_1},\dots,b_{i_n})$ является свободной булевой алгеброй со свободными образующими $b_{i_1},\dots,b_{i_n}$, то мы говорим, что B — свободная булева алгебра со свободными образующими $\{b_i \,|\, i \in I\}$.

1.4. Булева алгебра высказываний. Будем говорить, что два высказывания A, B эквивалентны, если высказывание $A \leftrightarrow B$ является тавтологией. Поскольку эквивалентность истинна тогда и только тогда, когда обе её части имеют одинаковое значение истинности, приходим к выводу: два высказывания A, B эквивалентны тогда и только тогда, когда при любых значениях истинности элементарных высказываний X_i оба высказывания A, B одновременно истинны или ложны. Отсюда и из того факта, что значение истинности высказываний $A\&B$, $A \vee B$, $\neg A$, $A \to B$, $A \leftrightarrow B$ вполне определяется значениями истинности высказываний A, B, сразу вытекает следующее важное утверждение.

Лемма. (1) *Всякое высказывание эквивалентно самому себе.*

(2) *Если высказывание A эквивалентно высказыванию B, то высказывание B эквивалентно высказыванию A.*

(3) *Если высказывание A эквивалентно высказыванию B, а высказывание B эквивалентно высказыванию C, то высказывание A эквивалентно высказыванию C.*

(4) *Если высказывание A_1 эквивалентно высказыванию A, а высказывание B_1 эквивалентно высказыванию B, то высказывания $A_1\&B_1$, $A_1 \vee B_1$, $\neg A_1$, $A_1 \to B_1$, $A_1 \leftrightarrow B_1$ эквивалентны соответственно высказываниям $A\&B$, $A \vee B$, $\neg A$, $A \to B$, $A \leftrightarrow B$.*

Первые три утверждения леммы показывают, что эквивалентность высказываний действительно является отношением эквивалентности на множестве всех высказываний. Поэтому множество высказываний разбивается в объединение классов эквивалентности. Пусть $\mathfrak{X}$ — множество классов эквивалентности высказываний. Класс эквивалентности, содержащий высказывание A, будем обозначать через $[A]$. Определим на $\mathfrak{X}$ действия сложения, умножения и дополнения, положив

$$[A] + [B] = [(A \vee B)], \quad [A] \cdot [B] = [(A\&B)], \quad [A]' = [(\neg A)];$$

последнее утверждение леммы показывает, что эти определения не зависят от выбора высказываний, представляющих классы эквивалентности. Обозначим также через 0 и 1 классы [л] и [и], а через x_i — классы $[X_i]$.

Теорема. *Множество $\mathfrak{X}$ с введенными выше операциями является свободной булевой алгеброй со свободными образующими x_i, $i = 1, 2, \ldots$. Для любых высказываний A, B выполняются соотношения $[A \to B] = [A]' + [A] \cdot [B]$, $[A \leftrightarrow B] = [A] \cdot [B] + [A]' \cdot [B]'$. Высказывания A, B эквивалентны тогда и только тогда, когда $[A] = [B]$. Высказывание A является тавтологией тогда и только тогда, когда $[A] = [\text{и}] = 1$.*

Доказательство. Последние два утверждения приведены для полноты и фактически содержатся в самом определении множества $\mathfrak{X}$. Далее, непосредственная проверка показывает, что следующие пары высказываний эквивалентны, т.е. имеют одинаковые функции истинности:

(1) $A \vee A$ и A, $A\&A$ и A;

(2) $A \vee B$ и $B \vee A$, $A\&B$ и $B\&A$;

(3) $A \vee (B \vee C)$ и $(A \vee B) \vee C$, $A\&(B\&C)$ и $(A\&B)\&C$;

(4) $A\&(B \vee C)$ и $(A\&B) \vee (A\&C)$, $(A\&B) \vee C$ и $(A \vee C)\&(B \vee C)$;

(5) $A\&$(л) и (л), $A\&$(и) и A, $A \vee$ (л) и A, $A \vee$ (и) и (и);

(6) $A\&(\neg A)$ и (л), $A \vee (\neg A)$ и (и), $\neg(A \vee B)$ и $(\neg A)\&(\neg B)$, $\neg(A\&B)$ и $(\neg A) \vee (\neg B)$, $\neg(\neg A)$ и A;

(7) $A \to B$ и $(\neg A) \vee (A\&B)$, $A \leftrightarrow B$, $(A\&B) \vee ((\neg A)\&(\neg B))$.

Все утверждения теоремы, кроме того, что элементы x_i являются свободными образующими $\mathfrak{X}$, следуют отсюда; в частности, эквивалентность пар высказываний, собранных в (1)-(6), показывает, что выполняются все аксиомы булевой алгебры.

Ясно, что элементы x_i порождают алгебру $\mathfrak{X}$; для того, чтобы показать, что они являются свободными образующими $\mathfrak{X}$, достаточно проверить, что для любого n элементы $x_1, \ldots, x_n$ свободно порождают алгебру $S(x_1, \ldots, x_n)$, т.е. что для любых различных подмножеств I, J множества $\{0,1\}^n$ элементы

$$x_I = \sum_{(\varepsilon_1,\ldots,\varepsilon_n)\in I} (\prod_{i=1}^{n} b_i^{\varepsilon_i}), \quad x_J = \sum_{(\varepsilon_1,\ldots,\varepsilon_n)\in J} (\prod_{i=1}^{n} b_i^{\varepsilon_i})$$

различны. Но эти элементы являются классами эквивалентности высказываний

$$X_I = \bigvee_{(\varepsilon_1,\ldots,\varepsilon_n)\in I} ((\bigwedge_{i,\varepsilon_i=1} X_i)\&(\bigwedge_{j,\varepsilon_j=-1} \neg X_j)),$$
$$X_J = \bigvee_{(\varepsilon_1,\ldots,\varepsilon_n)\in J} ((\bigwedge_{i,\varepsilon_i=1} X_i)\&(\bigwedge_{j,\varepsilon_j=-1} \neg X_j)),$$

которые не эквивалентны, ибо по следствию 1 из §1.2 они имеют различные функции истинности.

1.5 Каноническая дизъюнктивно-конъюнктивная форма высказывания.

Теорема. *Всякое высказывание, зависящее только от элементарных высказываний $X_1, \ldots, X_n$, эквивалентно единственному высказыванию вида*

$$X_I = \bigvee_{(\varepsilon_1,\ldots,\varepsilon_n)\in I} ((\bigwedge_{i,\varepsilon_i=\text{и}} X_i)\&(\bigwedge_{j,\varepsilon_j=\text{л}} \neg X_j)),$$

где I — некоторое подмножество множества $\{\text{и}, \text{л}\}^n$.

Эта теорема немедленно следует из теоремы предыдущего пункта и из того, что всякий элемент свободной булевой алгебры, порожденной элементами $x_1, \ldots, x_n$, однозначно представим в виде $x_I = \sum_{(\varepsilon_1,\ldots,\varepsilon_n)\in I} (\prod_{i=1}^{n} x_i^{\varepsilon_i})$ для некоторого подмножества $I \subseteq \{1, -1\}^n$. Такой представитель класса эквивалентных высказываний называется канонической дизъюнктивно-конъюнктивной формой высказывания.

1.6 Идеалы и дуальные идеалы булевой алгебры. Пусть $\mathfrak{B}$ — булева алгебра; её непустое подмножество $\mathfrak{I}$ называется идеалом алгебры $\mathfrak{B}$, если для любых $x, y \in \mathfrak{I}$, $b \in \mathfrak{B}$ элементы $x + y$, bx принадлежат $\mathfrak{I}$.

Во всякой булевой алгебре есть два тривиальных идеала — 0 и вся алгебра. Пусть теперь $S \subseteq \mathfrak{B}$; очевидно, пересечение всех идеалов булевой алгебры $\mathfrak{B}$, содержащих S, снова является идеалом алгебры $\mathfrak{B}$, содержащим S. Этот идеал называется идеалом, порожденным множеством S, и является наименьшим идеалом, содержащим это множество элементов.

Теорема. *Пусть $\mathfrak{B}$ — булева алгебра, и пусть $S \subseteq \mathfrak{B}$. Идеал алгебры $\mathfrak{B}$, порожденный множеством S, является объединением идеалов, порожденных всеми конечными подмножествами S. Идеал, порожденный конечным множеством $\{b_1, \ldots, b_n\}$, порождается одним элементом $b = b_1 + \cdots + b_n$ и состоит из всех элементов вида ab, $a \in \mathfrak{B}$.*

Доказательство. Обозначим через $\mathfrak{J}$ объединение всех идеалов, порожденных конечными подмножествами S; каждый из этих идеалов содержится в идеале $\mathfrak{I}$, порожденном множеством S, и потому $\mathfrak{J} \subseteq \mathfrak{I}$. Обратно, ясно, что $\mathfrak{J}$ является идеалом алгебры $\mathfrak{B}$, содержащим множество S и, поскольку $\mathfrak{I}$ — наименьший идеал, содержащий S, находим, что $\mathfrak{I} \subseteq \mathfrak{J}$.

Пусть теперь $\mathfrak{I}$ — идеал, порожденный конечным множеством $b_1, \ldots, b_n$; тогда $b = b_1 + \cdots + b_n \in \mathfrak{I}$. Обратно, элемент $b_1 = b_1 \cdot 1 = b_1(1 + b_2 + \cdots + b_n) = b_1 + b_1(b_2 + \cdots + b_n) = b_1 b_1 + b_1(b_2 + \cdots + b_n) = b_1(b_1 + b_2 + \cdots + b_n) = b_1 b$ принадлежит идеалу, порожденному одним элементом b, и точно так же элементы $b_2 = b_2 b$, $\ldots$, $b_n = b_n b$ принадлежат идеалу, порожденному b. Итак, эти два идеала совпадают. Остается заметить, что идеал, порожденный единственным элементом b, состоит из всех элементов вида ab, $a \in \mathfrak{B}$.

В отличие от колец, где операции сложения и умножения отнюдь не равноправны, в булевой алгебре сложение и умножение обладают одними и теми же свойствами. В частности, если мы поменяем местами 0 и 1 и будем записывать сложение как умножение, а умножение — как сложение, мы снова получим булеву алгебру. Из этой дуальности следует, что в теории булевых алгебр понятие, дуальное понятию идеала, должно играть столь же важную роль, как и понятие идеала (что совсем не так для колец). Итак, мы приходим к следующему определению.

Пусть $\mathfrak{B}$ — булева алгебра; её непустое подмножество $\mathfrak{I}$ называется дуальным идеалом алгебры $\mathfrak{B}$, если для любых $x, y \in \mathfrak{I}$, $b \in \mathfrak{B}$ элементы xy, $b + x$ принадлежат $\mathfrak{I}$.

Во всякой булевой алгебре есть два тривиальных дуальных идеала — 1 и вся алгебра. Пусть теперь $S \subseteq \mathfrak{B}$; очевидно, пересечение всех дуальных идеалов булевой алгебры $\mathfrak{B}$, содержащих S, снова является дуальным идеалом алгебры $\mathfrak{B}$, содержащим S. Этот дуальный идеал называется дуальным идеалом, порожденным множеством S, и является наименьшим дуальным идеалом, содержащим это множество элементов.

Теорема. *Пусть $\mathfrak{B}$ — булева алгебра, и пусть $S \subseteq \mathfrak{B}$. Дуальный идеал алгебры $\mathfrak{B}$, порожденный множеством S, является объединением дуальных идеалов, порожденных всеми конечными подмножествами S. Дуальный идеал, порожденный конечным множеством $\{b_1, \ldots, b_n\}$, порождается одним элементом $b = b_1 \cdot \ldots \cdot b_n$ и состоит из всех элементов вида $a + b$, $a \in \mathfrak{B}$.*

1.7. Выводимость. Пусть S — некоторое множество высказываний; мы говорим, что высказывание A выводимо из множества высказываний S и записываем это в виде $S \vdash A$, если существует конечное (быть может, пустое) множество высказываний $Y_1, \ldots, Y_m \in S$, такое что высказывание $(Y_1 \& \ldots \& Y_m) \to A$ является тождественно истинным высказыванием (тавтологией). Пусть A — тавтология; поскольку высказывание (и) $\to A$ тоже является тавтологией, а

тождественно истинное высказывание "и" — это конъюнкция пустого множества высказываний, то высказывание A выводимо из S.

Теорема. *Высказывание A выводимо из множества высказываний S тогда и только тогда, когда его класс $[A]$ в булевой алгебре высказываний $\mathfrak{X}$ принадлежит дуальному идеалу, порожденному классами $[Y]$ всех высказываний $Y \in S$.*

Доказательство. Пусть $S \vdash A$; тогда существуют высказывания $Y_1, \ldots, Y_m \in S$, такие что высказывание $(Y_1 \& \ldots \& Y_m) \to A$ тождественно истинно. Обозначим через Z высказывание $Y_1 \& \ldots \& Y_m$. По теореме из §1.4 тождественная истинность высказывания $Z \to A$ означает, что $[Z]' + [Z][A] = 1$. Домножив обе части этого равенства на $[Z]$, получаем: $[Z] = [Z]([Z]' + [Z][A]) = [Z][A]$, откуда следует, что элемент

$$[A] = [A]([Z] + [Z]') = [A][Z] + [A][Z]' = [Z] + [A][Z]' = [Y_1] \ldots [Y_n] + A[Z]'$$

принадлежит дуальному идеалу булевой алгебры $\mathfrak{X}$, порожденному элементами $[Y_1]$, ... ,$[Y_m]$.

Обратно, пусть класс эквивалентности $[A]$ высказывания A принадлежит дуальному идеалу, порожденному классами высказываний, принадлежащих S. По теореме из предыдущего пункта, существуют высказывания $Y_1, \ldots, Y_n \in S$ и высказывание X, такие что $[A] = [Y_1] \ldots [Y_n] + [X]$. Обозначим, как и выше, через Z высказывание $Y_1 \& \ldots \& Y_n$; тогда $[A] = [Z] + [X]$. Находим теперь, что $[Z]' + [Z][A] = [Z]' + [Z]([Z] + [X]) = [Z]' + [Z] + [Z][X] = 1$, а это означает, что высказывание $Z \to A$ тождественно истинно, т.е. что высказывание A выводимо из высказывания $Z = Y_1 \& \ldots \& Y_n$.

1.8.Правила подстановки и силлогизма. Покажем, что если высказывание выводимо из множества высказываний $\mathfrak{S}$, то оно может быть получено многократным применением нескольких простых правил.

Теорема. *Пусть S — некоторое множество высказываний.*

(1) *Если $X \in S$, то X выводимо из S.*
(2) *Если высказывание X — тавтология, то X выводимо из S.*
(3) *Если высказывания X, $X \to Y$ выводимы из S, то и высказывание Y выводимо из S.*
(4) *Любое высказывание, выводимое из S, может быть получено многократным применением правил (1)-(3).*

Доказательство. Утверждение (2) уже было отмечено выше, а утверждение (1) тривиально: высказывание $X \to X$ является тавтологией. Докажем теперь (3). Пусть $\mathfrak{I}$ — дуальный идеал алгебры высказываний $\mathfrak{X}$, порожденный классами всех высказываний из S. Если высказывания X, $X \to Y$ выводимы из S, то, по теореме из §1.7, их классы $[X]$, $[X \to Y] = [X]' + [X][Y]$ принадлежат $\mathfrak{I}$, а потому и $[Y] = [Y] + [X]([X]' + [X][Y]) \in \mathfrak{I}$, а это и значит, по той же теореме, что высказывание Y выводимо из S.

Несколько сложнее доказывается обратное утверждение (4). Сначала индукцией по m покажем, что если высказывания Y_1, ... ,Y_m принадлежат S,

то высказывание $Y_1\&\ldots\&Y_m$ получается применением правил (1)-(3). База индукции доставляется правилом (1). Пусть $m > 1$ и уже доказано, что высказывание $Y_1\&\ldots\&Y_{m-1}$ получается применением правил (1)-(3). Высказывание

$$(Y_1\&\ldots\&Y_{m-1}) \to (Y_m \to (Y_1\&\ldots\&Y_m))$$

является тавтологией, т.е. оно получается при помощи правила (2). Применяя к последним двум высказываниям правило (3), видим, что высказывание $Y_m \to (Y_1\&\ldots\&Y_m)$ получается применением правил (1)-(3). Опять применяя правило (3), на сей раз к высказываниям $Y_m \in S$, $Y_m \to (Y_1\&\ldots\&Y_m)$, найдем, что высказывание $Y_1\&\ldots\&Y_m$ получается применением правил (1)-(3).

Пусть высказывание A выводимо из S; тогда найдутся такие высказывания $Y_1,\ldots,Y_m \in S$, что высказывание $(Y_1\&\ldots\&Y_m) \to A$ — тавтология, т.е. оно получается при помощи правила (2). Но мы только что доказали, что высказывание $Y_1\&\ldots\&Y_m$ получается применением правил (1)-(3). Высказывание A получается из предыдущих двух высказываний по правилу (3).

Теорема полностью доказана.

Правило (3) называется правилом силлогизма, или *modus ponens*. Обычно его иллюстрируют следующим рассуждением:

$$\left.\begin{array}{l}\text{Все люди смертны.}\\ \text{Сократ — человек.}\end{array}\right\} \quad \text{Следовательно, Сократ смертен.}$$

Конечно, этот пример не совсем точен. Правильнее здесь было бы вместо первого высказывания поставить его специальный случай: "Если Сократ человек, то Сократ смертен".

Обратимся теперь к правилу (2). Строго говоря, это не одно правило, а бесконечно много правил, потому что имеется бесконечно много тавтологий. Однако, используя *modus ponens* и еще одно правило — правило подстановки — мы можем вывести все тавтологии из некоторого конечного множества тавтологий. Этот основной конечный набор тавтологий можно выбрать многими способами; мы приведем здесь один такой набор; хотя некоторые входящие в него тавтологии могут быть выведены из других (так что набор не минимален), нам он кажется наиболее естественным: тавтологии (6)-(18) по существу совпадают с аксиомами булевой алгебры, тавтологии (4) и (5) выражают характеристические свойства дизъюнкции и конъюнкции, а остальные тавтологии из этого набора сводят импликацию и эквивалентность к булевым операциям.

(1) $(A \leftrightarrow B) \to ((A \to B)\&(B \to A))$;
(2) $((A \to B)\&(B \to A)) \to (A \leftrightarrow B)$;
(3) $(A \to B) \leftrightarrow (\neg A \vee B)$;
(4) $A \to (A \vee B)$;
(5) $(A\&B) \to A$;
(6) $(A\&B) \leftrightarrow (B\&A)$;
(7) $((A\&B)\&C) \leftrightarrow (A\&(B\&C))$;
(8) $(A\&A) \leftrightarrow A$;
(9) $(A \vee B) \leftrightarrow (B \vee A)$;

(10) $((A \vee B) \vee C) \leftrightarrow (A \vee (B \vee C))$;
(11) $(A \vee A) \leftrightarrow A$;
(12) $(A\&(B \vee C)) \leftrightarrow ((A \vee C)\&(B \vee C))$;
(13) $(A \vee (B\&C)) \leftrightarrow ((A\&C) \vee (B\&C))$;
(14) $(\neg(A\&B)) \leftrightarrow (\neg A \vee \neg B)$;
(15) $(\neg(A \vee B)) \leftrightarrow (\neg A\&\neg B)$;
(16) $(\neg(\neg A)) \leftrightarrow A$;
(17) $(A\&(B \vee \neg B)) \leftrightarrow A$;
(18) $(A \vee (B\&\neg B)) \leftrightarrow A$.

Правило подстановки. *Пусть $F(A_1, A_2, \ldots, A_m)$ — тавтология, и пусть Y_1, Y_2, ... ,Y_m — произвольные высказывания; тогда высказывание, полученное из $F(A_1, A_2, \ldots, A_m)$ подстановкой вместо каждого вхождения букв A_1, A_2, ... , A_m соответствующих высказываний $Y_1, Y_2, \ldots, Y_m$, является тавтологией.*

Теорема. *Любая тавтология может быть получена из тавтологий (1)-(18) при помощи правил подстановки и силлогизма.*

Мы опускаем доказательство этой теоремы: она нам не понадобится.

Следствие. *Пусть S — некоторое множество высказываний. Любое высказывание, выводимое из S, может быть получено из тавтологий (1)-(18) и из суждений, принадлежащих S, многократным применением правил подстановки и силлогизма.*

1.9. Непротиворечивость. Будем говорить, что множество S высказываний противоречиво, если тождественно ложное высказывание "л" выводимо из S, т.е. $S \vdash$ л. Если же тождественно ложное высказывание не выводимо из S, то множество высказываний S называется непротиворечивым. Из теоремы §1.7 следует, что множество высказываний S противоречиво тогда и только тогда, когда дуальный идеал, порожденный классами всех высказываний из S, содержит 0. Но тогда этот дуальный идеал содержит также любой элемент $x = 0 \cdot y + x$ булевой алгебры высказываний $\mathfrak{X}$, т.е. он совпадает с $\mathfrak{X}$. Таким образом, из противоречивого множества высказываний выводимо любое высказывание.

2. Исчисление предикатов

2.1. Предикаты на множестве. Как и в §1.1, в этом пункте мы не стремимся к полной строгости; наша цель — дать интуитивное представление о тех понятиях, которые будут формализованы ниже. Пусть M — некоторое множество, и пусть для каждого набора $c_1, \ldots, c_n \in M$ задано высказывание $P(c_1, \ldots, c_n)$. Мы говорим тогда, что P — n-местный предикат на множестве M. Для любых $c_1, \ldots, c_n \in M$ высказывание $P(c_1, \ldots, c_n)$ истинно или ложно; предикат P полностью определяется заданием множества $P_M \subseteq M^n$ всех тех наборов $(c_1, \ldots, c_n) \in M^n$, для которых высказывание $P(c_1, \ldots, c_n)$ истинно.

Приведем несколько примеров предикатов, из которых станет ясно, что на языке предикатов можно выразить многие математические соотношения.

Предикат сложения. Высказывание $P(a, b, c)$ истинно тогда и только тогда, когда $a + b = c$.

Предикат строгого неравенства. Высказывание $P(a,b)$ истинно тогда и только тогда, когда $a < b$.

Предикат равенства. Высказывание $P(a,b)$ истинно тогда и только тогда, когда $a = b$. Поскольку предикат равенства играет особую роль, мы будем обозначать его привычным образом, т.е. записывать высказывание не в виде $P(a,b)$, а в виде "$a = b$".

Из высказываний, связанных с предикатами, можно по правилам исчисления высказываний строить новые высказывания. Например, если $P(c_1,c_2,c_3)$, $Q(c)$, $R(c_1,c_2)$ — предикаты на множестве M, и $a,b,c \in M$, то можно составить высказывания $(P(a,b,b)\&\neg Q(a)) \vee R(b,a)$, $((a=c)\&Q(b)) \to P(a,b,c)$ и др.

Как и выше, наряду с самими высказываниями можно рассматривать связанную с ними алгебру высказываний. Пусть, например, на множестве M заданы предикаты равенства и предикаты P, Q, R из предыдущего абзаца; рассмотрим алгебру высказываний $\mathfrak{A}$, свободно порожденную всеми высказываниями видов $(a=b)$, $P(a,b,c)$, $Q(a)$, $R(a,b)$, где элементы a, b, c независимо пробегают множество M. Точнее говоря,

(1) и, л $\in \mathfrak{A}$;
(2) выражения $(a=b)$, $P(a,b,c)$, $Q(a)$, $R(a,b)$ принадлежат $\mathfrak{A}$ для любых $a,b,c \in M$;
(3) если $A,B \in \mathfrak{A}$, то $(A\&B)$, $(A\vee B)$, $(A \to B)$, $(A \leftrightarrow B)$, $(\neg A)$ принадлежат $\mathfrak{A}$.

Никакое выражение, которое не может быть получено по указанным правилам, не входит в $\mathfrak{A}$.

Отметим, однако, существенную разницу с алгеброй высказываний из §1.2: там элементарные высказывания X_i могли иметь любые значения истинности, в то время как высказывание $(a=a)$ обязательно истинно. Кроме того, истинными являются и составные высказывания вида $(a=a_1) \to (R(a,b) \to R(a_1,b))$ и другие подобные им высказывания. Это, конечно, связано с тем, что в число предикатов мы включили предикат равенства, обладающий специфическими свойствами, в том числе, свойством: $a=a$ для любого $a \in M$.

Тот факт, что наши высказывания зависят от параметров, пробегающих множество M, позволяет формулировать суждения другого типа. Пусть некоторое высказывание $A(c_1,\ldots,c_n)$ зависит от параметров $c_1,\ldots,c_n$; пусть, далее, это высказывание истинно не только в случае, когда первый параметр равен c_1, но и при любом его значении $c \in M$ (и тех же значениях остальных параметров). В этой ситуации мы будем переменный первый параметр обозначать x, а утверждение о том, что высказывание справедливо при любом значении x записывать так: $\forall x(A(x,c_2,\ldots,c_n))$. Аналогично, если среди высказываний $A(c,c_2,\ldots,c_n)$, $c \in M$, есть хоть одно верное, будем писать: $\exists x(A(x,c_2,\ldots,c_n))$.

Введенные только что символы $\forall$ и $\exists$ называются квантором всеобщности и квантором существования. Отметим, что в случае конечного множества M в них нет необходимости: утверждение $\forall x(A(x,c_2,\ldots,c_n))$ равносильно высказыванию $\bigwedge\limits_{c\in M} A(c,c_2,\ldots,c_n)$, а утверждение $\exists x(A(x,c_2,\ldots,c_n))$ — высказыванию $\bigvee\limits_{c\in M} A(c,c_2,\ldots,c_n)$. Однако, для бесконечных множеств, и тем более в

ситуации, когда множество M не зафиксировано, не удается свести кванторы к операциям исчисления высказываний.

2.2. Исчисление предикатов. В этом пункте мы строим формальную систему, в которую вкладываются содержательные рассмотрения предыдущего пункта. Как и в §1.2, предметом нашего рассмотрения являются слова в некотором конечном алфавите. На сей раз алфавит состоит из букв

$$,\ (\ )\ =\ \&\ \vee\ \neg\ \to\ \leftrightarrow\ \forall\ \exists\ c_n\ x_n\ P_n\ \text{и}\ \text{л}$$

($n = 1, 2, \dots$). Этот алфавит бесконечен, но при желании его можно свести к конечному алфавиту, введя вместо трех бесконечных серий букв три буквы c, x, P и еще одну букву $'$ и обозначив $c_1 = c$, $x_1 = x$, $P_1 = P$, $c_2 = c'$, $x_3 = x''$ и т.д. Буквы c_i будем называть символами констант, буквы x_i — символами переменных, буквы P_i — символами предикатов. В дальнейшем мы обычно не будем строго следовать этой системе обозначений и будем использовать буквы $c, d, \dots$ (возможно, с индексами) для записи символов констант, буквы $x, y, z, \dots$ — для записи символов переменных, буквы $P, Q, R \dots$ — для записи символов предикатов. Каждому символу предиката соотнесем натуральное число; если символу P соответствует число n, то говорим, что P — символ n-местного предиката.

Не все слова представляют для нас интерес: некоторые из них — просто бессмысленные наборы букв. Следующее определение вводит сразу два понятия: осмысленное выражение и свободное или связанное вхождение символа переменной в осмысленное выражение.

Определение.

(1) "и" *и* "л" — *осмысленные выражения;*

(2) $(x = y)$, $(x = c)$, $(c = d)$ — *осмысленные выражения, и все вхождения символов переменных в них свободные;*

(3) *если* P — *символ* n*-местного предиката, и каждая из букв* $t_1, \dots, t_n$ *обозначает символ переменной или символ константы, то* $P(t_1, \dots, t_n)$ — *осмысленное выражение, и все вхождения символов переменных в него свободны;*

(4) *если* A, B — *осмысленные выражения, то* $(A\&B)$, $(A \vee B)$, $(A \to B)$, $(A \leftrightarrow B)$, $(\neg A)$ — *тоже осмысленные выражения; при этом каждое свободное (связанное) вхождение символа переменной в* A *или* B *остается свободным (связанным) и в* $(A\&B)$, $(A \vee B)$, $(A \to B)$, $(A \leftrightarrow B)$, $(\neg A)$;

(5) *если* A — *осмысленное выражение, все вхождения символа переменной* x *в которое свободны, то* $(\forall x A)$ *и* $(\exists x A)$ — *осмысленные выражения, все вхождения символа переменной* x *в которые связанные, а вхождения остальных переменных — такие же, как в* A.

Никакое выражение, которое не может быть получено по указанным правилам, не является осмысленным.

Как и в исчислении высказываний, некоторые скобки в осмысленных выражениях мы будем для краткости опускать без ущерба для их понимания: эти скобки могут быть восстановлены единственным естественным образом.

Прежде, чем сформулировать следующее определение, рассмотрим ситуацию, несколько напоминающую нашу. Пусть $f(x)$ — некоторая функция натурального аргумента. Тогда выражения $\sum\limits_{s=1}^{n} f(s)$, $\sum\limits_{t=1}^{n} f(t)$ являются функциями только от верхнего предела суммирования n и не зависят от "связанных переменных" s, t. Поэтому обычно эти два выражения отождествляются, хотя и являются графически различными. Аналогичное отождествление произведем и для осмысленных выражений.

Определение. *Пусть A, A_1 — осмысленные выражения; будем считать, что $A \equiv A_1$, если A можно преобразовать в A_1, применив несколько раз следующие правила* (1)-(3).

(1) *Если A — осмысленное выражение, то $A \equiv A$.*

(2) *если A, B, A_1, B_1 — осмысленные выражения, и $A \equiv A_1$, $B \equiv B_1$, то $(A\&B) \equiv (A_1\&B_1)$, $(A \vee B) \equiv (A_1 \vee B_1)$, $(A \to B) \equiv (A_1 \to B_1)$, $(A \leftrightarrow B) \equiv (A_1 \leftrightarrow B_1)$, $(\neg A) \equiv (\neg A_1)$.*

(3) *если $A(x)$ — осмысленное выражение, y — символ переменной, не входящей свободно в $A(x)$ и $A(y)$ — выражение, получающееся из слова $A(x)$ заменой всех свободных вхождений символа переменной x на символ переменной y, то $(\forall x A(x)) \equiv (\forall y A(y))$, $(\exists x A(x)) \equiv (\exists y A(y))$.*

Иначе говоря, $A \equiv A_1$, если слово A_1 получается из слова A заменой связанных вхождений символов переменных на другие символы переменных, причем должны соблюдаться некоторые правила предосторожности. В частности, все вхождения символа переменной, связанных одним квантором, должны заменяться на одну и ту же букву.

Если A, A_1 — осмысленные выражения, и $A \equiv A_1$, то мы отождествляем выражения A, A_1, полагая, что это — две записи одного и того же осмысленного выражения.

Осмысленное выражение, в которое ни один символ переменной не входит свободно, называется суждением.

2.3. Интерпретации символов констант и предикатов. Модели. Содержательное описание исчисления предикатов из §2.1 получается из формальной схемы предыдущего пункта при интерпретировании символов констант и предикатов в некотором множестве. Пусть $\mathfrak{C}$ — множество символов констант, а $\mathfrak{P}$ — множество символов предикатов. Для самого исчисления предикатов $\mathfrak{C} = \{c_1, c_2, \dots\}$, $\mathfrak{P} = \{P_1, P_2, \dots\}$; однако в дальнейшем мы будем допускать в качестве $\mathfrak{C}$ и $\mathfrak{P}$ любые множества, поскольку основные содержательные результаты не зависят от конкретного вида множеств символов констант и предикатов. Пусть M — множество, и пусть каждому символу константы $c \in \mathfrak{C}$ сопоставлен элемент $c_M \in M$, а каждому символу n-местного предиката $P \in \mathfrak{P}$ сопоставлено подмножество P_M n-й декартовой степени M^n множества M. Набор, состоящий из множества M, элементов c_M ($c \in \mathfrak{C}$) и подмножеств P_M ($P \in \mathfrak{P}$) называется интерпретацией множеств символов констант $\mathfrak{C}$ и символов предикатов $\mathfrak{P}$.

Пусть $A = A(x_1, \dots, x_N)$ — осмысленное выражение со свободными символами переменных $x_1, \dots, x_N$, в записи которого использованы только символы

констант из $\mathfrak{C}$ и символы предикатов из $\mathfrak{P}$; для любых элементов $m_1, \ldots, m_N$ присвоим выражению $A(m_1, \ldots, m_N)$ значение истинности в интерпретации $\{M; c_M, P_M\}$. Присвоение значения истинности проведем индукцией по построению выражения A. Выражения $c = d$, $c = m$, $m = m'$, где $c, d \in \mathfrak{C}$, $m, m' \in M$, истинны в интерпретации M тогда и только тогда, когда, соответственно, $c_M = d_M$ или $c_M = m$ или $m = m'$. Выражение $P(t_1, \ldots, t_n)$, в котором каждый символ t_i означает или элемент из M, или символ константы из $\mathfrak{C}$, истинно в интерпретации M тогда и только тогда, когда $(m_1, \ldots, m_n) \in P_M$, где $m_i = t_i$, если t_i — элемент из M, и $m_i = (t_i)_M$, если $t_i \in \mathfrak{C}$ — символ константы. Значения истинности выражений $A\&B$, $A \vee B$, $A \to B$, $A \leftrightarrow B$, $\neg A$ определяются по правилам исчисления высказываний. Если выражение $A(x_1, \ldots, x_N)$ имеет вид $\forall x B(x, x_1, \ldots, x_N)$, то выражение $A(m_1, \ldots, m_N)$ считается истинным тогда и только тогда, когда выражение $B(m, m_1, \ldots, m_N)$ истинно для любого $m \in M$. Наконец, если выражение $A(x_1, \ldots, x_N)$ имеет вид $\exists x B(x, x_1, \ldots, x_N)$, то выражение $A(m_1, \ldots, m_N)$ считается истинным тогда и только тогда, когда найдется такой элемент $m \in M$, что выражение $B(m, m_1, \ldots, m_N)$ истинно.

Начиная отсюда, для множества символов предикатов $\mathfrak{P}$ и множества символов констант $\mathfrak{C}$ будем обозначать через $\mathfrak{A}(\mathfrak{P}, \mathfrak{C})$ множество всех суждений, в записи которых участвуют лишь символы предикатов, принадлежащие $\mathfrak{P}$, и символы констант, принадлежащие $\mathfrak{C}$. Иногда мы будем опускать упоминание о множестве символов предикатов и писать $\mathfrak{A}(\mathfrak{C})$ вместо $\mathfrak{A}(\mathfrak{P}, \mathfrak{C})$. Пусть $\mathfrak{S} \in \mathfrak{A}(\mathfrak{P}, \mathfrak{C})$ — некоторое множество суждений. Интерпретация $\{M; c_M, P_M\}$ множеств символов констант $\mathfrak{C}$ и символов предикатов $\mathfrak{P}$ называется моделью $\mathfrak{S}$, если все суждения из $\mathfrak{S}$ истинны в этой интерпретации.

Обычная формальная аксиоматическая теория строится следующим образом: задаются множества символов констант $\mathfrak{C}$ и символов предикатов $\mathfrak{P}$ и некоторое множество суждений $\mathfrak{S} \in \mathfrak{A}(\mathfrak{P}, \mathfrak{C})$, называемых аксиомами, и изучаются всевозможные утверждения, которые можно вывести из аксиом при помощи правил вывода, изложенных выше, а также всевозможные модели системы аксиом. В качестве примера рассмотрим аксиоматическую теорию с одним символом констант e и одним 3-местным символом предиката P со следующей системой аксиом:

(1) $\forall x \forall y \exists z P(x, y, z)$;
(2) $\forall x \forall y \forall z \forall t((P(x, y, z) \& P(x, y, t)) \to (z = t))$;
(3) $\forall x \forall y \forall z \forall t \forall u \forall v \forall w((P(x, y, t) \& P(t, z, u) \& P(y, z, v) \& P(x, v, w)) \to (u = w))$;
(4) $\forall x(P(x, e, x) \& P(e, x, x))$;
(5) $\forall x \exists y(P(x, y, e) \& P(y, x, e))$.

Пусть G — любая модель этой системы аксиом. Соотношение $P(x, y, z)$ запишем в виде $xy = z$; первая аксиома означает, что для любых двух элементов $x, y \in G$ существует их произведение $z = xy$, а вторая аксиома показывает, что это произведение определено однозначно. Таким образом, G является множеством с одной бинарной операцией умножения. Остальные аксиомы утверждают, что это умножение ассоциативно, что e является единицей для него и что всякий элемент из G обратим. Таким образом, моделями множества аксиом (1)-(5) являются группы.

2.4. Универсально верные суждения. В исчислении высказываний мы выделили класс тавтологий — суждений, истинных при любых значениях истинности элементарных высказываний. Точно так же, универсально верными суждениями в исчислении предикатов назовем такие суждения, которые истинны при любой интерпретации символов констант и предикатов, входящих в запись этих суждений. В этом пункте мы опишем несколько способов построения универсально верных суждений. *A priori* не ясно, достаточно ли этих правил для построения всех универсально верных суждений, и поэтому мы пока будем называть суждения, полученные по этим правилам, выводимыми (точнее, выводимыми из пустого множества суждений).

(1) *Правило подстановки.* Пусть $F(X_1, X_2, \ldots, X_m)$ — тавтология исчисления высказываний, и пусть Y_1, Y_2, ... ,Y_m — произвольные суждения; тогда суждение, полученное из $F(X_1, X_2, \ldots, X_m)$ подстановкой вместо каждого вхождения букв X_1, X_2, ... , X_m соответствующих суждений Y_1, Y_2, ... ,Y_m, выводимо.

(2) *Modus ponens.* Если суждения X, $X \to Y$ выводимы, то и суждение Y выводимо.

Перед тем, как сформулировать другие правила построения универсально верных суждений, введем одно полезное обозначение. Пусть $A(t)$ — осмысленное выражение, а t — символ константы или переменной, и пусть c – символ константы; через $A(c)$ мы будем обозначать слово, получающееся из слова $A(t)$ заменой всех свободных вхождений t, если t — символ переменной, или всех вхождений t, если t — символ константы, на символ c.

(3) Суждения $(c = c)$, $(c = d) \to (d = c)$, $((c = d)\&(d = e)) \to (c = e)$ выводимы.

(4) Если $A(c)$ — любое суждение, то $(c = d) \to (A(c) \to A(d))$ — выводимое суждение.

(5) Пусть $A(x)$ — осмысленное выражение, в которое свободно входит только символ переменной x, B — любое суждение; тогда

$$(\forall x A(x)) \to A(c),$$
$$(\neg(\forall x A(x))) \leftrightarrow (\exists x(\neg A(x))),$$
$$((\forall x A(x))\&B) \leftrightarrow (\forall x(A(x\&B))),$$
$$((\exists x A(x))\&B) \leftrightarrow (\exists x(A(x\&B)))$$

— выводимые суждения.

Наконец, отметим еще один, принципиально отличный от предыдущих, способ построения выводимых суждений. Для того, чтобы обосновать его, дадим сначала его интуитивный смысл. Ясно, что если суждение $\forall x A(x)$ верно, то для любого символа константы должно быть верно и суждение $A(c)$; нам хотелось бы, чтобы и обратно, если суждение $A(c)$ верно для всех символов констант, то было бы верно и суждение $\forall x A(x)$. Но верно для всех символов констант — это то же самое, что верно для произвольного символа константы. Мы приходим к следующему правилу построения выводимых суждений.

(6) Пусть $A(x)$ — осмысленное выражение с единственным символом переменной x, входящим в него свободно. Если c — символ константы,

не входящий в $A(x)$, и суждение $A(c)$ выводимо, то и суждение $\forall x A(x)$ выводимо.

Еще раз отметим, что в последнем правиле c — символ константы, не связанный никакими дополнительными ограничениями; вообще говоря, суждение $((A(c)) \to (\forall x A(x)))$ не обязано быть верным.

Теорема. *Всякое выводимое суждение является универсально верным (т.е. истинным при любой интерпретации символов констант и предикатов). Обратно, всякое универсально верное суждение выводимо.*

Доказательство. Докажем, что суждения, построенные по правилам (1)-(6), универсально верны. Напомним, что суждения являются высказываниями; правила (1) и (2) как раз и являются переформулировками соответствующих правил исчисления высказываний. Совершенно очевидно, что по правилам (3)-(5) получаются суждения, истинные при любой интерпретации символов констант и предикатов. Осталось показать, что и по правилу (6) получаются универсально верные суждения. Пусть $\{M; c_M, P_M\}$ — любая интерпретация множеств констант и предикатов, и пусть $m \in M$. Предположим, что мы уже убедились в универсальной верности выводимого суждения $A(c)$. Значение истинности выражения $A(m)$ в интерпретации M совпадает совпадает со значением истинности суждения $A(c)$ в интерпретации, отличающейся от интерпретации M только тем, что символу константы c ставится в соответствие не элемент c_M, а элемент m. Но суждение $A(c)$ истинно в любой интерпретации; поэтому выражение $A(m)$ истинно в интерпретации M для любого $m \in M$, т.е. суждение $\forall x A(x)$ истинно в интерпретации M.

Обратное утверждение значительно глубже и будет доказано ниже как следствие теоремы Геделя о полноте.

2.5. Непротиворечивость. Теорема Геделя о полноте. Пусть теперь $\mathfrak{S}$ — некоторое множество суждений; мы говорим, что суждение A выводимо из $\mathfrak{S}$, если существуют суждения $X_1, \ldots, X_m \in \mathfrak{S}$, такие что суждение $(X_1 \& \ldots \& X_m) \to A$ выводимо (т.е. выводимо из пустого множества суждений). Система суждений $\mathfrak{S}$ называется непротиворечивой, если тождественно ложное суждение "л" не выводимо из $\mathfrak{S}$.

Ясно, что если для множества суждений существует модель, то это множество суждений непротиворечиво. Оказывается, верно и обратное.

Теорема Геделя о полноте. *Пусть $\mathfrak{S} \subseteq \mathfrak{A}(\mathfrak{P}, \mathfrak{C})$ — некоторое непротиворечивое множество суждений. Тогда существует модель этого множества суждений. Более того, если множества $\mathfrak{P}$, $\mathfrak{C}$ конечны, то существует не более чем счетная модель $\mathfrak{S}$, а если хотя бы одно из них бесконечно, существует модель множества $\mathfrak{C}$, мощность которой не превосходит максимума мощностей множеств $\mathfrak{P}$, $\mathfrak{C}$.*

Доказательство этой теоремы будет дано в следующем параграфе.

То же самое ограничение на мощность, что и в теореме Геделя, будет встречаться у нас еще несколько раз. Для сокращения речи будем называть множества, мощность которых удовлетворяет этому условию, множествами малой мощности (по отношению к множествам символов констант и предикатов $\mathfrak{C}$,

$\mathfrak{P}$). В этих терминах теорема Геделя гарантирует существование модели малой мощности.

В следующих пунктах мы укажем несколько важных следствий теоремы Геделя.

2.6. Выводимость и существование модели.

Теорема. *Пусть* $\mathfrak{X} \subseteq \mathfrak{A}(\mathfrak{C}, \mathfrak{P})$ — *непротиворечивое множество суждений. Если суждение* $A \in \mathfrak{A}(\mathfrak{C}, \mathfrak{P})$ *не выводимо из* $\mathfrak{X}$, *то существует модель множества суждений* $\mathfrak{X}$, *в которой суждение* A *ложно. Иначе говоря, суждение* $A \in \mathfrak{A}(\mathfrak{C}, \mathfrak{P})$ *выводимо из* $\mathfrak{X}$ *тогда и только тогда, когда оно истинно во всех моделях множества суждений* $\mathfrak{X}$. *В частности, суждение выводимо (т.е. выводимо из пустого множества) тогда и только тогда, когда оно универсально верно.*

Доказательство. Заметим сначала, что высказывание

$$((X_2 \& \neg X_1) \to (\text{л})) \to (X_2 \to X_1)$$

тождественно истинно. Пусть суждение $A \in \mathfrak{A}(\mathfrak{C}, \mathfrak{P})$ не выводимо из $\mathfrak{X}$. Если бы множество суждений $\mathfrak{X} \cup \{\neg A\}$ было противоречивым, то существовало бы конечное множество суждений $Y_1, \ldots, Y_n \in \mathfrak{X}$, такое что суждение $(Y_1 \& \ldots \& Y_n \& \neg A) \to (\text{л})$ было бы выводимым. Подставляя в указанное выше тождественно истинное высказывание суждение $Y_1 \& \ldots \& Y_n$ вместо X_2 и A вместо X_1 и пользуясь *modus ponens*, мы увидели бы, что $(Y_1 \& \ldots \& Y_n) \to A$ — выводимое суждение , т.е. что суждение A выводимо из $\mathfrak{X}$ вопреки предположению. Итак, множество суждений $\mathfrak{X} \cup \{\neg A\}$ непротиворечиво, и по теореме Гёделя о полноте существует его модель. Эта модель является моделью множества суждений $\mathfrak{X}$, но суждение A в этой модели ложно, поскольку в ней выполняется суждение $\neg A$.

Последнее утверждение только что доказанной теоремы показывает, что для построения всех универсально верных суждений достаточно пользоваться лишь правилами (1)-(6). Иначе говоря, эти правила составляют полную систему правил вывода универсально верных суждений; этим объясняется название теоремы Геделя: это по существу теорема о полноте системы правил вывода (1)-(6).

2.7. Теорема компактности.

Теорема. *Если для всякого конечного подмножества множества суждений* $\mathfrak{X} \subseteq \mathfrak{A}(\mathfrak{C}, \mathfrak{P})$ *существует модель, то существуют и модель всего множества суждений* $\mathfrak{X}$.

Доказательство. Если бы множество суждений $\mathfrak{X}$ было противоречивым, то существовали бы суждения $X_1, \ldots, X_n \in \mathfrak{X}$, такие что суждение

$$(X_1 \& \ldots \& X_n) \to (\text{л})$$

было бы выводимым. Но тогда было бы противоречивым уже конечное множество суждений $\{X_1, \ldots, X_n\} \subseteq \mathfrak{X}$, и для него не существовало бы модели, что противоречит предположению теоремы. Следовательно, множество суждений $\mathfrak{X}$ непротиворечиво, и по теореме Гёделя о полноте существует модель этого множества суждений.

2.8. Существование сколь угодно больших моделей.

Теорема. *Если для множества суждений $\mathfrak{X} \subseteq \mathfrak{A}(\mathfrak{C}, \mathfrak{P})$ существует бесконечная модель или даже сколь угодно большие конечные модели, то существуют и модели множества суждений $\mathfrak{X}$ сколь угодно большой мощности.*

Доказательство. Расширим множество символов констант $\mathfrak{C}$, добавив к нему произвольное множество $\mathfrak{D}$. Обозначим через $\mathfrak{X}' \subseteq \mathfrak{A}(\mathfrak{C} \cup \mathfrak{D}, \mathfrak{P})$ множество суждений, полученное из $\mathfrak{X}$ добавлением суждений $\neg(d = d')$ для всех пар $d, d' \in \mathfrak{D}$, $d \neq d'$.

Каждое конечное подмножество $\mathfrak{Y}$ множества $\mathfrak{X}'$ допускает модель. Действительно, в $\mathfrak{Y}$ участвует лишь конечное число элементов $d_1, \ldots, d_m \in \mathfrak{D}$. По условию, существует модель M множества суждений $\mathfrak{X}$, состоящая не менее чем из m элементов; сопоставляя символам констант $d_1, \ldots, d_m$ различные элементы из множества M, мы превратим M в интерпретацию множества символов констант $\mathfrak{C} \cup \{d_1, \ldots, d_m\}$ и символов предикатов $\mathfrak{P}$, в которой истинны все суждения из $\mathfrak{X}$ и суждения $\neg(d_i = d_j)$, $1 \leq i, j \leq m$, $i \neq j$. В частности, в M выполнены все суждения из $\mathfrak{Y}$, так что M — модель множества суждений $\mathfrak{Y}$.

По теореме компактности существует и модель M' всего множества суждений $\mathfrak{X}'$; очевидно, она является моделью множества суждений $\mathfrak{X}$, а её мощность не меньше мощности множества $\mathfrak{D}$, так как всем символам констант из $\mathfrak{D}$ должны соответствовать различные элементы из M'.

3. Доказательство теоремы Гёделя о полноте

3.1. Максимальные непротиворечивые и экзистенциально полные множества суждений. Определим два важных класса множеств суждений. Подмножество $\mathfrak{S}$ множества суждений $\mathfrak{A}(\mathfrak{P}, \mathfrak{C})$ называется экзистенциально полным, если для любого суждения вида $\exists x(A(x))$, принадлежащего $\mathfrak{S}$, найдется символ константы $c \in \mathfrak{C}$, такой что суждение $A(c)$ тоже принадлежит множеству $\mathfrak{S}$ (здесь, как обычно, $A(x)$ — осмысленное выражение, в которое свободно входит только символ переменной x).

Множество суждений $\mathfrak{S} \subseteq \mathfrak{A}(\mathfrak{P}, \mathfrak{C})$ называется максимальным непротиворечивым подмножеством $\mathfrak{A}(\mathfrak{P}, \mathfrak{C})$, если множество суждений $\mathfrak{S}$ непротиворечиво, но любое его собственное расширение уже не является непротиворечивым.

Предложение. *Пусть $\mathfrak{S}$ — максимальное непротиворечивое подмножество $\mathfrak{A}(\mathfrak{P}, \mathfrak{C})$, и пусть A — любое суждение из $\mathfrak{A}(\mathfrak{P}, \mathfrak{C})$. Тогда одно, и только одно, из суждений A, $\neg A$ содержится в $\mathfrak{S}$. Если суждение A выводимо из $\mathfrak{S}$, то $A \in \mathfrak{S}$. В частности, все выводимые суждения (т.е. суждения, выводимые из пустого множества суждений) принадлежат $\mathfrak{S}$.*

Доказательство. Оба суждения A, $\neg A$ не могут содержаться в непротиворечивом множестве $\mathfrak{S}$, так как в противном случае тождественно ложное суждение $A\&\neg A$ было бы выводимо из $\mathfrak{S}$, что несовместимо с непротиворечивостью $\mathfrak{S}$. Пусть $A, \neg A \notin \mathfrak{S}$; поскольку $\mathfrak{S}$ — максимальное непротиворечивое множество, оба множества суждений $\mathfrak{S} \cup \{A\}$, $\mathfrak{S} \cup \{\neg A\}$ не являются непротиворечивыми. Поэтому существуют суждения $B_1, \ldots, B_m, B_{m+1}, \ldots, B_n \in \mathfrak{B}$, такие

что суждения

$$(A\&B_1\&\ldots\&B_m)\to(\text{л}),\quad (\neg A\&B_{m+1}\&\ldots\&B_n)\to(\text{л})$$

выводимы. Далее, высказывание

$$(((X\&Y)\to(\text{л}))\&((\neg X\&Z)\to(\text{л})))\to((Y\&Z)\to(\text{л}))$$

является, как нетрудно выяснить, вычисляя функцию истинности, тавтологией. Подставляя сюда A, $B_1\&\ldots\&B_m$ и $B_{m+1}\&\ldots\&B_n$ вместо X, Y, Z и пользуясь *modus ponens*, находим, что и суждение

$$(B_1\&\ldots\&B_m\&B_{m+1}\&\ldots\&B_n)\to(\text{л})$$

выводимо, а это означает, что $\mathfrak{S}$ — противоречивое множество суждений. Следовательно, предположение о том, что ни суждение A, ни суждение $\neg A$ не принадлежат $\mathfrak{S}$, было неверно.

Если суждение A выводимо из $\mathfrak{S}$ и $A\notin\mathfrak{S}$, то, как мы только что доказали, суждение $\neg A$ принадлежит $\mathfrak{S}$; таким образом, оба суждения A, $\neg A$ выводимы из $\mathfrak{S}$, а потому и тождественно ложное суждение $A\&\neg A$ выводимо из $\mathfrak{S}$ вопреки непротиворечивости множества суждений $\mathfrak{S}$.

3.2. Интерпретации максимальных непротиворечивых экзистенциально полных множеств суждений.

Теорема. *Пусть $M=\{M;c_M,P_M\}$ — интерпретация множеств символов констант $\mathfrak{C}$ и символов предикатов $\mathfrak{P}$, такая что для любого элемента $m\in M$ существует символ константы $c\in\mathfrak{C}$, для которого $m=c_M$. Множество $\mathfrak{S}$ всех суждений из $\mathfrak{A}(\mathfrak{P},\mathfrak{C})$, истинных в интерпретации M, является максимальным непротиворечивым и экзистенциально полным. Обратно, пусть $\mathfrak{S}\subseteq\mathfrak{A}(\mathfrak{P},\mathfrak{C})$ — максимальное непротиворечивое и экзистенциально полное множество суждений; тогда существует такая интерпретация $M=\{M;c_M,P_M\}$ множеств $\mathfrak{C}$, $\mathfrak{P}$, что для любого элемента $m\in M$ существует символ константы $c\in\mathfrak{C}$, для которого $m=c_M$, и суждение из $\mathfrak{A}(\mathfrak{P},\mathfrak{C})$ истинно в M тогда и только тогда, когда оно содержится в множестве $\mathfrak{S}$.*

Доказательство. Пусть сначала $\mathfrak{S}$ — множество всех суждений из $\mathfrak{A}(\mathfrak{P},\mathfrak{C})$, истинных в интерпретации M. Ясно, что оно непротиворечиво. Если суждение $A\in\mathfrak{A}(\mathfrak{P},\mathfrak{C})$ не принадлежит $\mathfrak{S}$, то оно не истинно в интерпретации M; это значит, что его отрицание $\neg A$ истинно в M и потому принадлежит $\mathfrak{S}$. Таким образом, множество суждений $\mathfrak{S}\cup\{A\}$ содержит одновременно суждения A, $\neg A$, и потому противоречиво. Следовательно, $\mathfrak{S}$ — *максимальное* непротиворечивое множество суждений. Далее, если суждение $\exists x(A(x))$ принадлежит $\mathfrak{S}$, то оно истинно в M, т.е. найдется символ константы $c\in\mathfrak{C}$, такой что суждение $A(c)$ (точнее, суждение $A(c_M)$) истинно в M и потому принадлежит множеству $\mathfrak{S}$. Итак, множество суждений $\mathfrak{S}$ экзистенциально полно.

Сложнее доказывается обратное утверждение. Пусть $\mathfrak{S}\subseteq\mathfrak{A}(\mathfrak{P},\mathfrak{C})$ — максимальное непротиворечивое и экзистенциально полное множество суждений. Две константы $c,d\in\mathfrak{C}$ будем считать эквивалентными и писать $c\sim d$, если суждение $c=d$ содержится в $\mathfrak{S}$.

Лемма 1. *Отношение $c \sim d$ является отношением эквивалентности на множестве $\mathfrak{C}$. Если P — символ n-местного предиката, $c_1, \ldots, c_n, d_1, \ldots, d_n \in \mathfrak{C}$, $c_1 \sim d_1$, ... , $c_n \sim d_n$ и суждение $P(c_1, \ldots, c_n)$ содержится в $\mathfrak{S}$, то и суждение $P(d_1, \ldots, d_n)$ содержится в $\mathfrak{S}$.*

Доказательство. Суждение $c = c$ выводимо и потому принадлежит $\mathfrak{S}$; значит, $c \sim c$. Если $c \sim d$, то суждение $c = d$ принадлежит $\mathfrak{S}$, и из него и выводимого суждения $(c = d) \to (d = c)$, тоже принадлежащего $\mathfrak{S}$, по *modus ponens* выводится суждение суждение $d = c$. По предложению из предыдущего пункта суждение $d = c$ тоже принадлежит $\mathfrak{S}$, т.е. $d \sim c$. Точно так же, если $c \sim d$, $d \sim e$, то суждения $c = d$, $d = e$ вместе с выводимым суждением $((c = d)\&(d = e)) \to (c = e)$ принадлежат $\mathfrak{S}$; по предложению из предыдущего пункта выводимое из них суждение $c = e$ тоже принадлежат $\mathfrak{S}$, т.е. $c \sim e$. Итак, отношение $\sim$ является эквивалентностью.

Аналогично доказывается и второе утверждение леммы. Если $c_1 \sim d_1$, ... , $c_n \sim d_n$, то суждения $c_1 = d_1$, ... , $c_n = d_n$ принадлежат $\mathfrak{S}$. Из них, суждения $P(c_1, c_2, \ldots, c_n)$ и выводимых суждений

$$(c_1 = d_1) \to (P(c_1, c_2, \ldots, c_n) \to P(d_1, c_2, \ldots, c_n)),$$
$$(c_2 = d_2) \to (P(d_1, c_2, \ldots, c_n) \to P(d_1, d_2, \ldots, c_n)), \ldots,$$
$$(c_n = d_n) \to (P(d_1, d_2, \ldots, c_n) \to P(d_1, d_2, \ldots, d_n))$$

последовательно выводятся суждения $P(d_1, c_2, \ldots, c_n)$, $P(d_1, d_2, \ldots, c_n)$, ... , $P(d_1, d_2, \ldots, d_n)$. По предложению из предыдущего пункта последнее суждение $P(d_1, d_2, \ldots, d_n)$ принадлежит $\mathfrak{S}$.

Обозначим через M множество классов эквивалентности множества $\mathfrak{C}$ по отношению $\sim$. Для каждого символа константы $c \in C$ обозначим через c_M класс эквивалентности элемента c, а для каждого символа n-местного предиката $P \in \mathfrak{P}$ обозначим через P_M подмножество декартовой степени M^n, состоящее из всех таких наборов $(m_1, \ldots, m_n)$, что суждение $P(c_1, \ldots, c_n)$ принадлежит $\mathfrak{S}$ для любых элементов $c_1, \ldots, c_n \in \mathfrak{C}$, классы эквивалентности которых равны соответственно $m_1, \ldots, m_n \in M$. Таким образом, элементы c_M и множества P_M составляют интерпретацию множества суждений $\mathfrak{S} \subseteq \mathfrak{A}(\mathfrak{P}, \mathfrak{C})$.

Для доказательства теоремы осталось показать, что значения истинности суждения $A \in \mathfrak{A}(\mathfrak{P}, \mathfrak{C})$ в интерпретации $M = \{M; c_M, P_M\}$ и высказывания $(A \in \mathfrak{S})$ совпадают. Пусть это не так, и пусть $A \in \mathfrak{A}(\mathfrak{P}, \mathfrak{C})$ — суждение наименьшей длины (как слово в алфавите из символов констант, предикатов, переменных и других логических знаков), такое что его значение истинности в интерпретации M не совпадает со значением истинности высказывания $(A \in \mathfrak{S})$. Рассмотрим все возможные варианты (1)-(5) для суждения A и покажем, что в каждом из них мы приходим к противоречию.

(1). Суждение "и", истинно в любой интерпретации и принадлежит $\mathfrak{S}$, а суждение "л" не истинно в любой интерпретации и не принадлежит непротиворечивому множеству суждений $\mathfrak{S}$. Поэтому суждение A не совпадает ни с "и", ни с "л".

(2), (3). Интерпретация M построена так, что суждения видов $c = d$, $P(c_1, \ldots, c_n)$ истинны в M тогда и только тогда, когда они принадлежат $\mathfrak{S}$.

Поэтому суждение A не может совпадать с суждением одного из видов $c = d$, $P(c_1, \ldots, c_n)$.

(4). Пусть $B, C \in \mathfrak{A}(\mathfrak{P}, \mathfrak{C})$. Суждение $B\&C$ выводимо из суждений B и C, и наоборот, суждения B и C выводимы из суждения $B\&C$; поэтому $(B\&C) \in \mathfrak{S}$ тогда и только тогда, когда $B \in \mathfrak{S}$ и $C \in \mathfrak{S}$. Поэтому значения истинности высказываний $(B \in \mathfrak{S})\&(C \in \mathfrak{S})$ и $(B\&C) \in \mathfrak{S}$ совпадают. Далее, очевидно, что совпадают значения истинности высказываний $\neg(B \in \mathfrak{S})$ и $(\neg B) \in \mathfrak{S}$. Отсюда, пользуясь тем, что значения истинности для $B \vee C$, $B \to C$, $B \leftrightarrow C$ совпадают со значениями истинности для $\neg((\neg B)\&(\neg C))$, $\neg(B\&(\neg C))$, $\neg((\neg(B\&C))\&(\neg B)\&(\neg C))$, находим, что значения истинности высказываний $(B \in \mathfrak{S}) \vee (C \in \mathfrak{S})$, $(B \in \mathfrak{S}) \to (C \in \mathfrak{S})$, $(B \in \mathfrak{S}) \leftrightarrow (C \in \mathfrak{S})$ совпадают со значениями истинности высказываний $(B \vee C) \in \mathfrak{S}$, $(B \to C) \in \mathfrak{S}$, $(B \leftrightarrow C) \in \mathfrak{S}$.

Если суждение A имеет один из видов $B\&C$, $\neg B$, $B \vee C$, $B \to C$, $B \leftrightarrow C$, то суждения B, C короче суждения A, и потому их значения истинности в интерпретации M совпадают со значениями истинности высказываний $(B \in \mathfrak{S})$, $(C \in \mathfrak{S})$. Из рассуждений предыдущего абзаца мы видим теперь, что и значения истинности суждения A и высказывания $(A \in \mathfrak{S})$ совпадают, вопреки выбору суждения A.

(5). Пусть суждение A имеет вид $\forall x B(x)$. Если $A \in \mathfrak{S}$, то для всех символов констант $c \in \mathfrak{C}$ суждения $B(c)$, выводимые из суждения $\forall x B(x)$, принадлежат $\mathfrak{S}$, и, поскольку слово $B(c)$ короче слова $\forall x B(x)$, все суждения $B(c)$ истинны в интерпретации M. Следовательно, суждение $\forall x B(x)$ истинно в интерпретации M. Если же высказывание $(A \in \mathfrak{S})$ ложно, то суждение $\exists x(\neg B(x))$, равносильное суждению $\neg A$, принадлежит множеству суждений $\mathfrak{S}$, и, поскольку это множество суждений экзистенциально полно, найдется символ константы $c \in \mathfrak{C}$, такой что суждение $\neg B(c)$ принадлежит $\mathfrak{S}$. Но суждение $\neg B(c)$ короче суждения A; поэтому оно истинно в интерпретации M, и, значит, суждение $B(c)$ не истинно в интерпретации M. Следовательно, суждение A, имеющее вид $\forall x B(x)$, не истинно в M. Итак, в обоих случаях значение истинности суждения A в интерпретации M совпадает со значением истинности высказывания $(A \in \mathfrak{S})$, что противоречит нашему предположению.

Двойственным образом разбирается случай суждения A вида $\exists x B(x)$. Если оно принадлежит $\mathfrak{S}$, то из экзистенциальной полноты $\mathfrak{S}$ следует, что найдется символ константы $c \in \mathfrak{C}$, такой что суждение $B(c)$ принадлежит $\mathfrak{S}$; оно короче суждения A и потому истинно в интерпретации M. Следовательно, суждение $\exists x B(x)$ истинно в интерпретации M. Если же суждение A не принадлежит $\mathfrak{S}$, то суждение $\forall x(\neg B(x))$, равносильное суждению $\neg A$, принадлежит множеству суждений $\mathfrak{S}$, и вместе с ним множеству $\mathfrak{S}$ принадлежат все суждения $\neg B(c)$, $c \in \mathfrak{C}$. Отсюда следует, что ни одно из суждений $B(c)$ не принадлежит $\mathfrak{S}$ и, поскольку эти суждения короче суждения A, ни одно из них не истинно в интерпретации M. Поэтому суждение A, имеющее вид $\exists x B(x)$, не истинно в M. Снова мы получили, что значение истинности суждения A в интерпретации M совпадает со значением истинности высказывания $(A \in \mathfrak{S})$.

Этим и завершается доказательство теоремы.

3.3. Существование максимальных непротиворечивых множеств суждений.

Теорема. *Для всякого непротиворечивого множества суждений* $\mathfrak{S} \in \mathfrak{A}(\mathfrak{C})$ *существует содержащее его максимальное непротиворечивое множество суждений* $\mathfrak{B} \in \mathfrak{A}(\mathfrak{C})$.

Доказательство. Конечно, наиболее естественным при доказательстве подобных утверждений является использование леммы Цорна. Пусть $\mathcal{M}$ — множество всех непротиворечивых множеств суждений $\mathfrak{B} \subseteq \mathfrak{A}(\mathfrak{C})$, содержащих множество $\mathfrak{S}$. Множество $\mathcal{M}$ естественным образом упорядочено отношением включения; покажем, что оно индуктивно, т.е. что любое линейно упорядоченное подмножество множества $\mathcal{M}$ имеет верхнюю грань, тоже принадлежащую $\mathcal{M}$

Пусть $\{\mathfrak{B}_i \,|\, i \in I\}$ — линейно упорядоченное подмножество $\mathcal{M}$. Обозначим через $\mathfrak{B}$ объединение всех подмножеств $\mathfrak{B}_i$ множества $\mathfrak{A}(\mathfrak{C})$ $(i \in I)$. Множество $\mathfrak{B}$ содержит все множества $\mathfrak{B}_i$, и для того, чтобы показать, что $\mathfrak{B}$ — верхняя грань для семейства $\{\mathfrak{B}_i \,|\, i \in I\}$, достаточно установить, что $\mathfrak{B} \in \mathcal{M}$, т.е. что множество суждений $\mathfrak{B}$ непротиворечиво. Но это действительно так: в противном случае нашлись бы суждения $A_1, \ldots, A_n \in \mathfrak{B}$, такие что суждение $(A_1 \& \ldots \& A_n) \to (\text{л})$ выводимо; но конечное множество суждений $A_1, \ldots, A_n$ содержится уже в каком-то из множеств $\mathfrak{B}_i$, $i \in I$, и, значит, это множество $\mathfrak{B}_i$ не является непротиворечивым, т.е. $\mathfrak{B}_i \notin \mathcal{M}$ вопреки предположению.

Итак, частично упорядоченное отношением включения множество $\mathcal{M}$ индуктивно, и по лемме Цорна в нем есть максимальный элемент $\mathfrak{B}$. Множество $\mathfrak{B}$ и будет максимальным непротиворечивым множеством суждений, содержащим $\mathfrak{S}$.

3.4. Существование экзистенциально полных расширений множества суждений.

Теорема. *Для любого непротиворечивого множества суждений* $\mathfrak{S} \subseteq \mathfrak{A}(\mathfrak{P}, \mathfrak{C})$ *существуют множество символов констант* $\mathfrak{C}' \supseteq \mathfrak{C}$ *малой мощности и экзистенциально полное максимальное непротиворечивое множество суждений* $\mathfrak{S}' \subseteq \mathfrak{A}(\mathfrak{P}, \mathfrak{C}')$, *содержащее* $\mathfrak{S}$.

Доказательство. Пусть $\mathfrak{C}_0 = \mathfrak{C}$, и пусть $\mathfrak{S}_0 \subseteq \mathfrak{A}(\mathfrak{C}_0)$ — максимальное непротиворечивое множество суждений, содержащее $\mathfrak{S}$. Пусть уже построены множество символов констант $\mathfrak{C}_i$ и максимальное непротиворечивое множество суждений $\mathfrak{S}_i \subseteq \mathfrak{A}(\mathfrak{C}_i)$. Обозначим через $\mathfrak{M}$ множество всех осмысленных выражений $A = A(x)$ с единственной свободной переменной x, таких что суждение $\exists x(A(x))$ содержится в $\mathfrak{S}_i$. Для каждого $A \in \mathfrak{M}$ введем новый символ константы c_A и обозначим через $\mathfrak{C}_{i+1}$ множество, полученное из $\mathfrak{C}_i$ добавлением всех новых символов констант c_A, а через $\mathfrak{S}'_{i+1} \subseteq \mathfrak{A}(\mathfrak{C}_{i+1})$ — множество суждений, полученное из $\mathfrak{S}_i$ добавлением всех суждений $A(c_A)$, $A \in \mathfrak{M}$.

Покажем, что множество суждений $\mathfrak{S}'_{i+1}$ непротиворечиво. Если бы оно было противоречиво, то для некоторых суждений $B_1, \ldots, B_m \in \mathfrak{S}_i$ и выражений $A_1, \ldots, A_n \in \mathfrak{M}$ суждение $(B_1 \& \ldots \& B_m \& A_1(c_{A_1}) \& \ldots \& A_n(c_{A_n})) \to (\text{л})$ было бы выводимо. Из правил исчисления высказываний отсюда бы следовало, что выводимо и эквивалентное предыдущему суждение

$$\neg(B_1 \& \ldots \& B_m \& A_1(c_{A_1}) \& \ldots \& A_n(c_{A_n})),$$

которое в свою очередь эквивалентно суждению

$$\neg B_1 \vee \cdots \vee \neg B_n \vee \neg A_1(c_{A_1}) \vee \cdots \vee \neg A_n(c_{A_n})).$$

По правилу (6) отсюда следует выводимость суждения

$$\forall x_1 \ldots \forall x_n(\neg B_1 \vee \cdots \vee \neg B_m \vee \neg A_1(x_1) \vee \cdots \vee \neg A_n(x_n)),$$

которое по другим правилам вывода эквивалентно суждению

$$\neg B_1 \vee \cdots \vee \neg B_m \vee \neg(\exists x_1(A_1(x_1))) \vee \cdots \vee \neg(\exists(A_n(x_n))).$$

Из него и из принадлежащих множеству $\mathfrak{S}_i$ суждений $B_1, \ldots, B_m, \exists x_1(A_1(x_1)), \ldots, \exists(A_n(x_n))$ по правилам исчисления высказываний выводится тождественно ложное суждение

$$(B_1 \& \neg B_1) \vee \cdots \vee (B_m \& \neg B_m) \vee$$
$$\vee(\exists x_1(A_1(x_1)) \& \neg(\exists x_1(A_1(x_1)))) \cdots \vee (\exists(A_n(x_n)) \& \neg(\exists(A_n(x_n)))),$$

а это несовместимо с непротиворечивостью $\mathfrak{S}_i$.

Итак, множество суждений $\mathfrak{S}'_{i+1} \subseteq \mathfrak{A}(\mathfrak{C}_{i+1})$ непротиворечиво, и его можно дополнить до максимального непротиворечивого множества суждений $\mathfrak{S}_{i+1} \subseteq \mathfrak{A}(\mathfrak{C}_{i+1})$.

Обозначим теперь через $\mathfrak{C}'$ объединение всех множеств $\mathfrak{C}_i$, а через $\mathfrak{S}' \subseteq \mathfrak{A}(\mathfrak{C}')$ — объединение всех множеств суждений $\mathfrak{S}_i$, $i = 0, 1, \ldots$. Покажем, что $\mathfrak{S}'$ — экзистенциально полное и максимальное непротиворечивое множество суждений. Действительно, если суждение $\exists x(A(x))$ содержится в $\mathfrak{S}'$, то это суждение содержится уже в некотором $\mathfrak{S}_i$, а тогда в множестве $\mathfrak{S}'_{i+1} \subseteq \mathfrak{S}_{i+1} \subseteq \mathfrak{S}'$ есть суждение $A(c_A)$, где $c_A \in \mathfrak{C}_{i+1} \subseteq \mathfrak{C}'$. Таким образом, множество суждений $\mathfrak{S}'$ экзистенциально полно. Если бы это множество не было бы максимальным непротиворечивым, то существовало бы суждение $A \in \mathfrak{A}(\mathfrak{C}')$, такое что ни суждение A, ни суждение $\neg A$ не принадлежали бы $\mathfrak{S}'$. Но для записи суждения A используется лишь конечное число символов констант из $\mathfrak{C}'$, и потому существует номер i, для которого $A \in \mathfrak{A}(\mathfrak{C}_i)$; по лемме 1, одно из суждений A, $\neg A$ принадлежит максимальному непротиворечивому множеству суждений $\mathfrak{S}_i \subseteq \mathfrak{S}'$, что противоречит выбору суждения A.

Из наших построений ясно, что $\mathfrak{C}'$ — множество малой мощности. Теорема полностью доказана.

3.5. Доказательство теоремы Геделя. Теперь мы можем завершить доказательство теоремы Геделя о полноте. Пусть $\mathfrak{C} \subseteq \mathfrak{A}(\mathfrak{P}, \mathfrak{C})$ — непротиворечивое множество суждений. По теореме из §3.4 существует множество символов констант $\mathfrak{C}' \supseteq \mathfrak{C}$ малой мощности и максимальное непротиворечивое экзистенциально полное множество суждений $\mathfrak{S}' \subseteq \mathfrak{A}(\mathfrak{P}, \mathfrak{C}')$, содержащее $\mathfrak{S}$. Далее, по теореме из §3.2 существует такая интерпретация $M = \{M; c_M, P_M\}$ множеств $\mathfrak{C}'$, $\mathfrak{P}$, что для любого элемента $m \in M$ существует символ константы $c \in \mathfrak{C}'$, для которого $m = c_M$ (и потому мощность M не больше мощности $\mathfrak{C}'$), и суждение из $\mathfrak{A}(\mathfrak{P}, \mathfrak{C}')$ истинно в M тогда и только тогда, когда оно содержится в множестве $\mathfrak{S}'$. Таким образом, интерпретация M является моделью множества суждений $\mathfrak{S}'$ и тем более моделью содержащегося в нем множества суждений $\mathfrak{S}$.

4. Теорема Лёвенгейма-Скулема

4.1. Элементарная эквивалентность. Пусть опять $\mathfrak{P}$, $\mathfrak{C}$ — какие-то множества символов предикатов и констант. Две интерпретации M, N этих множеств называются элементарно эквивалентными, если множество суждений из $\mathfrak{A}(\mathfrak{P},\mathfrak{C})$, истинных в интерпретации M, совпадает с множеством суждений из $\mathfrak{A}(\mathfrak{P},\mathfrak{C})$, истинных в интерпретации N.

Пусть $M=\{M;c_M,P_M\}$ — интерпретация множества символов констант $\mathfrak{C}$ и множества символов предикатов $\mathfrak{P}$, и пусть N — подмножество множества M, содержащее элементы c_M для всех символов констант $c\in\mathfrak{C}$. Если $P\in\mathfrak{P}$ — символ n-местного предиката, то обозначим через P_N пересечение множества $P_M\subseteq M^n$ с n-й декартовой степенью N^n множества N; если $c\in C$, то положим $c_N=c_M\in N\subseteq M$. Набор $N=\{N;c_N,P_N\}$ представляет собой интерпретацию множества символов констант $\mathfrak{C}$ и множества символов предикатов $\mathfrak{P}$; мы будем говорить, что N — подинтерпретация интерпретации M (согласно правилам русской орфографии, следовало бы писать *подынтерпретация*, но мы все же предпочтём вариант с "и"). Отметим, что подинтерпретация полностью определяется подмножеством $N\subseteq M$, от которого требуется лишь, чтобы оно содержало все элементы c_M.

Подинтерпретация N интерпретации M называется элементарной подинтерпретацией, если она не только элементарно эквивалентна M, но еще и удовлетворяет более сильному условию: если $A(x_1,\dots,x_s)$ — любое осмысленное выражение (не обязательно суждение), в записи которого участвуют только символы предикатов, принадлежащие $\mathfrak{P}$, и символы констант, принадлежащие $\mathfrak{C}$, и $n_1,\dots,n_s$ — любые элементы из $N\subseteq M$, то значения истинности выражения $A(n_1,\dots,n_s)$ в интерпретациях M и N совпадают.

4.2. Теорема Лёвенгейма-Скулема. Пусть M — некоторая интерпретации множества символов констант $\mathfrak{C}$ и множества символов предикатов $\mathfrak{P}$, и пусть $\mathfrak{X}$ — множество суждений из $\mathfrak{A}(\mathfrak{P},\mathfrak{C})$, истинных в интерпретации M. Теорема Геделя о полноте утверждает существование модели малой мощности для множества суждений $\mathfrak{X}$; однако, она ничего не говорит о связи этой модели с исходной моделью M. Более точный результат дает следующая теорема.

Теорема Лёвенгейма-Скулема. *Для любой интерпретации множества символов констант $\mathfrak{C}$ и множества символов предикатов $\mathfrak{P}$ существует её элементарная подинтерпретация малой мощности.* ∎

Доказательство. Рассуждения, приводящие к теореме Лёвенгейма-Скулема, напоминают рассуждения из §3.2-3.4, но намного проще (следует отметить, что и исторически эта теорема была получена ранее теоремы Геделя о полноте). Пусть $M=\{M;c_M,P_M\}$ — интерпретация множества символов констант $\mathfrak{C}$ и множества символов предикатов $\mathfrak{P}$. Обозначим через $M_0\subseteq M$ множество всех элементов c_M, отвечающих символам констант $c\in\mathfrak{C}$. Ясно, что M_0 — множество малой мощности.

Определим возрастающую цепочку подмножеств малой мощности $M_0\subseteq M_1\subseteq\dots$ множества M, удовлетворяющих следующему условию:

(∗) для каждого осмысленного выражения $A(x,x_1,\dots,x_n)$ и каждых элементов $m\in M$, $m_1,\dots,m_n\in M_i$ найдется элемент $m'\in M$, такой что

значения истинности выражений $A(m, m_1, \ldots, m_n)$ и $A(m', m_1, \ldots, m_n)$ в интерпретации M совпадают.

Пусть множество M_i уже построено; если $A(x, x_1, \ldots, x_n)$ — осмысленное выражение, $m_1, \ldots, m_n \in M_i$ и $\varepsilon \in \{\text{и}, \text{л}\}$ таковы, что множество элементов $m' \in M$, для которых значение истинности выражения $A(m', m_1, \ldots, m_n)$ в интерпретации M совпадает с ε, непусто, то выберем в этом непустом множестве какой-то один элемент $m'(\varepsilon, A, m_1, \ldots, m_n) \in M$. Отметим, что, осуществляя этот выбор одновременно для всех возможных наборов $(\varepsilon, A, m_1, \ldots, m_n)$, мы пользуемся аксиомой выбора. В качестве M_{i+1} возьмем множество, полученное присоединением к множеству M_i всех выбранных элементов $m'(\varepsilon, A, m_1, \ldots, m_n)$. Ясно, что M_{i+1} — множество малой мощности, удовлетворяющее условию $(*)$.

Объединение N всех множеств M_i, $i = 0, 1, 2, \ldots$ — тоже множество малой мощности. Покажем, что N — элементарная подинтерпретация интерпретации M. Для этого надо доказать, что для каждого осмысленного выражения $A(x_1, \ldots, x_n)$ и каждых элементов $m_1, \ldots, m_n \in N$ значения истинности выражения $A(m_1, \ldots, m_n)$ в интерпретациях N и $M \supseteq N$ совпадают, что мы и сделаем индукцией по построению выражения $A(x_1, \ldots, x_n)$.

Если выражение A имеет один из видов $c = d$, $c = m$, $m = m'$, $P(t_1, \ldots, t_n)$, где $c, d \in \mathfrak{C}$, $m, m' \in N$, P — символ n-местного предиката, то, очевидно, истинность этого выражения в интерпретациях N и M одна и та же. Если A представляется в форме $B\&C$, $B \vee C$, $B \to C$, $B \leftrightarrow C$ или $\neg B$, то его значение истинности определяется по правилам исчисления высказываний значениями истинности выражений B, C, которые, по предположению индукции, одинаковы для обеих интерпретаций. Остается рассмотреть случай, когда выражение $A(x_1, \ldots, x_n)$ имеет вид $\forall x B(x, x_1, \ldots, x_n)$ или $\exists x B(x, x_1, \ldots, x_n)$.

Пусть $m_1, \ldots, m_n \in N \subseteq M$; тогда $m_1, \ldots, m_n \in M_i$ для какого-то номера i. Если значение истинности выражения $\forall x B(x, m_1, \ldots, m_n)$ в интерпретации M истинно, то $B(m, m_1, \ldots, m_n)$ истинно в M для всех $m \in M$ и тем более для всех $m \in N$; таким образом, выражение $\forall x B(x, m_1, \ldots, m_n)$ истинно в подинтерпретации N. Если же выражение $\forall x B(x, m_1, \ldots, m_n)$ не истинно в интерпретации M, то существует элемент $m \in M$, такой что выражение $B(m, m_1, \ldots, m_n)$ не истинно в интерпретации M; по построению множества M_{i+1}, существует элемент $m' \in M_{i+1} \subseteq N$, такой что выражение $B(m', m_1, \ldots, m_n)$ не истинно в интерпретации M, а потому, по предположению индукции, и в интерпретации N. Таким образом, выражение $\forall x B(x, m_1, \ldots, m_n)$ не истинно в интерпретации N.

Дуальным образом рассматривается выражение $\exists x B(x, m_1, \ldots, m_n)$. Если оно не истинно в интерпретации M, то $B(m, m_1, \ldots, m_n)$ не истинно в M для всех $m \in M$ и тем более для всех $m \in N$; таким образом, выражение $\exists x B(x, m_1, \ldots, m_n)$ не истинно в подинтерпретации N. Если же выражение $\exists x B(x, m_1, \ldots, m_n)$ истинно в интерпретации M, то существует элемент $m \in M$, такой что выражение $B(m, m_1, \ldots, m_n)$ истинно в интерпретации M; по построению множества M_{i+1}, существует элемент $m' \in M_{i+1} \subseteq N$, такой что выражение $B(m', m_1, \ldots, m_n)$ истинно в интерпретации M, а потому, по предположению индукции, и в интерпретации N. Таким образом, выражение $\exists x B(x, m_1, \ldots, m_n)$ истинно в интерпретации N.

5. Аксиоматика Z_1 полукольца натуральных чисел

Натуральные числа обычно определяются при помощи аксиом Пеано. В этой системе аксиом натуральные числа образуют множество $\mathbb{N}_0$ с единственной заданной на нем унарной операцией следования: для каждого натурального числа x определено единственное натуральное число x', следующее за x. При этом должны выполняться следующие условия (аксиомы Пеано):

(1) Если $x' = y'$, то $x = y$.
(2) Существует натуральное число $0 \in \mathbb{N}_0$, такое что $x' \neq 0$ ни для какого $x \in \mathbb{N}_0$.
(3) Если M — подмножество множества $\mathbb{N}_0$, содержащее 0 и такое, что для любого элемента $x \in M$ следующий за ним элемент x' также принадлежит M, то $M = \mathbb{N}_0$.

Это определение не может непосредственно быть выраженным в формальном виде, так как в нем участвует понятие множества; и если первые две аксиомы Пеано еще могут быть выражены формально, то из третьей — аксиомы индукции — понятие множества никак не исключить. Поэтому приходится чем-то пожертвовать; обычно жертвуют общим понятием подмножества, и вместо этого аксиому индукции формулируют только для тех подмножеств, которые могут быть заданы формально.

В формальной арифметике Z_1 два символа тернарных предикатов $S(x, y, z)$, $P(x, y, z)$ и два символа констант 0, 1. Следующие суждения считаются истинными в Z_1.

(1) $\forall x \forall y \exists z (S(x, y, z))$;
(2) $\forall x \forall y \forall z \forall t ((S(x, y, z) \& S(x, y, t)) \to (z = t))$;
(3) $\forall x \forall y \exists z (P(x, y, z))$;
(4) $\forall x \forall y \forall z \forall t ((P(x, y, z) \& P(x, y, t)) \to (z = t))$;
(5) $\forall x (S(x, 0, x) \& P(x, 1, x))$;
(6) $\forall x \forall y \forall z ((S(x, 1, z) \& S(y, 1, z)) \to (x = y))$;
(7) $\forall x \forall y \forall z \forall t \forall u \forall v \forall w ((S(x, y, t) \& S(t, z, u) \& S(y, z, v) \& S(x, v, w)) \to (u = w))$;
(8) $\forall x \forall y \forall z \forall t \forall u \forall v \forall w ((P(x, y, t) \& P(t, z, u) \& P(y, z, v) \& P(x, v, w)) \to (u = w))$;
(9) $\forall x \forall y \forall z \forall t \forall u \forall v \forall w \forall p ((S(x, y, t) \& P(t, z, u) \& P(x, z, v) \& P(y, z, w) \&$
$\& S(v, w, p)) \to (u = p))$;
(10) $\forall x \forall y \forall z \forall t ((S(x, y, z) \& S(y, x, t)) \to (z = t))$;
(11) $\forall x \forall y \forall z \forall t ((P(x, y, z) \& P(y, x, t)) \to (z = t))$.

6. Примитивно рекурсивные функции

6.1. Элементарные функции. Как обычно, мы обозначаем через $\mathbb{N}_0$ множество, состоящее из 0 и всех натуральных чисел. Все функции, рассматриваемые в этой главе, являются функциями нескольких переменных $x_1, x_2, \ldots$ из $\mathbb{N}_0$ со значениями в $\mathbb{N}_0$. Следующие функции мы будем называть элемен-

тарными:

$$o(x_1) = 0,$$
$$s(x_1) = x_1 + 1,$$
$$\mathrm{id}(x_1) = x_1,$$
$$\mathrm{pr}_1(x_1, x_2) = x_1,\ \mathrm{pr}_2(x_1, x_2) = x_2.$$

6.2. Подстановка. Пусть $f(x_1, \dots, x_n)$, $g_1(x_1, \dots, x_m), \dots, g_n(x_1, \dots, x_m)$ – некоторые функции; мы будем говорить, что функция

$$h(x_1, \dots, x_m) = f(g_1(x_1, \dots, x_m), \dots, g_n(x_1, \dots, x_m))$$

получена из функций $f, g_1, \dots, g_n$ подстановкой.

6.3. Примитивная рекурсия. Опишем еще один способ построения новых функций из уже имеющихся. Этот способ называется примитивной рекурсией и по существу представляет собой построение значений функции по индукции. Точнее, пусть $h(x_1, \dots, x_{n-1})$, $g(x_1, \dots, x_{n-1}, x_n, x_{n+1})$ – две функции; мы говорим, что функция $f(x_1, \dots, x_{n-1}, x_n)$ получена из них примитивной рекурсией, если

$$f(x_1, \dots, x_{n-1}, 0) = h(x_1, \dots, x_{n-1}),$$
$$f(x_1, \dots, x_{n-1}, x_n + 1) = g(x_1, \dots, x_{n-1}, x_n, f(x_1, \dots, x_{n-1}, x_n)).$$

Ясно, что каждое значение функции f может быть найдено по этим формулам, и притом однозначно, так что функция f однозначно определена функциями h, g.

6.4. Примитивно рекурсивные функции. Все функции, которые могут быть получены при помощи операций подстановки и примитивной рекурсии из элементарных функций o, s, id, pr_1, pr_2, называются примитивно рекурсивными. Точнее говоря,

(1) функции o, s, id, pr_1, pr_2 примитивно рекурсивны;
(2) если $f(x_1, \dots, x_n)$, $g_1(x_1, \dots, x_m), \dots, g_n(x_1, \dots, x_m)$ – примитивно рекурсивные функции, то и функция

$$h(x_1, \dots, x_m) = f(g_1(x_1, \dots, x_m), \dots, g_n(x_1, \dots, x_m)),$$

полученная из них подстановкой функция, примитивно рекурсивна;
(3) если h, g – примитивно рекурсивные функции, то функция, полученная из них при помощи примитивной рекурсии, примитивно рекурсивна;
(4) функции, которые не могут быть получены из элементарных функций многократным применением операций подстановки и примитивной рекурсии, не являются примитивно рекурсивными.

6.5. Простейшие примитивно рекурсивные функции.

Проекции. Функции $\mathrm{pr}_i^{(n)}$, определенные равенствами $\mathrm{pr}_i^{(n)}(x_1,\dots,x_n)=x_i$, примитивно рекурсивны для любых $n>2$, $1\le i\le n$, так как они получаются подстановками:

$$\mathrm{pr}_i^{(n)}(x_1,\dots,x_n)=\mathrm{pr}_{s_1}(x_1,\mathrm{pr}_{s_2}(x_2,\dots,\mathrm{pr}_{s_{n-1}}(x_{n-1},x_n)\dots)),$$

где $s_j=2$ при $j<i$, $s_j=1$ при $j\ge i$.

Константы. Функции $s(o(x_1))$, $s(s(o(x_1)))$, ..., представляют собой функции одной переменной x_1, значения которых тождественно равны 1,2,... , а функции $o(p_1^{(n)}(x_1,\dots,x_n))$, $s(o(p_1^{(n)}(x_1,\dots,x_n)))$, $s(s(o(p_1^{(n)}(x_1,\dots,x_n))))$, ..., являются функциями n переменных, значения которых тождественно равны 0,1,2,... Таким образом, постоянные функции примитивно рекурсивны.

Сумма и произведение. Сумма $\mathrm{sum}(x_1,x_2)=x_1+x_2$ может быть определена при помощи примитивной рекурсии

$$\mathrm{sum}(x_1,0)=x_1 \qquad =\mathrm{id}(x_1),$$
$$\mathrm{sum}(x_1,x_2+1)=\mathrm{sum}(x_1,x_2)+1=s(\mathrm{pr}_3^{(3)}(x_1,x_2,\mathrm{sum}(x_1,x_2)))\,.$$

Правые части обоих равенств примитивно рекурсивны, потому и функция sum получена примитивно рекурсивна.

Произведение $\mathrm{prod}(x_1,x_2)=x_1x_2$ определяется примитивной рекурсией

$$\mathrm{prod}(x_1,0)=0 \qquad =o(x_1),$$
$$\mathrm{prod}(x_1,x_2+1)=\mathrm{prod}(x_1,x_2)+x_1=\mathrm{sum}(x_1,\mathrm{prod}(x_1,x_2))\,.$$

Следовательно, prod – примитивно рекурсивная функция.

В дальнейшем мы не будем проявлять столь щепетильный формализм, как в рассмотренных примерах, и будем обычно употреблять для вводимых функций более естественные обозначения; читатель легко сможет восстановить пропущенные детали. В частности, аргументы функций мы не всегда будем обозначать $x_1,x_2,\dots$, а для суммы и произведения будем обычно использовать привычные знаки $x+y$, xy.

Усеченная разность. Модуль разности. Не для любых чисел из $\mathbb{N}_0$ их разность принадлежит $\mathbb{N}_0$; поэтому в качестве суррогата разности приходится использовать так называемую усеченную разность: усеченная разность $x\ominus y$ чисел x и y равна $x-y$, если $x\ge y$, и равна 0, если это не так. Для задания усеченной разности сначала зададим функцию одного аргумента $\alpha(x)=x\ominus 1$ примитивной рекурсией

$$0\ominus 1=0,$$
$$(x+1)\ominus 1=x\,.$$

Усеченная разность задается теперь такой примитивной рекурсией:

$$x\ominus 0=x,$$
$$x\ominus(y+1)=(x\ominus y)\ominus 1=\alpha(x\ominus y)\,.$$

Примитивно рекурсивной функцией является и модуль разности $|x-y|=(x\ominus y)+(y\ominus x)$. Эта функция получается из суммы подстановкой вместо слагаемых соответствующих усеченных разностей.

Знак и антизнак. Определим функцию $\operatorname{sgn}(x)$, положив $\operatorname{sgn}(0)=0$, $\operatorname{sgn}(x)=1$ при $x>0$, и функцию $\overline{\operatorname{sgn}}(x)$, положив $\overline{\operatorname{sgn}}(0)=1$, $\overline{\operatorname{sgn}}(x)=0$ при $x>0$. Обе эти функции задаются примитивными рекурсиями

$$\begin{cases} \operatorname{sgn}(0)=0, \\ \operatorname{sgn}(x+1)=1; \end{cases} \qquad \begin{cases} \overline{\operatorname{sgn}}(0)=1, \\ \overline{\operatorname{sgn}}(x+1)=0. \end{cases}$$

Неполное частное и остаток. Не всегда возможно разделить одно натуральное число на другое; поэтому вместо деления мы вводим деление с остатком. Пусть $x, y \in \mathbb{N}_0$. Если $y>0$ неполным частным $[x/y]$ называется такое целое число, что $[x/y]y \le x$, $([x/y]+1)y > x$, а остаток определяется формулой $\operatorname{rest}(x,y)=x-[x/y]y$; для того, чтобы сделать неполное частное и остаток определенными всегда, условимся считать, что $[x/0]=0$, $\operatorname{rest}(x,0)=x$. Остаток и неполное частное могут быть заданы такими примитивными рекурсиями:

$$\begin{aligned} \operatorname{rest}(0,y) &= 0, \\ \operatorname{rest}(x+1,y) &= (\operatorname{rest}(x,y)+1)\cdot \operatorname{sgn}|y-(\operatorname{rest}(x,y)+1)|\,; \end{aligned}$$

$$\begin{aligned} [0/y] &= 0, \\ [(x+1)/y] &= [x/y]+\overline{\operatorname{sgn}}(\operatorname{rest}(x+1),y)\,. \end{aligned}$$

6.6. Суммы и произведения с переменными пределами. Для примитивно рекурсивной функции $f(x_1,\dots,x_{n-1},x_n)$ положим

$$F(x_1,\dots,x_{n-1},x_n)=\sum_{i=0}^{x_n} f(x_1,\dots,x_{n-1},i)\,.$$

Эта функция примитивно рекурсивна, так как она может быть определена примитивной рекурсией

$$\begin{aligned} F(x_1,\dots,x_{n-1},0) &= 0\,, \\ F(x_1,\dots,x_{n-1},x_n+1) &= F(x_1,\dots,x_{n-1},x_n)+f(x_1,\dots,x_{n-1},x_n+1)\,. \end{aligned}$$

Отсюда следует, что примитивно рекурсивна и функция

$$\sum_{i=x_n}^{x_{n+1}} f(x_1,\dots,x_{n-1},i) =$$

$$\sum_{i=0}^{x_{n+1}} f(x_1,\dots,x_{n-1},i) \ominus \sum_{i=0}^{x_n} f(x_1,\dots,x_{n-1},i) \;+\operatorname{sgn}(x_{n+1}\ominus x_n) f(x_1,\dots,x_{n-1},x_n)\,.$$

Подставляя вместо x_n, x_{n+1} произвольные примитивно рекурсивные функции $g(x_1,\dots,x_{n-1},x_n)$, $h(x_1,\dots,x_{n-1},x_n)$, получаем, что функция

$$\sum_{i=g(x_1,\dots,x_n)}^{h(x_1,\dots,x_n)} f(x_1,\dots,x_{n-1},i)$$

тоже примитивно рекурсивна. Таким же образом показывается, что произведение значений примитивно рекурсивной функции с переменными верхним и нижним пределами, выражаемыми примитивно рекурсивными функциями, само является примитивно рекурсивной функцией.

6.7. Кусочное задание примитивно рекурсивной функции. Пусть

$$g_1(x_1,\dots,x_n),\dots,g_m(x_1,\dots,x_n),\ h_1(x_1,\dots,x_n),\dots,h_m(x_1,\dots,x_n),\ h(x_1,\dots,x_n)$$

– примитивно рекурсивные функции, причем никакие две из функций $g_1,\dots,g_m$ ни при каких значениях переменных не обращаются одновременно в 0. Тогда функция $f(x_1,\dots,x_n)$, определенная условиями

$$f(x_1,\dots,x_n)=\begin{cases} h_1(x_1,\dots,x_n), & \text{если} \quad g_1(x_1,\dots,x_n)=0,\\ \dots & \\ h_m(x_1,\dots,x_n), & \text{если} \quad g_m(x_1,\dots,x_n)=0,\\ h(x_1,\dots,x_n) & \text{в остальных случаях,}\end{cases}$$

примитивно рекурсивна, так как

$$f=h_1\overline{\operatorname{sgn}}(g_1)+\dots+h_m\overline{\operatorname{sgn}}(g_m)+h\cdot\operatorname{sgn}(g_1\cdots g_m)\,.$$

6.8. Ограниченная минимизация. Пусть $f(x_1,\dots,x_n,t)$ – такая функция, что для любых $x_1,\dots,x_n$ уравнение $f(x_1,\dots,x_n,t)=0$ имеет решение (напомним, что значения функции и все аргументы предполагаются принадлежащими множеству натуральных чисел $\mathbb{N}_0$, так что и решение предполагается натуральным). Обозначим через $(\mu_t f)(x_1,\dots,x_n)$ наименьшее решение этого уравнения. Вообще говоря, функция $\mu_t f$ не примитивно рекурсивна, даже если f примитивно рекурсивна. Однако, если f примитивно рекурсивна и существует такая примитивно рекурсивная функция $g(x_1,\dots,x_n)$, что для любых $x_1,\dots,x_n$ уравнение $f(x_1,\dots,x_n,t)=0$ имеет решение $t\le g(x_1,\dots,x_n)$, то $\mu_t f$ – примитивно рекурсивная функция. Действительно,

$$(\mu_t f)(x_1,\dots,x_n)=\sum_{i=0}^{g(x_1,\dots,x_n)}\operatorname{sgn}\Big(\prod_{j=0}^{i}f(x_1,\dots,x_n,j)\Big)\,.$$

Действительно, фигурирующее в этой формуле произведение отлично от 0 лишь до тех пор, пока мы не дойдем до решения t_0 уравнения (а мы до него дойдем по условию), и в сумме слагаемые, отвечающие индексам $i<t_0$, равны 1, а все остальные слагаемые равны 0. Вместо $(\mu_t f)(x_1,\dots,x_n)$ мы будем писать иногда $\mu_t f(x_1,\dots,x_n,t)$; еще раз отметим, что это функция только от $x_1,\dots,x_n$, но не от t.

6.9. Теоретико-числовые функции. Количество делителей числа x

$$div(x)=\sum_{i=0}^{x}\overline{\operatorname{sgn}}(\operatorname{rest}(x,i))$$

и количество простых чисел, не превосходящих x,

$$\pi(x)=\sum_{i=0}^{x}\overline{\operatorname{sgn}}(|div(x)-2|)$$

являются примитивно рекурсивными, как композиции примитивно рекурсивных функций (мы считаем, что $div(0) = 0$, а во второй формуле используем, что число является простым тогда и только тогда, когда число его делителей равно 2). Перенумеруем все простые числа в порядке возрастания: $p_0 = 2, p_1 = 3, p_2 = 5, \ldots$ Тогда n-е простое число – это наименьшее число, такое что $\pi(x) = n+1$, т.е. $p_x = \mu_y|\pi(y) - (x+1)|$. Таким образом, функция p_x получается минимизацией из примитивно рекурсивной функции $|\pi(y)-(x+1)|$, и для доказательства её примитивной рекурсивности достаточно доказать, что решение уравнения $|\pi(y) - (x+1)| = 0$ ограничено сверху примитивно рекурсивной функцией от x. Но это действительно так: $p_x \le 2^{2^x}$; в самом деле, это верно для $x = 0$, и, если это доказано для всех меньших x значений аргумента, то

$$p_x \le p_0 p_1 \cdots p_{x-1} + 1 \le 2^{2^0} 2^{2^1} \cdots 2^{2^{x-1}} + 1 < 2 \cdot 2^{1+2+\ldots+2^{x-1}} = 2^{2^x},$$

ибо число $N = p_0 p_1 \cdots p_{x-1} + 1$ не делится ни на одно из чисел p_0, p_1, ... , p_{x-1} и потому все его простые делители (а хотя бы один простой делитель существует) больше p_{x-1} и не больше N, а, значит, $p_x \le N$. Обозначим через $\exp(x, y)$ показатель степени, с которым простое число p_x входит в разложение y в произведение простых чисел (для $y = 0$ считаем, что $\exp(x, y) = 0$ для всех x). Ясно, что

$$\exp(x,y) = \begin{cases} \mu_z \overline{\operatorname{sgn}}(\operatorname{rest}(y, p_x^z)) \ominus 1, \text{ если } \overline{\operatorname{sgn}}(y) = 0\,, \\ 0 \text{ в остальных случаях,} \end{cases}$$

так что $\exp(x, y)$ – тоже примитивно рекурсивная функция.

6.10. Координатные функции. Пусть $n \ge 1$ – натуральное число; построим примитивно рекурсивные функции $c_1^{(n)}(x)$, ... , $c_n^{(n)}(x)$, $d^{(n)}(x_1, \ldots, x_n)$, такие что

$$d^{(n)}(c_1^{(n)}(x), \ldots, c_n^{(n)}(x)) = x, \quad c_i^{(n)}(d^{(n)}(x_1, \ldots, x_i, \ldots, x_n)) = x_i \ (1 \le i \le n)$$

для всех $x, x_1, \ldots, x_n \in \mathbb{N}_0$. Эти равенства в точности означают, что наши функции осуществляют взаимно обратные биективные отображения $\mathbb{N}_0^n \to \mathbb{N}_0$, $\mathbb{N}_0 \to \mathbb{N}_0^n$. Функции $c_i^{(n)}$ называются координатными функциями.

При $n = 1$ положим $c_1^{(1)}(x) = d^{(1)}(x) = x$. Рассмотрим случай $n = 2$. Поскольку этот случай наиболее важный и часто встречающийся, мы будем использовать вместо $c_1^{(2)}$, $c_2^{(2)}$ более простые обозначения c_1, c_2. Функция $d^{(2)}(x, y) = [(x + y)(x + y + 1)/2] + x$ примитивно рекурсивна. Для построения функций c_1, c_2 определим вспомогательную функцию $h(z) = \mu_t(\overline{\operatorname{sgn}}(t^2 + t \ominus 2z)) \ominus 1$. Иначе говоря, $h(z)$ – наибольшее число, такое что $[h(z)(h(z) + 1)/2] \le z$. Функция $h(z)$ получена минимизацией из примитивно рекурсивной функции, и, поскольку $h(z) \le z$, эта минимизация ограниченная. Таким образом, $h(z)$ – примитивно рекурсивная функция. Тогда и функции $c_1(z) = z \ominus [h(z)(h(z) + 1)/2]$, $c_2(z) = h(z) \ominus c_1(z)$ примитивно рекурсивны. При этом

$$d^{(2)}(c_1(z), c_2(z)) = [(c_1(z) + c_2(z))(c_1(z) + c_2(z) + 1)/2] + c_1(z) = [h(z)(h(z) + 1)/2] + z \ominus [h(z)(h(z) + 1)/2] = z.$$

Далее, для любых $x, y \in \mathbb{N}_0$ имеем: $(x+y)(x+y+1)/2 \le d^{(2)}(x,y)$, $(x+y+1)(x+y+2)/2 > (x+y)(x+y+1)/2+(x+y) \ge (x+y)(x+y+1)/2+x = d^{(2)}(x,y)$, и потому $h(d^{(2)}(x,y)) = x+y$, $c_1(d^{(2)}(x,y)) = d^{(2)}(x,y) - [(x+y)(x+y+1)/2] = x$, $c_2(d^{(2)}(x,y)) = y$. Отметим, что функции $d^{(2)}$, c_1, c_2, которые мы только что определили, имеют простой смысл: они осуществляют перечисление целочисленных точек плоскости с неотрицательными координатами по прямым $x+y=b$, т.е. в следующем порядке: (0,0), (0,1), (1,0), (0,2), (1,1), (2,0), (0,3), (1,2), (2,1), (3,0)... Конечно, возможны и другие варианты построения функций c_2^i, $d^{(2)}$. Если уже определены функции $d^{(n-1)}$, $c_i^{(n-1)}$ $(n>2)$, то следующим образом определим функции $d^{(n)}$, $c_i^{(n)}$:

$$d^{(n)}(x_1,\dots,x_{n-1},x_n) = d^{(2)}(d^{(n-1)}(x_1,\dots,x_{n-1}),x_n),$$
$$c_i^{(n)}(y) = c_i^{(n-1)}(c_1(y)) \quad \text{при } 1 \le i < n, \quad c_n^{(n)}(y) = c_2(y).$$

Из последнего определения, в частности, следует, что $c_n^i(y)$ является примитивно рекурсивной функцией не только от y, но и от n и i.

6.11. Функция Гёделя. Наряду с координатными функциями, нам понадобится и так называемая функция Гёделя $\Gamma(x,y)$. Примитивно рекурсивная функция двух аргументов $\Gamma(x,y)$ называется функцией Гёделя, если для любого m и любого набора $a_0, a_1, \dots, a_m \in \mathbb{N}_0$ существует число $t \in \mathbb{N}_0$, такое что $\Gamma(t,0) = a_0, \Gamma(t,1) = a_1, .., \Gamma(t,m) = a_m$. Примером функции Гёделя является введенная в предыдущем пункте функция $\exp(x,y)$; точнее, функция $\Gamma(x,y) = \exp(y,x)$ является функцией Гёделя, так как для любых $a_0, a_1, \dots, a_m \in \mathbb{N}_0$ имеем для $t = p_o^{a_0} p_1^{a_1} \cdots p_m^{a_m}$:

$$\begin{aligned} \Gamma(t,0) &= \exp(0,t) = a_0, \\ \Gamma(t,1) &= \exp(1,t) = a_1, \\ &\dots \\ \Gamma(t,m) &= \exp(m,t) = a_m\,. \end{aligned}$$

Функция Гёделя, как и координатные функции, определена неоднозначно. Зафиксируем раз и навсегда какие-то координатные функции и функцию Гёделя.

7. Рекурсивно перечислимые множества

7.1. Определение рекурсивно перечислимого множества чисел.

Теорема. *Пусть M – непустое подмножество множества натуральных чисел $\mathbb{N}_0$. Следующие условия равносильны:*

(1) *для некоторого n существует примитивно рекурсивная функция от n переменных $f(x_1,\dots,x_n)$, множество значений которой совпадает с M;*
(2) *существует примитивно рекурсивная функция $f(x)$, множество значений которой совпадает с M;*
(3) *существует примитивно рекурсивная функция $h(a,x)$, такая что уравнение $h(a,x)=0$ (относительно неизвестной x) имеет решение тогда и только тогда, когда $a \in M$;*

(4) *для некоторого n существует такая примитивно рекурсивная функция $h(a, x_1, \dots, x_n)$ от $n+1$ переменных, что уравнение $h(a, x_1, \dots, x_n) = 0$ (относительно неизвестных $x_1, \dots, x_n$) имеет решение тогда и только тогда, когда $a \in M$.*

Доказательство. (1)⇒(2). Пусть $f(x_1, \dots, x_n)$ – примитивно рекурсивная функция, множество значений которой совпадает с M; тогда множество значений функции $g(x) = f(c_1(x), \dots, c_n(x))$, где $c_1, .., , c_n$ – координатные функции, тоже совпадает с M. (2)⇒(3). Пусть $f(x)$ – примитивно рекурсивная функция, множество значений которой совпадает с M; положим $h(a, x) = |f(x) - a|$. Разрешимость уравнения $h(a, x) = 0$ равносильна существованию $x \in \mathbb{N}_0$, такого что $f(x) = a$, т.е. тому, что число a принадлежит множеству значений M функции $f(x)$. (3)⇒(4) – очевидно. (4)⇒(1). Пусть $h(a, x_1, \dots, x_n)$ – такая примитивно рекурсивная функция, что уравнение $h(a, x_1, \dots, x_n) = 0$ разрешимо относительно $x_1, \dots, x_n$ тогда и только тогда, когда $a \in M$. Выберем произвольный элемент $b \in M$ и положим

$$f(x, x_1, \dots, x_n) = x \cdot \overline{\operatorname{sgn}}(h(x, x_1, \dots, x_n)) + b \cdot \operatorname{sgn}(h(x, x_1, \dots, x_n)).$$

Если $x \in M$, то существуют $x_1, \dots, x_n \in \mathbb{N}_0$, для которых $h(x, x_1, \dots, x_n) = 0$ и $f(x, x_1, \dots, x_n) = x \cdot 1 + b \cdot 0 = x$. Таким образом, множество значений функции $f(x, x_1, \dots, x_n)$ содержит M. Обратно, пусть $z = f(x, x_1, \dots, x_n)$ принадлежит множеству значений функции $f(x, x_1, \dots, x_n)$; если $h(x, x_1, \dots, x_n) = 0$, то $z = x$ принадлежит M, так как существует решение $x_1, \dots, x_n$ уравнения $h(x, x_1, \dots, x_n) = 0$, а если $h(x, x_1, \dots, x_n) \neq 0$, то $z = b \in M$. Теорема полностью доказана.

Подмножество M множества $\mathbb{N}_0$ называется рекурсивно перечислимым, если оно либо пусто, либо удовлетворяет равносильным требованиям только что доказанной теоремы.

7.2. Рекурсивно перечислимые подмножества декартовых степеней $\mathbb{N}_0$. Подмножество M декартовой степени $\mathbb{N}_0^n$ множества натуральных чисел называется рекурсивно перечислимым, если подмножество

$$M_0 = \{d^{(n)}(a_1, \dots, a_n) \mid (a_1, \dots, a_n) \in M\}$$

множества $\mathbb{N}_0$ рекурсивно перечислимо (здесь, как и раньше, через $d^{(n)}$ обозначается примитивно рекурсивная функция, нумерующая точки из $\mathbb{N}_0^n$).

Теорема. *Пусть M – непустое подмножество $\mathbb{N}_0^n$; следующие условия равносильны:*

(1) *M рекурсивно перечислимо;*
(2) *для некоторого m существуют такие примитивно рекурсивные функции $f_1(t_1, \dots, t_m), \dots, f_n(t_1, \dots, t_m)$, что M состоит из всех точек вида $(f_1(t_1, \dots, t_m), \dots, f_n(t_1, \dots, t_m))$, где $t_1, \dots, t_m$ независимо пробегают $\mathbb{N}_0$;*
(3) *существуют примитивно рекурсивные функции $f_1(t), \dots, f_n(t)$, такие что M состоит из всех точек $(f_1(t), \dots, f_n(t))$, $t \in \mathbb{N}_0$;*

(4) *существует примитивно рекурсивная функция* $h(a_1, \dots, a_n, x)$, *такая что уравнение* $h(a_1, \dots, a_n, x) = 0$ *(относительно неизвестной* x*) имеет решение тогда и только тогда, когда* $(a_1, \dots, a_n) \in M$;

(5) *для некоторого* m *существует такая примитивно рекурсивная функция* $h(a_1, \dots, a_n, x_1, \dots, x_m)$ *от* $n + m$ *переменных, что уравнение*

$$h(a_1, \dots, a_n, x_1, \dots, x_n) = 0$$

(относительно неизвестных $x_1, \dots, x_n$*) имеет решение тогда и только тогда, когда* $(a_1, \dots, a_n) \in M$.

Доказательство. Повторяя доказательство теоремы 5.1, мы получим равносильность условий (2)-(5); остается установить равносильность (1) и (3).

(1)⇒(3). Если $M \subseteq \mathbb{N}_0^n$ – рекурсивно перечислимое множество, то, по определению, множество $M_0 = \{d^{(n)}(a_1, \dots, a_n) \,|\, (a_1, \dots, a_n) \in M\}$ является рекурсивно перечислимым подмножеством $\mathbb{N}_0$ и потому совпадает с множеством значений некоторой примитивно рекурсивной функции $f(t)$. Координатные функции $c_1^{(n)}, \dots, c_n^{(n)}$ осуществляют отображение $\mathbb{N}_0 \to \mathbb{N}_0^n$, обратное к $d^{(n)}$; поэтому M – это множество точек $(f_1(t), \dots, f_n(t))$, где через $f_i(t)$ обозначены примитивно рекурсивные функции $c_i^{(n)}(f(t))$ $(1 \le i \le n)$.

(3)⇒(1).Пусть M – множество точек $(f_1(t), \dots, f_n(t))$, где t пробегает $\mathbb{N}_0$, а $f_1(t), \dots, f_n(t)$ – примитивно рекурсивные функции. Тогда множество $M_0 = \{d^{(n)}(a_1, \dots, a_n) \,|\, (a_1, \dots, a_n) \in M\}$ представляет собой множество значений примитивно рекурсивной функции $d^{(n)}(f_1(t), \dots, f_n(t))$ и потому является рекурсивно перечислимым подмножеством $\mathbb{N}_0$. Но это и означает, что множество $M \subseteq \mathbb{N}_0^n$ рекурсивно перечислимо.

7.3. Свойства рекурсивно перечислимых множеств. Покажем, что объединение и пересечение конечного числа рекурсивно перечислимых множеств рекурсивно перечислимы. Действительно, пусть $f_i(a_1, \dots a_n, x)$ $(1 \le i \le k)$ – такие примитивно рекурсивные функции, что уравнение относительно x

$$f_i(a_1, \dots, a_n, x) = 0$$

тогда и только тогда имеет решение, когда $(a_1, \dots, a_n) \in M_i$. Функции

$$f(a_1, \dots, a_n, x_1, \dots, x_k) = \sum_{i=1}^{k} f_i(a_1, \dots, a_n, x_i)\,,$$

$$g(a_1, \dots, a_n, x_1, \dots, x_k) = \prod_{i=1}^{k} f_i(a_1, \dots, a_n, x_i)$$

примитивно рекурсивны, и уравнения

$$f(a_1, \dots, a_n, x_1, \dots, x_k) = 0, \quad g(a_1, \dots, a_n, x_1, \dots, x_k) = 0$$

разрешимы относительно $x_1, \dots, x_k$ тогда и только тогда, когда $(a_1, \dots, a_n)$ принадлежит соответственно пересечению и объединению множеств $M_1, \dots, M_k$.

8. Рекурсивные функции

8.1. Определение рекурсивных функций. В свойствах примитивно рекурсивных функций, приведенных в предыдущей главе, отсутствовало упоминание обратных функций. И это не случайно: обратная к примитивно рекурсивной функции, даже если она существует, не обязана быть примитивно рекурсивной.

При нашем подходе к определению рекурсивной функции мы будем пользоваться понятием графика функции. Пусть $f(x_1, \dots, x_n)$ – некоторая функция; её графиком называется множество точек $(x_1, \dots, x_n, f(x_1, \dots, x_n)) \in \mathbb{N}_0^{n+1}$, где $x_1, \dots, x_n$ независимо пробегают множество натуральных чисел $\mathbb{N}_0$. Функция $f(x_1, \dots, x_n)$ называется рекурсивной (в другой терминологии общерекурсивной), если её график рекурсивно перечислим. Отметим простейшие свойства рекурсивных функций. Всякая примитивно рекурсивная функция рекурсивна. Действительно, если $f(x_1, \dots, x_n)$ – примитивно рекурсивная функция, то её график – множество всех точек $(x_1, \dots, x_n, f(x_1, \dots, x_n))$; но все координаты $x_1, \dots, x_n, f(x_1, \dots, x_n)$ – примитивно рекурсивные функции от $x_1, \dots, x_n$, и по теореме 5.2 это множество рекурсивно перечислимо. Пусть $f(x_1, \dots, x_n)$ – рекурсивная функция; поскольку её график рекурсивно перечислим, существуют такие примитивно рекурсивные функции $g_1(t), \dots, g_n(t), g(t)$, что этот график состоит из точек $(g_1(t), \dots, g_n(t), g(t))$. Поскольку $x_1, \dots, x_n$ независимо друг от друга пробегают $\mathbb{N}_0$ и определяют значение функции f, функции $g_1(t), \dots, g_n(t), g(t)$ обладают свойствами:

(1) для любых чисел $x_1, \dots, x_n \in \mathbb{N}_0$ найдется число $t \in \mathbb{N}_0$, для которого $g_1(t) = x_1, \dots, g_n(t) = x_n$;
(2) если $g_1(t) = g_1(t'), \dots, g_n(t) = g_n(t')$, то $g(t) = g(t')$;
(3) $f(g_1(t), \dots, g_n(t)) = g(t)$ для любого $t \in \mathbb{N}_0$.

Предшествующее представление рекурсивной функции будем называть её примитивно рекурсивной параметризацией. Из существования параметризации сразу следует, что всякая рекурсивная функция может быть получена из примитивно рекурсивных при помощи подстановки и единственный раз примененной операции минимизации (см. 6.8). Действительно, для указанной параметризации

$$f(x_1, \dots, x_n) = g(\mu_t(|g_1(t) - x_1| + \dots + |g_n(t) - x_n|)).$$

Отметим, что по свойству (1) уравнение $|g_1(t) - x_1| + \dots + |g_n(t) - x_n| = 0$ всегда имеет решение t, так что функция $\mu_t(|g_1(t) - x_1| + \dots + |g_n(t) - x_n|)$ имеет смысл.

8.2. Подстановка для рекурсивных функций.

Теорема. *Пусть $f(x_1, \dots, x_n)$, $g_1(y_1, \dots, y_m)$, $\dots$, $g_n(y_1, \dots, y_m)$ – рекурсивные функции. Тогда функция $h(y_1, \dots, y_m)$, получающаяся из f подстановкой вместо неизвестных функций $g_1, \dots, g_n$ (так что $h = t[f, g_1, \dots, g_n]$), тоже рекурсивна.*

Доказательство. Пусть

$$\Delta = \{(p_1(t), \dots p_n(t), p(t)) \mid t \in \mathbb{N}_0\},$$
$$\Sigma_i = \{(q_{i1}(s_i), \dots q_{im}(s_i), q_i(s_i)) \mid s_i \in \mathbb{N}_0\}$$

– графики функций f, g_i $(1 \le i \le n)$ с примитивно рекурсивными компонентами p_i, q_{ij}, p, q_i. Для того, чтобы точка $(a_1, \dots, a_m, a)$ принадлежала графику Λ функции h, необходимо и достаточно, чтобы существовали такие $t, s_1, \dots, s_n$ и $x_1, \dots, x_n$, что

$$q_{i1}(s_i) = a_1, \dots, q_{im}(s_i) = a_m,\ q_i(s_i)) = x_i \quad (1 \le i \le n)$$

(эти равенства означают, что $g_i(a_1, \dots, a_m) = x_i$),

$$p_1(t) = x_1, \dots, p_n(t) = x_n,\ p(t) = b$$

(это значит, что $f(x_1, \dots, x_n) = b$). Но эта система равенств равносильна одному уравнению

$$|p(t) - b| + \sum_{i=1}^{n}(|q_i(s_i) - x_i| + |p_i(t) - x_i|) + \sum_{j=1}^{m}|q_{ij}(s_i) - a_j|) = 0\,,$$

левая часть которого – примитивно рекурсивная функция от $a_1, ..., a_m, b, t$, $s_1, ..., s_n, x_1, ..., x_n$. Таким образом, $(a_1, \dots, a_m, b) \in \Lambda$ тогда и только тогда, когда наше уравнение разрешимо относительно $t, s_1, \dots, s_n, x_1, \dots, x_n$. По теореме 5.2 это означает, что график Λ функции h рекурсивно перечислим, т.е. сама функция $h(y_1, \dots, y_m)$ рекурсивна.

8.3. Минимизация для рекурсивных функций.

Теорема. *Пусть $f(x_1, \dots, x_n, t)$ – такая рекурсивная функция, что для любых $x_1, \dots, x_n \in \mathbb{N}_0$ существует решение t уравнения $f(x_1, \dots, x_n, t) = 0$. Тогда функция $(\mu_t f)(x_1, \dots, x_n)$ также рекурсивна.*

Доказательство. Пусть

$$\Delta = \{(p_1(s), \dots p_n(s), p(s), q(s))\ |s \in \mathbb{N}_0\}$$

– график функции f с примитивно рекурсивными компонентами p_i, p, q. Для того, чтобы точка $(x_1, \dots, x_n, a)$ принадлежала графику Λ функции $\mu_t f$, необходимо и достаточно, чтобы

$$f(x_1, \dots, x_n, 0) \ne 0, \dots, f(x_1, \dots, x_n, a \ominus 1) \ne 0,\ f(x_1, \dots, x_n, a) = 0\,.$$

Для этого необходимо, чтобы для $i = 0, 1, \dots, a$ существовали значения параметра s_i, для которых

$$p_1(s_i) = x_1, \dots, p_n(s_i) = x_n,\ p(s_i) = i\,,$$
$$q(s_i) \ne 0,\ \text{если } i < a, \quad q(s_a) = 0\,.$$

К сожалению, количество неизвестных s_i зависит от a; чтобы устранить это неудобство, используем функцию Гёделя $\Gamma(s, i)$. Согласно определению этой примитивно рекурсивной функции существует число $s \in \mathbb{N}_0$, такое что

$\Gamma(s,0)=s_0,\ \Gamma(s,1)=s_1,..,\Gamma(s,a)=s_a$. Подставляя эти выражения в предыдущие равенства, преобразуем их к системе уравнений

$$p_1(\Gamma(s,i))=x_1,\dots,p_n(\Gamma(s,i))=x_n,\ p(\Gamma(s,i))=i\,,$$
$$\overline{\mathrm{sgn}}(q(\Gamma(s,i)))=0,\ \text{если } i<a,\quad \mathrm{sgn}(q(\Gamma(s,a)))=0\,,$$

которая равносильна одному уравнению

$$\mathrm{sgn}(q(\Gamma(s,a)))+\sum_{i=0}^{a\ominus 1}\overline{\mathrm{sgn}}(q(\Gamma(s,i)))+\sum_{i=0}^{a}(|p(\Gamma(s,i))-i|+\sum_{j=1}^{n}|p_j(\Gamma(s,i))-x_j|)=0\,,$$

левая часть которого – примитивно рекурсивная функция от $a,s,x_1,\dots,x_n$. Таким образом, $(x_1,\dots,x_n,a)$ принадлежит графику Λ функции $\mu_t f$ тогда и только тогда, когда наше уравнение разрешимо относительно s. По теореме 5.2 это означает, что график Λ рекурсивно перечислим, т.е. сама функция $(\mu_t f)(x_1,\dots,x_n)$ рекурсивна.

8.4. Примитивная рекурсия для рекурсивных функций.

Теорема. *Пусть $h(x_1,\dots,x_{n-1})$, $g(x_1,\dots,x_{n-1},x_n,x_{n+1})$ – рекурсивные функции. Тогда функция $f(x_1,\dots,x_n)$, полученная из них примитивной рекурсией, также рекурсивна.*

Доказательство. Пусть

$$\Delta=\{(p_1(s),\dots p_{n-1}(s),p(s))\ |s\in\mathbb{N}_0\}\,,$$
$$\Sigma=\{(q_1(t),\dots q_{n-1}(t),q_n(t),q_{n+1}(t),q(t))\ |t\in\mathbb{N}_0\}$$

– графики функций h, g с примитивно рекурсивными компонентами p_i, q_j, p, q. Точки

$$(x_1,\dots,x_{n-1},0,y_0),$$
$$(x_1,\dots,x_{n-1},1,y_1),$$
$$\dots$$
$$(x_1,\dots,x_{n-1},a,y_a)$$

принадлежат графику Λ функции f тогда и только тогда, когда

$$\begin{aligned}y_0&=h(x_1,\dots,x_{n-1}),\\ y_1&=g(x_1,\dots,x_{n-1},0,y_0),\\ y_2&=g(x_1,\dots,x_{n-1},1,y_1),\\ &\dots\\ y_a&=g(x_1,\dots,x_{n-1},a\ominus 1,y_{a\ominus 1})\,,\end{aligned}$$

т.е. точка $(x_1,\dots,x_{n-1},,y_0)$ принадлежит Δ, а точки $(x_1,\dots,x_{n-1},i,y_i,y_{i+1})$ $(0\le i<a)$ принадлежат Σ. Для этого необходимо и достаточно существование таких s_0, $s_1,\dots,s_a$, что

$$p_1(s_0)=x_1,\dots,p_{n-1}(s_0)=x_{n-1},\ p(s_0)=y_0,$$
$$q_1(s_i)=x_1,\dots,q_{n-1}(s_i)=x_{n-1},\ q_n(s_i)=i\ominus 1,\ ,q_{n+1}(s_i)=y_{i\ominus 1}\,,q(s_i)=y_i$$

$(1 \le i \le a)$. Исключая из этой системы равенств величины $y_0, y_1, \dots y_{a-1}$ и обозначая y_a через b, находим, что для того, чтобы точка $(x_1, \dots, x_{n-1}, a, b)$ принадлежала графику Λ функции f, необходимо и достаточно, чтобы существовали s_0, $s_1, \dots, s_a \in \mathbb{N}_0$, такие что

$$\begin{gathered} p_1(s_0) = x_1, \dots, p_{n-1}(s_0) = x_{n-1},\ p(s_0) = q_{n+1}(s_1), \\ q_1(s_i) = x_1, \dots, q_{n-1}(s_i) = x_{n-1},\ q_n(s_i) = i \ominus 1 \quad (1 \le i \le a)\,, \\ q(s_i) = q_{n+1}(s_{i+1}) \quad (1 \le i < a)\,, \quad q(s_a) = b\,. \end{gathered}$$

Заменяя, как и выше, неизвестные s_i на $\Gamma(s, i)$, преобразуем эти равенства к системе уравнений

$$\begin{gathered} p_1(\Gamma(s,0)) = x_1, \dots, p_{n-1}(\Gamma(s,0)) = x_{n-1},\ p(\Gamma(s,0)) = q_{n+1}(\Gamma(s,1)), \\ q_1(\Gamma(s,i)) = x_1, \dots, q_{n-1}(\Gamma(s,i)) = x_{n-1},\ q_n(\Gamma(s,i)) = i \ominus 1 \quad (1 \le i \le a)\,, \\ q(\Gamma(s,i)) = q_{n+1}(\Gamma(s,i+1)) \quad (1 \le i < a)\,, \quad q(\Gamma(s,a)) = b\,, \end{gathered}$$

которая равносильна одному уравнению

$$|p(\Gamma(s,0)) - q_{n+1}(\Gamma(s,1))| + \sum_{i=1}^{a-1} |q(\Gamma(s,i)) - q_{n+1}(\Gamma(s,i+1))| + |q(\Gamma(s,a)) - b| + \\ \sum_{j=1}^{n-1} (|p_j(\Gamma(s,0)) - x_j| + \sum_{i=1}^{a} |q_j(\Gamma(s,0)) - x_j|) + \sum_{i=1}^{a} |q_n(\Gamma(s,i)) - (i \ominus 1)| = 0\,,$$

левая часть которого представляет собой примитивно рекурсивную функцию от $a, b, s, x_1, \dots, x_{n-1}$. Таким образом, $(x_1, \dots, x_{n-1}, a, b)$ принадлежит графику Λ функции f тогда и только тогда, когда наше уравнение разрешимо относительно s. По теореме 5.2 это означает, что график Λ рекурсивно перечислим, т.е. сама функция $f(x_1, \dots, x_n)$ рекурсивна.

8.5. Другое описание класса рекурсивных функций. Соединяя результаты предыдущих пунктов, мы получаем следующую характеризацию рекурсивных функций.

Теорема. *Класс рекурсивных функций совпадает с классом функций, которые могут быть получены из элементарных функций* o, s, id, pr_1, pr_2 *при помощи применения (вообще говоря, многократного) операций подстановки, примитивной рекурсии и минимизации.*

Доказательство. В конце пункта 6.1 было отмечено, что любая рекурсивная функция получается минимизацией из примитивно рекурсивной функции, которая, в свою очередь, может быть получена из элементарных функция подстановками и примитивными рекурсиями. Таким образом, класс рекурсивных функций содержится в классе функций, которые могут быть получены из элементарных функций при помощи подстановок, примитивных рекурсий и минимизаций. Обратно, элементарные функции рекурсивны, и теоремы 6.2–6.4 показывают, что подстановки, примитивные рекурсии и минимизации не выводят за пределы класса рекурсивных функций, который, таким образом,

содержит класс функций, которые получаются из элементарных подстановками, примитивными рекурсиями и минимизациями.

До сих пор у нас не было ни одного примера рекурсивных, но не примитивно рекурсивных функций; в следующих пунктах мы докажем существование таких функций.

8.6. Рекурсия второй ступени. Напомним, что координатные функции $c_1, c_2 : \mathbb{N}_0 \to \mathbb{N}_0$, $d^{(2)} : \mathbb{N}_0^2 \to \mathbb{N}_0$ примитивно рекурсивны, и отображение $x \rightsquigarrow (c_1(x), c_2(x))$, $(x, y) \rightsquigarrow d^{(2)}(x, y)$ являются взаимно обратными соответствиями между множеством $\mathbb{N}_0$ и его декартовым квадратом.

При вычислении значений функции, получающейся при помощи примитивной рекурсии, мы должны знать значения этой функции для меньших значений аргумента. Рассмотрим теперь функцию от двух аргументов, определяемую следующим образом:

$$f(0,0) = a,$$
$$f(x,y) = g(x, y, f(c_1(\varphi(x,y)), c_2(\varphi(x,y)))),$$

где $a \in \mathbb{N}_0$, $g(x,y,z)$, $\varphi(x,y)$ — примитивно рекурсивные функции, причем $\varphi(x,y) < d^{(2)}(x,y)$. Нетрудно видеть, что функция $f(x,y)$ корректно определена и примитивно рекурсивна. Действительно, функция $h(z)$, определенная условиями

$$h(0) = a,$$
$$h(z) = g(c_1(z), c_2(z), h((\varphi(c_1(z), c_2(z))))),$$

примитивно рекурсивна, а $f(x,y) = h(d^{(2)}(x,y))$. Предыдущее построение по существу использует полное упорядочение декартова квадрата множества $\mathbb{N}_0$, причем получившееся вполне упорядоченное множество снова изоморфно $\mathbb{N}_0$. Однако, декартов квадрат множества $\mathbb{N}_0$ допускает и другие полные упорядочения, например, лексикографическое. Будем обозначать лексикографический порядок на $\mathbb{N}_0^2$ символом $\preceq$:

$$(x,y) \preceq (z,t), \quad \text{если } x < z \text{ или } x = z, y \le t.$$

Лексикографический порядок позволяет определить новый способ построения функций, который мы будем называть рекурсией второй ступени. Пусть $\varphi(x,y,z)$, $\psi(x,y,z)$, $\alpha(x,y)$, $\beta(x,y)$ — такие примитивно рекурсивные функции, что $(\alpha(x,y), \beta(x,y)) \prec (x,y)$, $(\varphi(x,y,z), \psi(x,y,z)) \prec (x,y)$ для любой пары $(x,y) \in \mathbb{N}_0^2$, $(x,y) \ne (0,0)$, и любого $z \in \mathbb{N}_0$. Пусть, далее, $a \in \mathbb{N}_0$ и $g(x,y,z,t)$ — примитивно рекурсивная функция, и пусть $f(x,y)$ — такая функция, что

$$f(0,0) = a,$$
$$f(x,y) = g(x, y, f(u,v), f(\varphi(x,y,f(u,v)), \psi(x,y,f(u,v)))),$$

где $u = \alpha(x,y)$, $v = \beta(x,y)$. Покажем, что функция $f(x,y)$ полностью определена этими свойствами. Точнее говоря, мы докажем более точное утверждение. Назовем набор точек $(x,y) = (x_0,y_0) \succ (x_1,y_1) \succ \cdots \succ (x_m,y_m) = (0,0)$ и

чисел $z_0, z_1, \ldots, z_m$ вычисляющим значение функции f в точке (x, y), если для любого i, $0 \leq i < m$, существуют номера $j, l > i$, для которых $\alpha(x_i, y_i) = x_j$, $\beta(x_i, y_i) = y_j$, $\varphi(x_i, y_i, z_j) = x_l$, $\psi(x_i, y_i, z_j) = y_l$, $g(x_i, y_i, z_j, z_l) = z_i$; обратной индукцией по i находим, что из этих условий следует, что $z_i = f(x_i, y_i)$; в частности, значение функции $f(x, y) = f(x_0, y_0)$ равно z_0. Мы утверждаем, что вычисляющие наборы есть для всех точек $(x, y) \in \mathbb{N}_0^2$, и потому все значения функции $f(x, y)$ однозначно определены наложенными условиями. Если бы это было не так, то, поскольку множество $\mathbb{N}_0^2$ вполне упорядочено относительно лексикографического порядка, нашлась бы наименьшая пара (x, y), для которой нет вычисляющего набора; ясно, что $(x, y) \neq (0, 0)$. Но пара $(u, v) = (\alpha(x, y), \beta(x, y))$ предшествует паре (x, y), поэтому для нее есть набор M с нужными свойствами. В частности, определено значение $f(u, v)$. По нашему предположению, $(\varphi(x, y, f(u, v)), \psi(x, y, f(u, v)) \prec (x, y)$, и потому для пары

$$(\varphi(x, y, f(u, v)), \psi(x, y, f(u, v)))$$

тоже есть вычисляющий набор N. Но ясно, что объединение наборов M_1 и N после перенумерации, располагающей все точки объединения в порядке возрастания, и добавления точки (x, y) и числа

$$g(x, y, f(u, v), f(\varphi(x, y, f(u, v)), \psi(x, y, f(u, v))))$$

становится набором, вычисляющим значение функции f в точке (x, y), а это противоречит предположению о том, что таких наборов не существует. В описанной ситуации мы говорим, что функция $f(x, y)$ получена рекурсией второй ступени при помощи функций $g(x, y, z, t)$, $\varphi(x, y, z)$, $\psi(x, y, z)$, $\alpha(x, y)$, $\beta(x, y)$ при начальном условии $f(0, 0) = a$.

Теорема. *Функция, полученная из примитивно рекурсивных функций рекурсией второй ступени, рекурсивна.*

Доказательство. Пусть $\Delta \subseteq \mathbb{N}_0^3$ — график функции $f(x, y)$. Из предыдущих рассуждений видно, что точка (x, y, z) принадлежит графику Δ тогда и только тогда когда существуют такие числа m, x_i, y_i, z_i $(0 \leq i \leq m)$, что $x = x_0$, $y = y_0$, $z = z_0$ и для каждого i, $0 \leq i \leq m$, существуют числа j, l, $0 \leq j, k, l \leq m$, для которых $\alpha(x_i, y_i) = x_j$, $\beta(x_i, y_i) = y_j$, $\varphi(x_i, y_i, z_j) = x_l$, $\psi(x_i, y_i, z_j) = y_l$, $g(x_i, y_i, z_j, z_l) = z_i$. Эти условия равносильны одному равенству

$$|x - x_0| + |y - y_0| + |z - z_0| + \sum_{i=0}^{m} \Big(\prod_{j,l=0}^{m} (|\alpha(x_i, y_i) - x_j| + |\beta(x_i, y_i) - y_j| +$$
$$|\varphi(x_i, y_i, z_j) - x_l| + |\psi(x_i, y_i, z_j) - y_l| + |g(x_i, y_i, z_j, z_l) - z_i|) \Big) = 0.$$

Заменяя, как и выше, переменные x_i, y_i, z_i на $\Gamma(s, i)$, $\Gamma(t, i)$, $\Gamma(u, i)$, преобразуем это соотношение в равенство

$$|x - \Gamma(s, 0)| + |y - \Gamma(t, 0)| + |z - \Gamma(u, 0)| +$$
$$\sum_{i=0}^{m} \Big(\prod_{j,l=0}^{m} (|\alpha(\Gamma(s, i), \Gamma(t, i)) - \Gamma(s, j)| + |\beta(\Gamma(s, i), \Gamma(t, i)) - \Gamma(t, j)| +$$
$$|\varphi(\Gamma(s, i), \Gamma(t, i), \Gamma(u, j)) - \Gamma(s, l)| + |\psi(\Gamma(s, i), \Gamma(t, i), \Gamma(u, j)) - \Gamma(t, l)| +$$
$$|g(\Gamma(s, i), \Gamma(t, i), \Gamma(u, j), \Gamma(u, l)) - \Gamma(u, i)|) \Big) = 0.$$

Обозначим левую часть этого равенства через $h(x,y,z,m,s,t,u)$; ясно, что это примитивно рекурсивная функция. Таким образом, $(x,y,z)\in\Delta$ тогда и только тогда, когда уравнение $h(x,y,z,m,s,t,u)=0$ с примитивно рекурсивной левой частью разрешимо относительно m, s, t, u. Следовательно, график Δ функции $f(x,y)$ рекурсивно перечислим, и потому сама функция $f(x,y)$ рекурсивна.

9. Функция, универсальная для класса примитивно рекурсивных функций

9.1. Нумерация примитивно рекурсивных функций. Напомним, что любую примитивно рекурсивную функцию можно построить, исходя из элементарных функций $o(x)$, $s(x)$, $\mathrm{id}(x)$, $\mathrm{pr}_1(x_1,x_2)$, $\mathrm{pr}_2(x_1,x_2)$ при помощи подстановок и примитивных рекурсий. Процесс построения примитивно рекурсивной функции может быть закодирован в некотором алфавите, и, используя взаимно однозначное соответствие между словами в алфавите и натуральными числами, мы можем сопоставить нашей функции (точнее, процессу ее построения: одна и та же функция может быть получена из элементарных многими способами) некоторое натуральное число. Конечно, это можно сделать многими способами; здесь мы изложим один из вариантов такого сопоставления. Существенную роль в нашей конструкции играют примитивно рекурсивные функции $d^{(k)}(x_1,\dots,x_k)$, $c_1^{(k)}(x),\dots,c_k^{(k)}(x)$ из §6.10, осуществляющие взаимно обратные биекции $\mathbb{N}_0^k\to\mathbb{N}_0$, $\mathbb{N}_0\to\mathbb{N}_0^k$. Напомним (см. §6.10), что

$$c_i^{(k)}(d^{(k)}(x_1,\dots,x_k))=x_i,\quad d^{(2)}(d^{(k-1)}(x_1,\dots,x_{k-1}),x_k)=d^{(k)}(x_1,\dots,x_k).$$

Пусть $n\in\mathbb{N}_0$; построим примитивно рекурсивную функцию $f_n(x)$ одной переменной. Сначала определим эту функцию для первых значений n:

$$f_0(x)=o(x)=0,$$
$$f_1(x)=s(x)=x+1.$$

Пусть теперь $n>1$ и примитивно рекурсивные функции $f_m(x)$ уже определены для всех $m<n$. Число n однозначно раскладывается в произведение простых множителей: $n=2^{i_0}3^{i_1}\dots p_r^{i_r}$. Если $k=i_0\geq 1$, то положим

$$f_n(x)=f_{i_1}(d^{(k)}(f_{i_2}(x),\dots,f_{i_{1+k}}(x))).$$

Если $i_0=0$, но $i_1\geq 1$, т.е. $n=3^{i+1}5^j\dots p_r^{i_r}$ $(a\geq 0,\ j\geq 0,\ r\geq 2)$, то в качестве $f_n(x)$ возьмем функцию, получающуюся следующей примитивной рекурсией:

$$f_n(d^{(2)}(x,0))=f_i(x),$$
$$f_n(d^{(2)}(x,y+1))=f_j(d^{(2)}(d^{(2)}(x,y),f_n d^{(2)}(x,y))).$$

Если $i_0=i_1=0$, $i_2=1,2,3$, то в качестве функции $f_n(x)$ возьмем соответственно функции $\mathrm{id}(x)$, $c_1(x)$, $c_2(x)$. Во всех остальных случаях (т.е. при $i_0=i_1=0$ и $i_3=0$ или $i_3>3$) положим $f_n(x)=o(x)=0$.

Теорема. *Для любой примитивно рекурсивной функции $g(x)$ найдется номер $n \in \mathbb{N}_0$, такой что $g(x) = f_n(x)$ для всех $x \in \mathbb{N}_0$.*

Доказательство. Наше определение примитивно рекурсивной функции таково, что в нем участвуют функции от разного числа переменных, и даже при построении примитивно рекурсивных функций от одной переменной нам не обойтись без использования функций нескольких переменных. Поэтому нам придется несколько усилить доказываемое утверждение. Для любых натуральных чисел $k \geq 1$, n обозначим через f_n^k следующую функцию k переменных:

$$f_n^k(x_1, \ldots, x_k) = f_n(d^{(k)}(x_1, \ldots, x_k)).$$

Мы будем доказывать следующее утверждение:

Для любой примитивно рекурсивной функции от k переменных $g(x_1, \ldots, x_k)$ найдется номер $n \in \mathbb{N}_0$, такой что $g(x_1, \ldots, x_k) = f_n^k(x_1, \ldots, x_k)$ для всех $x_1, \ldots, x_k \in \mathbb{N}_0$.

По определению, примитивно рекурсивная функция $g(x_1, \ldots, x_k)$ является элементарной или получается из ранее построенных функций подстановкой или примитивной рекурсией. Мы будем доказывать наше утверждение индукцией по построению функции g. Убедимся сначала, что оно верно для элементарных функций:

$$o(x) = f_0(x) = f_0^1(x), \quad s(x) = f_1(x) = f_1^1(x), \quad \mathrm{id}(x) = f_5(x) = f_5^1(x),$$
$$\mathrm{pr}_1(x, y) = x = c_1(d^{(2)}(x, y)) = f_{25}(d^{(2)}(x, y)) = f_{25}^2(x, y)),$$
$$\mathrm{pr}_2(x, y) = y = c_2(d^{(2)}(x, y)) = f_{125}(d^{(2)}(x, y)) = f_{125}^2(x, y)).$$

Пусть теперь $g(x_1, \ldots, x_k) = h(q_1(x_1, \ldots, x_k), \ldots, q_l(x_1, \ldots, x_k))$ и пусть уже найдены такие номера j, i_1, $\ldots$, i_l, что

$$h(y_1, \ldots, y_l) = f_j^l(y_1, \ldots, y_l),$$
$$q_s(x_1, \ldots, x_k) = f_{i_s}^k(x_1, \ldots, x_k)$$

для $s = 1, \ldots, l$ и любых $x_1, \ldots, x_k, y_1, \ldots, y_l \in \mathbb{N}_0$. Для сокращения записи введем обозначения $\overrightarrow{x} = (x_1, \ldots, x_k)$, $z = d^{(k)}(x_1, \ldots, x_k)$. Для $n = 2^l 3^{i_1} \ldots p_{l+1}^{i_{l+1}}$ находим, что

$$g(x_1, \ldots, x_k) = h(q_1(\overrightarrow{x}), \ldots, q_l(\overrightarrow{x})) =$$
$$f_j^l(f_{i_1}^k(\overrightarrow{x}), \ldots, f_{i_l}^k(\overrightarrow{x})) = f_j(d^{(l)}(f_{i_1}^k(\overrightarrow{x}), \ldots, f_{i_l}^k(\overrightarrow{x})))$$
$$= f_j(d^{(l)}(f_{i_1}(z), \ldots, f_{i_l}(z))) = f_n(z) = f_n^k(x_1, \ldots, x_k).$$

Пусть, наконец, функция $g(x_1, \ldots, x_k)$ получена примитивной рекурсией

$$g(x_1, \ldots, x_{k-1}, 0) = h(x_1, \ldots, x_{k-1}),$$
$$g(x_1, \ldots, x_{k-1}, x_k + 1) = q(x_1, \ldots, x_{k-1}, x_k, g(x_1, \ldots, x_{k-1}, x_k)),$$

и пусть уже найдены такие номера i, j, что $h(x_1, \ldots, x_{k-1}) = f_i^{k-1}(x_1, \ldots, x_{k-1})$, $q(x_1, \ldots, x_{k-1}, x_k, y) = f_j^{k+1}(x_1, \ldots, x_{k-1}, x_k, y)$. Положим $n = 3^{i+1}5^j$; тогда

$$\begin{aligned} f_n^k(x_1, \ldots, x_{k-1}, 0) &= f_n(d^{(k)}(x_1, \ldots, x_{k-1}, 0)) = f_n(d^{(2)}(d^{(k-1)}(x_1, \ldots, x_{k-1}), 0)) \\ &= f_i(d^{(k-1)}(x_1, \ldots, x_{k-1})) = f_i^{k-1}(x_1, \ldots, x_{k-1}) = h(x_1, \ldots, x_{k-1}). \end{aligned}$$

Далее, обозначая для краткости $t = d^{(k-1)}(x_1, \ldots, x_{k-1})$ и пользуясь тем, что $d^{(k)}(x_1, \ldots, x_{k-1}, y) = d^{(2)}(d^{(k-1)}(x_1, \ldots, x_{k-1}), y) = d^{(2)}(t, y)$, находим:

$$\begin{aligned} f_n^k(x_1, \ldots, x_k + 1) &= f_n(d^{(k)}(x_1, \ldots, x_k + 1)) = f_n(d^{(2)}(t, x_k + 1)) \\ &= f_j(d^{(2)}(d^{(2)}(t, x_k), f_n(d^{(2)}(t, x_k)))) \\ &= f_j(d^{(2)}(d^{(k)}(x_1, \ldots, x_{k-1}, x_k), f_n(d^{(k)}(x_1, \ldots, x_{k-1}, x_k)))) \\ &= f_j(d^{(k+1)}(x_1, \ldots, x_k, f_n^k(x_1, \ldots, x_k))) \\ &= f_j^{k+1}(x_1, \ldots, x_k, f_n^k(x_1, \ldots, x_k)) = q(x_1, \ldots, x_k, f_n^k(x_1, \ldots, x_k)). \end{aligned}$$

Таким образом, функция $f_n^k(x_1, \ldots, x_{k-1}, x_k)$ получена той же примитивной рекурсией, что и функция $g(x_1, \ldots, x_{k-1}, x_k)$, и потому эти две функции совпадают. Теорема полностью доказана.

9.2. Универсальная функция для класса примитивно рекурсивных функций. Рассмотрим теперь функцию двух аргументов $U(x, y)$, определенную равенством $U(x, y) = f_x(y)$. Как следует из предыдущей теоремы, для каждой примитивно рекурсивной функции одной переменной $g(x)$ существует число $n \in \mathbb{N}_0$, такое что $g(x) = U(n, x)$ для любого $x \in \mathbb{N}_0$. Таким образом, все примитивно рекурсивные функции легко получаются из одной функции двух переменных $U(x, y)$, и потому естественно называть функцию $U(x, y)$ универсальной для класса примитивно рекурсивных функций.

Теорема. *Функция $U(x, y)$ рекурсивна.*

Доказательство. Из рассуждений предыдущего пункта видно, что построение функции $U(x, y)$ очень похоже на рекурсию второй ступени; однако, если при нашем определении рекурсии второй ступени для вычисления значения функции в точке (x, y) требовалось знать ее значение только в двух точках, то для вычисления значения $U(x, y) = f_x(y)$ в некоторых случаях (например, при подстановке) требуется знать значения функции U в нескольких точках, предшествующих (x, y), причем количество этих точек зависит от (x, y). Мы обойдем эту трудность, заменив функцию $U(x, y)$ тесно связанной с ней функцией $V(x, y) = \prod_{i=0}^{x} p_i^{U(i,y)}$. Докажем, что функция $V(x, y)$ может быть построена рекурсией второй ступени и поэтому она рекурсивна; утверждение теоремы немедленно следует отсюда, так как функция $U(x, y) = \exp(x, V(x, y))$ получается подстановкой в примитивно рекурсивную функцию $\exp(x, z)$ на место второго аргумента рекурсивной функции $V(x, y)$. В процессе доказательства нам будет удобно использовать две вспомогательные примитивно рекурсивные функции.

Лемма. 1. *Функция*

$$w(k,x,z) = d^{(k+1)}(\exp(\exp(2,x)),z),\dots,\exp(\exp(k+2,x),z)$$

примитивно рекурсивна как функция от k, x, z.

2. *Функция* $q(y) = d^{(2)}(c_1(y), c_2(y)\ominus 1)$ *примитивно рекурсивна. Если* $c_2(y) > 0$, *то* $q(y) < y$.

Доказательство. **1.** Эта функция получается примитивной рекурсией

$$\begin{aligned} w(0,x,z) &= \exp(\exp(2,x),z),\\ w(k+1,x,z) &= d^{(k+2)}(\exp(\exp(2,x),z),\dots,\exp(\exp(k+3,x),z))\\ &= d^{(2)}(d^{(k+1)}(\exp(\exp(2,x),z),\dots,\exp(\exp(k+3,x),z)))\\ &= d^{(2)}(w(k,x,z),\exp(\exp(k+3,x),z)). \end{aligned}$$

2. То, что функция $q(y)$ примитивно рекурсивна, очевидно. Если $c_2(y) > 0$, то $c_1(y) + (c_2(y)\ominus 1) < c_1(y) + c_2(y)$. Напомним, что определенные в §6.10 координатные функции нумеруют пары натуральных чисел так, что пара с меньшей суммой координат всегда предшествует паре с большей суммой координат; поэтому номер $q(y) = d^{(2)}(c_1(y), c_2(y)\ominus 1)$ пары $(c_1(y), c_2(y)\ominus 1)$ строго меньше номера $y = d^{(2)}(c_1(y), c_2(y))$ пары $(c_1(y), c_2(y))$.

Вернемся к доказательству того, что функция $V(x,y)$ строится рекурсией второй ступени. Для этого надо построить примитивно рекурсивные функции $\alpha(x,y)$, $\beta(x,y)$, $\varphi(x,y,z)$, $\psi(x,y,z)$, $g(x,y,z,t)$, связанные с функцией $V(x,y)$ как в §8.6:

$$(\alpha(x,y),\beta(x,y)) \prec (x,y), \quad (\varphi(x,y,z),\psi(x,y,z)) \prec (x,y)$$

для любой пары $(x,y) \in \mathbb{N}_0^2$, $(x,y) \neq (0,0)$, и любого $z \in \mathbb{N}_0$,

$$V(x,y) = g(x,y,V(u,v),V(\varphi(x,y,V(u,v)),\psi(x,y,V(u,v)))),$$

где $u = \alpha(x,y)$, $v = \beta(x,y)$. Мы зададим эти функции кусочно, разбив всю область задания на несколько областей.

Случай 1: $x = 0$. Ясно, что $V(0,y) = 2^{U(0,y)} = 2^{f_0(y)} = 2^0 = 1$, и можно положить $\alpha(0,y) = \beta(0,y) = \varphi(0,y,z) = \psi(0,y,z) = 0$, $g(0,y,z,t) = 1$.

Пусть теперь $x \geq 1$; во всех оставшихся случаях $\alpha(x,y) = x\ominus 1$, $\beta(x,y) = y$. Заметим, что при $x \geq 1$ справедливо соотношение

$$V(x,y) = V(x\ominus 1,y)p_x^{U(x,y)} = V(\alpha(x,y),\beta(x,y))p_x^{f_x(y)},$$

и потому достаточно указать такие функции $\varphi(x,y,z)$, $\psi(x,y,z)$, $h(x,y,z,t)$, что

$$(*) \qquad f_x(y) = h(x,y,V(x\ominus 1,y),V(\varphi(x,y,V(x\ominus 1,y)),\psi(x,y,V(x\ominus 1,y)))).$$

Случай 2: $\exp(0,x) > 0$. Тогда $x = 2^{k+1}3^{i_1}5^{i_2}\ldots$, где $k = \exp(0,x) - 1$, $i_s = \exp(s,x)$, и

$$f_x(y) = f_{i_1}(d^{(k+1)}(f_{i_2}(y),\ldots,f_{i_{k+2}}(y)) = f_{i_1}(d^{(k+1)}(\exp(i_2,z),\ldots,\exp(i_{k+2},z)) = f_{i_1}(w(k,x,z)) = \exp(\exp(1,x), V(x\ominus 1, w(\exp(0,x)\ominus 1, x, V(x\ominus 1, y)))),$$

где через z обозначено выражение $V(x\ominus 1, y)$. Эта формула получается из $(*)$, если положить $\varphi(x,y,z) = x$, $\psi(x,y,z) = w(\exp(0,x)\ominus 1, x, z)$, $h(x,y,z,t) = \exp(\exp(1,x),t)$.

Случай 3: $\exp(0,x) = 0$, $\exp(1,x) > 0$, $c_2(y) = 0$. В этом и следующем случаях $x = 3^{i+1}5^j\ldots$, где $i = \exp(1,x) - 1$, $j = \exp(2,x)$. Мы имеем:

$$f_x(y) = f_x(d^{(2)}(c_1(y),0)) = f_i(c_1(y)) = \exp(\exp(1,x)\ominus 1, V(x\ominus 1, c_1(y))),$$

что получается из $(*)$ при $\varphi(x,y,z) = x\ominus 1$, $\psi(x,y,z) = c_1(y)$, $h(x,y,z,t) = \exp(\exp(1,x)\ominus 1, t)$.

Случай 4: $\exp(0,x) = 0$, $\exp(1,x) > 0$, $c_2(y) > 0$. Тогда $f_x(y) =$

$$f_x(d^{(2)}(c_1(y),c_2(y))) = f_j(d^{(2)}(d^{(2)}(c_1(y),c_2(y)\ominus 1), f_x(d^{(2)}(c_1(y),c_2(y)\ominus 1))) = f_j(d^{(2)}(v(y), f_x(v(y)))) = \exp(\exp(2,x), d^{(2)}(v(y), \exp(x, V(x,v(y))))),$$

что совпадает с формулой $(*)$, если положить в ней $\varphi(x,y,z) = x$, $\psi(x,y,z) = v(y)$, $h(x,y,z,t) = \exp(\exp(2,x), d^{(2)}(v(y),\exp(x,t))$.

Случай 5: $\exp(0,x) = \exp(1,x) = 0$. В этом случае функция $f_x(y)$ совпадает с одной из элементарных функций от y:

$$\begin{aligned}
&f_1(y) = s(y),\\
&f_x(y) = \mathrm{id}(y), \quad \text{если } \exp(2,x) = 1,\\
&f_x(y) = \mathrm{c}_1(y), \quad \text{если } \exp(2,x) = 2,\\
&f_x(y) = \mathrm{c}_2(y), \quad \text{если } \exp(2,x) = 3,\\
&f_x(y) = o(y), \quad \text{если } \exp(2,x) \neq 1,2,3,\ x \neq 1.
\end{aligned}$$

Она на самом деле не зависит от z и t, и потому в качестве $\varphi(x,y,z)$, $\psi(x,y,z)$ можно взять любые функции (например, $\varphi(x,y,z) = \psi(x,y,z) = 0$), а в качестве $h(x,y,z,t)$ — соответственно функции $s(y)$, $\mathrm{id}(y)$, $c_1(y)$, $c_2(y)$, $o(y)$.

9.3. Пример рекурсивной, но не примитивно рекурсивной функции. Рассмотрим функцию $g(x) = U(x,x) + 1$. Поскольку функция $U(x,y)$ рекурсивна, функция $U(x,x)$, получающаяся из нее подстановкой, тоже рекурсивна, а вместе с ней рекурсивна и функция $g(x) = U(x,x)+1$. Но эта функция не примитивно рекурсивна: если бы это было не так, то существовал бы номер n, такой что $g(x) = f_n(x) = U(n,x)$, и мы имели бы $U(n,n) = g(n) = U(n,n)+1$.

10. Рекурсивные множества

10.1. Определение рекурсивного множества. Пусть A — подмножество $\mathbb{N}_0$; напомним, что характеристической функцией множества A называется функция, определенная следующим образом:

$$\chi_A(x) = \begin{cases} 1, & \text{если } x \in A, \\ 0, & \text{если } x \notin A. \end{cases}$$

Подмножество A множества $\mathbb{N}_0$ называется рекурсивным (примитивно рекурсивным) множеством, если функция $\chi_A(x)$ рекурсивна (примитивно рекурсивна).

Примитивно рекурсивные множества не играют сколько-нибудь важной роли. Напротив, рекурсивные множества имеют принципиальное значение: поскольку все значения рекурсивных функций и только рекурсивных функций могут быть вычислены, рекурсивные множества являются в точности теми множествами, для которых вопрос о принадлежности элемента множеству может быть в принципе решен.

10.2. Рекурсивные и рекурсивно перечислимые множества.

Теорема. *Всякое примитивно рекурсивное множество рекурсивно. Всякое рекурсивное множество рекурсивно перечислимо.*

Доказательство. Если множество A примитивно рекурсивно, то его характеристическая функция примитивно рекурсивна, а потому и рекурсивна; значит, множество A рекурсивно. Пусть теперь множество A рекурсивно. Тогда A можно охарактеризовать как множество точек $a \in \mathbb{N}_0$, таких что $\chi(a) = 1$; но это множество совпадает с множеством тех $a \in \mathbb{N}_0$, для которых уравнение $|a - 1|(x + 1) = 0$ имеет решение. Следовательно, множество A рекурсивно перечислимо.

Оказывается, все три класса множеств, участвующие в этой теореме, различны. Довольно легко построить рекурсивное, но не примитивно рекурсивное множество. Для этого опять воспользуемся универсальной функцией $U(x, y)$. Функция $h(x) = \overline{\operatorname{sgn}}(U(x, x))$ рекурсивна и принимает только два значения — 0 и 1; следовательно, она является характеристической функцией некоторого множества A (а именно, множества тех чисел $a \in \mathbb{N}_0$, для которых $h(a) = 1$). Это множество A рекурсивно. В то же время, если бы функция $h(x)$ была примитивно рекурсивна, то существовал бы номер $i \in \mathbb{N}_0$, такой что $h(x) = U(i, x)$, и тогда мы бы имели $\overline{\operatorname{sgn}}(U(i, i)) = h(i) = U(i, i)$, что невозможно. Следовательно, функция $\chi_A(x) = h(x)$ не примитивно рекурсивна, и потому множество A не примитивно рекурсивно.

Пример рекурсивно перечислимого, но не рекурсивного множества, несколько сложнее и будет предъявлен в конце этого параграфа.

10.3. Свойства рекурсивных множеств.

Теорема. *Объединение и пересечение конечного числа рекурсивных (примитивно рекурсивных) множеств рекурсивно (примитивно рекурсивно). Дополнение рекурсивного (примитивно рекурсивного) множества рекурсивно (примитивно рекурсивно).*

Доказательство. Пусть множества $A_1, \ldots, A_n$ рекурсивны (примитивно рекурсивны). Тогда функции $\chi_{A_1}(x), \ldots, \chi_{A_n}(x)$ рекурсивны (примитивно рекурсивны). Но ясно, что характеристическими функциями объединения и пересечения множеств $A_1, \ldots, A_n$ и дополнения множества A_1 являются функции $\operatorname{sgn}(\sum_{i=1}^{n} \chi_{A_i}(x))$, $\prod_{i=1}^{n} \chi_{A_i}(x)$, $\overline{\operatorname{sgn}}(\chi_{A_1}(x))$, и эти функции тоже рекурсивны (примитивно рекурсивны). А это и означает, что объединение и пересечение множеств $A_1, \ldots, A_n$ и дополнение множества A_1 рекурсивны (примитивно рекурсивны).

Заметим, что дополнение рекурсивно перечислимого множества не обязано быть рекурсивно перечислимым. Действительно, пусть множество A и его дополнение B оба рекурсивно перечислимы. Тогда существуют примитивно рекурсивные функции $f(x)$, $g(x)$, множествами значений которых являются соответственно множества A, B. Поскольку любое число $a \in \mathbb{N}_0$ принадлежит в точности одному из множеств A, B, в точности одно из уравнений $|f(x) - a| = 0$, $|g(x) - a| = 0$ разрешимо, а значит, уравнение $|f(x) - a||g(x) - a| = 0$ разрешимо относительно x всегда, и потому определена функция $h(y) = \mu_x(|f(x) - y||g(x) - y|)$, и эта функция рекурсивна. Ясно, что характеристической функцией множества A будет рекурсивная функция $\overline{\operatorname{sgn}}|f(h(y)) - y|$, а это означает, что множество A рекурсивно. Но мы упомянули выше, что бывают рекурсивно перечислимые, но не рекурсивные множества; приведенное рассуждение показывает, что дополнение таких множеств не может быть рекурсивно перечислимым.

10.4. Замечание о рекурсивно перечислимых множествах.

Теорема. *Пусть M – непустое подмножество $\mathbb{N}_0^n$; следующие условия равносильны:*

(1) *M рекурсивно перечислимо;*

(2) *для некоторого натурального числа m существуют такие рекурсивные функции $f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m)$, что M состоит из всех точек вида $(f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m))$, где $t_1, \ldots, t_m$ независимо пробегают $\mathbb{N}_0$;*

(3) *существуют рекурсивные функции $f_1(t), \ldots, f_n(t)$, такие что M состоит из всех точек $(f_1(t), \ldots, f_n(t))$, $t \in \mathbb{N}_0$;*

(4) *существует рекурсивная функция $h(a_1, \ldots, a_n, x)$, такая что уравнение $h(a_1, \ldots, a_n, x) = 0$ (относительно неизвестной x) имеет решение тогда и только тогда, когда $(a_1, \ldots, a_n) \in M$;*

(5) *для некоторого натурального числа m существует такая рекурсивная функция $h(a_1, \ldots, a_n, x_1, \ldots, x_m)$ от $n + m$ переменных, что уравнение*

$$h(a_1, \ldots, a_n, x_1, \ldots, x_n) = 0$$

(относительно неизвестных $x_1, \ldots, x_n$) имеет решение тогда и только тогда, когда $(a_1, \ldots, a_n) \in M$.

Замечание. Это утверждение отличается от теоремы из §7.2 только тем, что здесь вместо примитивно рекурсивных функций фигурируют функции из более широкого класса — рекурсивные функции; оно показывает, что такая

модификация определения не приводит к появлению более широкого класса множеств, чем класс рекурсивно перечислимых множеств.

Доказательство. Повторяя доказательство теоремы 5.1, мы получим равносильность условий (2)-(5); То, что из (1) следует (3), тривиально: по теореме из §7.2 для рекурсивно перечислимого множества существуют даже примитивно рекурсивные функции $f_1(t), \ldots, f_n(t)$, такие что M состоит из всех точек $(f_1(t), \ldots, f_n(t))$, $t \in \mathbb{N}_0$.

Заметим, что если $f(x)$ — рекурсивная функция и $g(t)$, $h(t)$ — такие примитивно рекурсивные функции, что график функции $f(x)$ состоит из всех точек вида $(g(t), h(t))$, то множество значений функции $f(x)$ совпадает с множеством значений примитивно рекурсивной функции $h(t)$ и потому является рекурсивно перечислимым подмножеством множества $\mathbb{N}_0$. Пусть теперь $f_1(t), \ldots, f_n(t)$ — такие рекурсивные функции, что множество M состоит из всех точек $(f_1(t), \ldots, f_n(t))$, $t \in \mathbb{N}_0$. Тогда множество

$$M_0 = \{d^{(n)}(a_1, \ldots, a_n) \,|\, (a_1, \ldots, a_n) \in M\} \subseteq \mathbb{N}_0$$

является множеством значений рекурсивной функции $d^{(n)}(f_1(t), \ldots, f_n(t))$ и потому, как мы только что заметили, является рекурсивно перечислимым подмножеством $\mathbb{N}_0$. Но это в точности означает, что множество $M \subseteq \mathbb{N}_0^n$ рекурсивно перечислимо. Таким образом, из (3) следует (1).

10.5. Существование рекурсивно перечислимого, но не рекурсивного множества.

Теорема. *Пусть $U(x, y)$ — рекурсивная функция, универсальная для класса примитивно рекурсивных функций, и пусть M — множество всех $x \in \mathbb{N}_0$, таких что уравнение $|U(c_1(x), t) - x| + |U(c_2(x), t)| = 0$ разрешимо относительно t. Множество M рекурсивно перечислимо, но не рекурсивно.*

Доказательство. Функция $|U(c_1(x), t) - x| + |U(c_2(x), t)| = 0$ рекурсивна относительно x и t; поэтому по теореме из предыдущего пункта множество M рекурсивно перечислимо. Покажем, что это множество не рекурсивно.

Предположим, что это не так. Тогда характеристическая функция $\chi_M(x)$ рекурсивна. Пусть $f(t)$, $g(t)$ — такие примитивно рекурсивные функции, что график функции $\chi_M(x)$ состоит из всех точек вида $(f(t), g(t))$; тогда $\chi_M(f(t)) = g(t)$ для любого $t \in \mathbb{N}_0$, и, поскольку функция $\chi_M(x)$ определена на всем множестве $\mathbb{N}_0$, для всякого числа $a \in \mathbb{N}_0$ найдется число $t_0 \in \mathbb{N}_0$, такое что $f(t_0) = a$.

Функции $f(t)$, $g(t)$ примитивно рекурсивны; поскольку функция $U(x, y)$ универсальна для класса примитивно рекурсивных функций, существует такие числа $a, b \in \mathbb{N}_0$, что $f(t) = U(a, t)$, $g(t) = U(b, t)$ для любого $t \in \mathbb{N}_0$. Пусть $n = d^{(2)}(a, b)$.

Если $n \in M$, то для всякого $t \in \mathbb{N}_0$, такого что $U(c_1(n), t) = U(a, t) = f(t) = n$ должно быть $U(c_2(n), t) = U(b, t) = g(t) = \chi_M(f(t)) = \chi_M(n) = 1$, и потому числа $|U(c_1(n), t) - n|$, $|U(c_2(n), t)|$ не могут одновременно обращаться в 0, т.е. уравнение $|U(c_1(n), t) - n| + |U(c_2(n), t)| = 0$ не имеет решения. Это значит, по определению множества M, что $n \notin M$.

Обратно, пусть $n \notin M$; пусть число $t_0 \in \mathbb{N}_0$ таково, что $f(t_0) = n$. Тогда

$$|U(c_1(n), t_0) - n| + |U(c_2(t_0))| = |U(a, t_0) - n| + |U(b, t_0)| = |f(t_0) - n| + |g(t_0)| = 0,$$

потому что $g(t_0) = \chi_M(f(t_0)) = \chi_M(n) = 0$. Следовательно, уравнение

$$|U(c_1(n), t) - n| + |U(c_2(n), t)| = 0$$

имеет решение t_0, а это означает, что $n \in M$.

В обоих случаях мы пришли к противоречию, которое показывает, что предположение о рекурсивности множества M было ошибочно.

11. Теорема Гёделя

Одним из наиболее знаменитых результатов математической логики является теорема Гёделя о неполноте системы Z_1.

Если система Z_1 непротиворечива, то существует такое суждение в теории Z_1, что ни это суждение, ни его отрицание не могут быть доказаны в Z_1.

В этом пункте мы дадим набросок доказательства этой теоремы, сформулировав основные идеи и отбросив их довольно скучное техническое осуществление.

Напомним, что все суждения являются словами в некотором конечном алфавите $a_0, a_1, \ldots, a_{n-1}$; будем при этом полагать, что a_0 — это правая скобка ")". Слову $a_{i_1} a_{i_2} \ldots a_{i_r}$ сопоставим натуральное число $i_r + i_{r-1} n + \cdots + i_2 n^{r-2} + i_1 n^{r-1}$. Мы получим биективное соответствие между положительными натуральными числами и теми словами, которые не начинаются с символа ")". Поскольку ни одно суждение не начинается с этого символа, все суждения получают некоторые номера, причем номер однозначно определяет суждение; этот номер называется гёделевым номером суждения. Отметим, что не всем номерам отвечают именно суждения (многим из них отвечают просто бессмысленные наборы букв), но для нас это не существенно.

Все доказательства в теории Z_1 тоже могут быть пронумерованы (аналогично тому, как выше мы пронумеровали все примитивно рекурсивные функции). При этом в результате n-го доказательства получается суждение, гёделев номер которого обозначим через $h(n)$. Нетрудно провести нумерацию доказательств так, чтобы получившаяся функция $h(n)$ была рекурсивна.

Пусть M — рекурсивно перечислимое, но не рекурсивное множество из предыдущего пункта. Еще один факт, доказательство которого мы опускаем: утверждение $n \in M$ и его отрицание $n \notin M$ могут быть выражены как суждения B_n, $\neg B_n$ в системе Z_1, причем гёделевы номера этих суждений $g(n)$, $g'(n)$ являются рекурсивными функциями от n.

Теорема. *Существует $n \in \mathbb{N}_0$, для которого ни суждение B_n, ни его отрицание не могут быть доказаны в Z_1.*

Доказательство. Если существует доказательство суждения B_n , то существует $t \in \mathbb{N}_0$, такое что $g(n) = h(t)$. Точно так же, если можно доказать суждение $\neg B_n$, то существует $t \in \mathbb{N}_0$, такое что $g'(n) = h(t)$. Предположим,

что для всех n можно доказать либо суждение B_n, либо суждение B'_n (оба суждения не могут быть одновременно доказуемы, так как тогда существовало бы доказательство тождественно ложного суждения $B_n\&\neg B_n$, т.е. система Z_1 была бы противоречива). Тогда уравнение $|g(n) - h(t)| \cdot |g'(n) - h(t)| = 0$ разрешимо для любого n; обозначим через $w(n)$ наименьшее решение этого уравнения:

$$w(n) = \mu_t(|g(n) - h(t)| \cdot |g'(n) - h(t)|).$$

Функция $w(n)$ рекурсивна; вместе с ней рекурсивна и функция

$$v(n) = \operatorname{sgn}(|g'(n) - h(w(n))|).$$

Лемма. *Функция $v(n)$ является характеристической функцией множества M.*

Доказательство. Если $n \in M$, то утверждение $n \notin M$ не может быть доказано. Тогда $|g'(n) - h(t)| \neq 0$ для всех $t \in \mathbb{N}_0$, и $v(n) = \operatorname{sgn}(|g'(n) - h(w(n))|) \neq 0$; но функция $v(x)$ принимает только значения 0, 1, и потому $v(n) = 1$.

Если $n \notin M$, то утверждение $n \in M$ не может быть доказано; поэтому $|g(n) - h(t)| \neq 0$ для всех $t \in \mathbb{N}_0$. Следовательно, число $w(n) = \mu_t(|g(n) - h(t)| \cdot |g'(n) - h(t)|)$ не является корнем уравнения $|g(n) - h(t)| = 0$ и потому $|g'(n) - h(w(n))| = 0$, т.е. $v(n) = \operatorname{sgn}(|g'(n) - h(w(n))|) = 0$.

Таким образом, мы получили, что рекурсивная функция $v(n)$ является характеристической функцией множества M, т.е. множество M рекурсивно. Это противоречие доказывает, что предположение о том, что для всякого n существует доказательство одного из суждений B_n, $\neg B_n$, неверно.