1. Логика и арифметика

1.1 Простые утверждения

1) Любую булеву функцию можно выразить формулой в КНФ или в ДНФ.

Теорема 10. *Для любой булевой функции существуют выражающие её КНФ и ДНФ.*

Доказательство. Доказательство будет конструктивным: мы укажем способ построения этих формул. Сначала построим ДНФ. Каждому набору значений, на котором функция истинна, мы сопоставим конъюнкт. Если переменная в этом наборе истинна, то в конъюнкт будет включена она сама, а если ложна, то будет включено её отрицание. Итоговая ДНФ будет дизъюнкцией всех таких конъюнктов. Формально можно записать так:

$$\varphi = \bigvee_{f(a_1,\ldots,a_n)=1} \bigwedge_{i=1}^{n} p_i^{a_i},$$

где p^a обозначает p, если $a = 1$, и $\neg p$, если $a = 0$. Эта формула действительно выражает функцию f. Конъюнкт $\bigwedge_{i=1}^{n} p_i^{a_i}$ истинен на наборе $(a_1, \ldots, a_n)$ и ложен на всех остальных. (Если a тоже понимать как переменную, то p^a это эквиваленция). Дизъюнкция же таких конъюнктов будет истинна только на тех наборах, которым соответствует один из конъюнктов, т.е. только на тех наборах, на которых функция равна 1. Значит, ДНФ φ представляет функцию f. Осталось заметить, что вся проведённая конструкция работает только в том случае, когда f не является тождественно ложной, иначе получится пустая внешняя дизъюнкция. Однако в этом случае можно представить f как $p \wedge \neg p$.

Теперь построим КНФ. Она будет сделана по похожей схеме. Теперь каждому набору значений, на котором функция ложна, мы сопоставим дизъюнкт. Если переменная в этом наборе истинна, то в дизъюнкт будет включено её отрицание, а если ложна, то она сама. Итоговая КНФ будет конъюнкцией всех таких дизъюнктов. Формально:

$$\psi = \bigwedge_{f(a_1,\ldots,a_n)=0} \bigvee_{i=1}^{n} p_i^{1-a_i}.$$

Можно заметить, что дизъюнкт $\bigvee_{i=1}^{n} p_i^{1-a_i}$ ложен на наборе $(a_1, \ldots, a_n)$ и истинен на всех остальных. Конъюнкция таких дизъюнктов будет ложна только на тех наборах, которым соответствует один из дизъюнктов, т.е. только на тех наборах, на которых функция равна 0. Значит, КНФ ψ представляет функцию f. Осталось заметить, что вся проведённая конструкция работает только в том случае, когда f не является тождественно истинной, иначе получится пустая внешняя конъюнкция. Однако в этом случае можно представить f как $p \vee \neg p$. □

2) Замкнутость классов Поста относительно композиции.

Определение: суперпозиция функций из множества F:

- Суперпозициz порядка 0 – все проекторы, т.е. функции вида $pr_i(p_1, \ldots, p_n) = p_i$
- Суперпозиция порядка $m+1$ – функция вида $h(p_1, \ldots, p_n) = f(g_1(p_1, \ldots, p_n), \ldots, g_k(p_1, \ldots, p_n))$, где $f \in F$, f зависит от k аргументов, $g_1, \ldots, g_k$ - суперпозиции порядка $\leqslant m$, хотя бы одно из них в тоности m.

Определение: Замыкание класса F – множество всех суперпозиций всех порядков функции из F (Обозначение: $[F]$) **Определение:** Класс замкнут, если $[F] = F$

Докажем замкнутость классов Поста для $f \in T_1, T_0, S, M, L$:

- $[T_1] = T_1: \quad h(1,\dots,1) = f(g_1(1,\dots,1),\dots,g_k(1,\dots,1)) = f(1,\dots,1) = 1$
- $[T_0] = T_0: \quad$ аналогично T_1
- $[M] = M: \left\{ \begin{array}{c} x_1 \leqslant y_1 \\ \dots \\ x_n \leqslant y_n \end{array} \right\} \Rightarrow \left\{ \begin{array}{c} g_1(x_1,\dots,x_n) \leqslant g_1(y_1,\dots,y_n) \\ \dots \\ g_k(x_1,\dots,x_n) \leqslant g_k(y_1,\dots,y_n) \end{array} \right\} \Rightarrow$
$f(g_1(x_1,\dots,x_n),\dots,g_k(x_1,\dots,x_n)) \leqslant f(g_1(y_1,\dots,y_n),\dots,g_k(y_1,\dots,y_n))$
- $[S] = S: \quad f(g_1(\neg p_1,\dots,\neg p_n),\dots,g_k(\neg p_1,\dots,\neg p_n)) = f(\neg g_1(p_1,\dots,p_n),\dots,\neg g_k(p_1,\dots,p_n)) = \neg f(g_1(p_1,\dots,p_n),\dots,g_k(p_1,\dots,p_n))$
- $[L] = L: \quad f(g_1(p_1,\dots,p_n),\dots,g_k(p_1,\dots,p_n)) = p_{i_1} \oplus \dots \oplus p_{i_m} \oplus \alpha \oplus \dots \dots \oplus p_{j_1} \oplus \dots \oplus p_{j_q} \oplus \beta \oplus \gamma$, где $\alpha, \beta\gamma \in \{0,1\}$. После сокращения дублей получится выражение такого же вида.

3) Вывод формулы вида $A \to A$ в исчислении высказываний.

Доказательство приведено в определениях пункт 6).

4) Теорема о корректности исчисления высказываний.

Корректность ИВ: Если $\vdash \phi$, то ϕ – тавтология

▲ 1) Любая аксиома есть тавтология. Проверяется непосредственно по таблице истинности.
2) Правило MP тоже корректно: если A и $A \to B$ всегда истинны, то B тоже всегда истинно. ■

5) Сведение задачи о выполнимости произвольной формулы к задаче о выполнимости 3-КНФ.

Утверждение: Пусть ϕ – КНФ. Тогда выполнимость ϕ эквивалентна выполнимости ϕ', образованной следующим образом: каждый дизъюнкт $(l_1 \vee l_2 \vee \dots \vee l_k)$ заменяется на такую КНФ: $(l_1 \vee x_1) \wedge (\neg x_1 \vee l_2 \vee x_2) \wedge \dots \wedge (\neg x_{k-2} \vee l_{k-1} \vee x_{k-1}) \wedge (\neg x_k \vee l_k)$, где переменные $x_1,\dots,x_k$ свои для каждого дизъюнкта.

▲ Пусть ϕ выполнима. Тогда при выполняющем наборе один из литералов $l_1,\dots,l_k$ истинен, например, l_j. Пусть тогда все x_i с $i < j$ равны 1, а все x_i с $i \geqslant j$ равны 0. Это сделает истинным все скобки в новой КНФ.

Пусть, напротив, выполнима ϕ'. Каждая из переменных x_i может сделать истинной ровно одну скобку. Значит, все они могут сделать истинными максимум $k-1$ скобку. Оставшаяся должна стать истинной за счёт l_j. А значит, и исходный дизъюнкт выполнен. ■

6) Представление задачи о раскраске графа и задачи о расстановке ферзей на шахматной доске как задачи о выполнимости КНФ.

- *Задача о 3-раскраске вершин графа.* Пусть задан некоторый неориентированный граф. Ставится вопрос: можно ли его вершины раскрасить в 3 цвета, так чтобы вершины одного цвета не были соединены ребром. КНФ строится так: для каждой вершины i заводится две переменных p_i и q_i. Будем считать, что пара значений $(0,1)$ кодирует первый цвет, пара $(1,0)$ второй цвет, а пара $(1,1)$ третий цвет. Чтобы исключить вариант $(0,0)$, добавим условия $(p_i \vee q_i)$. Далее, для каждого ребра (i, j) пара (p_i, q_i) должна отличаться от пары (p_j, q_j). Это выражается такой КНФ:

$$(p_i \vee p_j \vee q_i \vee q_j) \wedge (p_i \vee p_j \vee \neg q_i \vee \neg q_j) \wedge (\neg p_i \vee \neg p_j \vee q_i \vee q_j) \wedge (\neg p_i \vee \neg p_j \vee \neg q_i \vee \neg q_j)$$

Выполнимость конъюнкции всех таких формул эквивалентна раскрашиваемости исходного графа.

- *Задача о расстановке ферзей на шахматной доске.* Известна такая задача: можно ли расставить 8 ферзей на шахматной доске, так чтобы они не били друг друга. Мы заведём переменные p_{ij}, истинность которых означает, что в клетке с координатами (i, j) стоит ферзь.
  – По условию в одной строке не может быть двух ферзей, значит, в каждой должен быть ровно один. Достаточно написать дизъюнкты вида $(p_{i1} \vee p_{i2} \vee \ldots \vee p_{i8})$.
  – Далее, запишем условия, что в каждом столбце стоит не более одного ферзя. А именно, для каждого набора $(i, j \neq i, k)$ возьмём дизъюнкт $(\neg p_{ik} \vee \neg p_{jk})$. Аналогичные условия для строк можно записать отдельно, но они будут следовать из уже написанных.
  – Также нужно написать условия для диагоналей: $(\neg p_{ij} \vee \neg p_{i+k,j+k})$ и $(\neg p_{ij} \vee \neg p_{i+k,j-k})$ при всех i, всех $j < 8$ и всех $k > 0$ (записываются только те условия, где все индексы попадают в интервал от 1 до 8).
  Любой выполняющий набор для такой системы задаёт расстановку ферзей. Можно рассматривать разные варианты задачи: другой размер доски, фиксированное положение некоторых ферзей (тогда добавятся дизъюнкты p_{ij}) или запрещённые клетки (тогда добавятся дизъюнкты $\neq p_{ij}$).

В обоих случаях мы получили не 3-КНФ: в некоторых дизъюнктах больше трёх литералов.

7) Теорема о корректности метода резолюций: из выполнимой КНФ нельзя вывести $\perp$.

Теорема: Метод резолюций всегда заканчивает свою работу, причём для невыполнимых КНФ выводится $\perp$ (полнота), а для выполнимых не выводится (корректность). Таким образом, метод резолюций позволяет проверить выполнимость формулы: достаточно добавить все возможные резольвенты и проверить, встретился ли $\perp$.

▲ Всего существует конечное число дизъюнктов, так что в какой-то момент новые перестанут появляться, поэтому метод всегда заканчивает свою работу. Как обычно, корректность доказывается легко. Действительно, если исходная КНФ была выполнима, то она останется выполнимой после добавления любого числа резольвент. Но КНФ с $\perp$ выполнимой быть не может. Значит, для выполнимой КНФ $\perp$ не появится. ■

Пример: Невыполнимая КНФ $(x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee x_2) \wedge (\neg x_2 \vee x_3) \wedge \neg x_3$ опровергается так:
1) $(x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee x_2) \Rightarrow (x_2 \vee x_3)$
2) $(x_2 \vee x_3) \wedge (\neg x_2 \vee x_3) \Rightarrow x_3$
3) $x_3 \vee \neg x_3 \Rightarrow \perp$

8) Значение терма (формулы) первого порядка зависит только от значений его (её) параметров.

Теорема: Истинность формулы (значение терма) зависит только от её (его) параметров. Иными словами, если оценки π и ρ таковы, что $\forall x \in \mathrm{Param}(\phi)$ (или $x \in \mathrm{Param}(t)$) выполнено $\pi(x) = \rho(x)$, то $[\phi](\pi) = [\phi](\rho)$ (или $[t](\pi) = [t](\rho)$).
▲ Будем доказывать утверждение индукцией по построению терма, а затем формулы:

- Если $t = x$, то $[t](\pi) = \pi(x) = \rho(x) = [t](\rho)$

- Если $t = c$, то $[t](\pi) = [c] = [t](\rho)$

- Если $t = f(t_1, \ldots, t_k)$, то в силу $\mathrm{Param}(t_i) \subset \mathrm{Param}(t)$ по предположению индукции имеем $[t_i](\pi) = [t_i](\rho)$. Поэтому $[t](\pi) = [f]([t_1](\pi), \ldots, [t_k](\pi)) = [f]([t_1](\rho), \ldots, [t_k](\rho)) = [t](\rho)$;

- Если $\phi = P(t_1, \ldots, t_k)$, то рассуждение аналогично предыдущему;

- Если $\phi = \neg\psi$, то $[\phi](\pi) = \neg[\psi](\pi) = \neg[\psi](\rho) = [\phi](\rho)$. Здесь предположение индукции использовано во втором равенстве;

- Если $\phi = (\psi \wedge \gamma)$, то $[\phi](\pi) = [\psi](\pi) \wedge [\gamma](\pi) = [\psi](\rho) \wedge [\gamma](\rho) = [\phi](\rho)$. Здесь во втором равенстве использовано предположение индукции и вложения $\mathrm{Param}(\psi) \subset \mathrm{Param}(\phi)$ и $\mathrm{Param}(\gamma) \subset \mathrm{Param}(\phi)$. Случай $\phi = (\psi \vee \gamma)$ и $\phi = (\psi \to \gamma)$ разбираются аналогично;

- Если $\phi = \exists x\psi$, то ключевое соображение состоит в следующем: если $\pi(y) = \rho(y)$ для всех $y \in \mathrm{Param}(\psi) \setminus \{x\}$, то $\pi_{x \to m}(y) = \rho_{x \to m}(y)$ уже для всех $y \in \mathrm{Param}(\psi)$, в том числе для $y = x$. Действительно, $\pi_{x \to m}(y) = \rho_{x \to m}(y) = m$, а для $y \neq x$ равенство есть по предположению. Поэтому $[\phi](\pi) = \vee_{m \in M}[\psi](\pi_{x \to m}) = \vee_{m \in M}[\psi](\rho_{x \to m}) = [\phi](\rho)$. Аналогичное рассуждение работает и для $\phi = \forall x\psi$. ■

9) Выразимость свойств «равняться нулю», «равняться единице», «делиться нацело», «быть простым числом», «равняться наибольшему общему делителю», «равняться наименьшему общему кратному» в интерпретации $\langle \mathbb{N}, \cdot\, , = \rangle$.

Рассмотрим интерпретацию $\langle \mathbb{N}, \cdot\, , = \rangle$. Будем выражать в ней различные предикаты:

- $x = 0 \;\Leftrightarrow\; \forall y\; x \cdot y = x$

- $x = 1 \;\Leftrightarrow\; \forall y\; x \cdot y = y$

- $x \,\vdots\, y \;\Leftrightarrow\; \exists z\; x = y \cdot z$

- $Prime(p) \;\Leftrightarrow\; (p \neq 1 \;\wedge\; \forall q(p \,\vdots\, q \to (q = 1 \;\vee\; q = p)))$

- $d = \text{НОД}(x, y) \;\Leftrightarrow\; (x \,\vdots\, d \;\wedge\; y \,\vdots\, d \;\wedge\; \forall k((x \,\vdots\, k \;\wedge\; y \,\vdots\, k) \to d \,\vdots\, k))$

- $d = \text{НОК}(x, y) \;\Leftrightarrow\; (d \,\vdots\, x \;\wedge\; d \,\vdots\, y \;\wedge\; \forall k((k \,\vdots\, x \;\wedge\; k \,\vdots\, y) \to k \,\vdots\, d))$

10) Любую формулу первого порядка можно привести к предваренной нормальной форме.

Определение: Формула находится в предварённой нормальной форме, если вначале идут кванторы по некоторым переменным в некотором порядке, а затем — бескванторная формула.

Теорема: Для любой формулы существует эквивалентная ей формула в предваренной нормальной форме.

▲ Алгоритм будет таким: сначала переименовать связанные переменные, так чтобы под всеми кванторами были разные переменные, притом не совпадающие с именами свободных переменных. Затем вынести все кванторы наружу, меняя их при выносе из отрицания или посылки импликации по правилам 4-7 из списка ниже. ■

4) Обобщённые законы де Моргана

$$\neg\forall x\, \phi \leftrightarrow \exists x\, \neg\phi$$

$$\neg\exists x\, \phi \leftrightarrow \forall x\, \neg\phi$$

"Квантор выносится наружу"

5) Взаимодействие кванторов и конъюнкции

$$(\forall x\, \phi \ \wedge\ \forall x\, \psi) \leftrightarrow \forall x(\phi \wedge \psi)$$

$$\exists x(\phi \wedge \psi) \rightarrow (\exists x\, \phi\ \wedge \exists x\, \psi)$$

Обратное неверно. Например, существуют прямоугольные треугольники, существуют равносторонние треугольники, но не существует прямоугольного равностороннего треугольника

$(\exists x\, \phi \wedge \psi) \leftrightarrow \exists x\ (\phi \wedge \psi)$, если ψ не зависит от x

6) Взаимодействие кванторов и дизъюнкции

$$(\exists x\, \phi \vee \exists x\, \psi) \leftrightarrow \exists x(\phi \vee \psi)$$

$$(\forall x\, \phi \vee \forall x\, \psi) \rightarrow \forall x\ (\phi \vee \psi)$$

Обратное неверно : например, любое целое число чётное или нечётное, но неверно, что все числа чётные или все числа нечётные

$(\forall x\, \phi \vee \psi) \leftrightarrow \forall x\ (\phi \vee \psi)$, если ψ не зависит от x

7) Взаимодействие кванторов и импликации

$$(\forall x\, \phi \rightarrow \exists x\, \psi) \leftrightarrow \exists x(\phi \rightarrow \psi)$$

$$(\exists x\, \phi \rightarrow \forall x\, \psi) \rightarrow \forall x(\phi \rightarrow \psi)$$

$(\exists x\, \phi \rightarrow \psi) \leftrightarrow \forall x(\phi \rightarrow \psi)$, если ψ не зависит от x

$(\phi \rightarrow \forall x\, \psi) \leftrightarrow \forall x(\phi \rightarrow \psi)$, если ϕ не зависит от x

Пример: $\exists x A(x) \wedge \exists x B(x) \ \Leftrightarrow\ \exists x A(x) \wedge \exists y B(y) \ \Leftrightarrow\ \exists x(A(x) \wedge \exists y B(y)) \ \Leftrightarrow\ \exists x \exists y(A(x) \wedge B(x))$

11) Вывод правила обобщения в исчислении предикатов.

Правило обобщения:

$$\frac{\phi}{\forall x\ \phi}$$

▲ 1) ϕ – считаем, что уже вывели
2) ψ – некоторая аксиома, не зависящая от x
3) $\phi \to (\psi \to \phi)$ – аксиома 1
4) $\psi \to \phi$ – MP из 1 и 3
5) $\psi \to \forall x\phi$ – 2-ое правило Бернайса
6) $\forall x\phi$ – MP из 2 и 5 ■

12) Вывод формулы вида xy $\to$ yx в исчислении предикатов.

Доказательство приведено в определениях пункт 12).

13) Любое совместное множество формул первого порядка непротиворечиво.

▲ От противного: пусть Γ – противоречиво. Если $\Gamma \vdash \phi$ и все формулы из Γ верны на некотором наборе (def: совместности), то ϕ верно на том же наборе. При этом $\Gamma \vdash \phi$ и $\Gamma \vdash \neg\phi$, то Γ ϕ и $\neg\phi$ одновременно верны на этом наборе, противоречие $\Leftrightarrow$ Γ – непротиворечиво. ■

14) Из теоремы Гёделя о полноте исчисления предикатов в сильной форме (любая непротиворечивая теория имеет модель) следует теорема в слабой форме (любая общезначимая формула выводима в исчислении предикатов).

Напомним определения:

Определение: Множество Γ замкнутых формул в сигнатуре называется теорией.

Определение: Формула называется замкнутой, если множество ее параметров пусто. Иначе говоря, все переменные замкнутой формулы должны быть связаны кванторами.

Определение: Интерпретация M сигнатуры σ называется моделью теории Γ, если все формулы из Γ истинны в M.

Утверждение: Сильная формулировка о полноте $\Rightarrow$ слабая формулировка

▲ Пусть ϕ – общезначимая формула. Значит, $\forall x \phi$ тоже общезначимая формула (по корректности правила обощения). Значит, $\{\neg \forall x \phi\}$ – теория, не имеющая моделей. По контрапозиции к сильной формулировке получаем, что $\{\neg \forall x \phi\}$ – противоречива. Таким образом, $\{\neg \forall x \phi\} \vdash \psi, \neg \psi$. Тогда можно вывести $\neg\neg\forall x \phi \Rightarrow \vdash \forall x \phi \Rightarrow \vdash \phi$ (по аксиоме 12) ■

15) Выразимость в арифметике свойства «быть степенью двойки».

Пусть задано $\langle \mathbb{N}, 0, S, +, \cdot, = \rangle$

$x \,\vdots\, y \Leftrightarrow \exists z \; x = y \cdot z$

x является степенью 2 $\Leftrightarrow \forall d (x \,\vdots\, d \to (d = 1 \vee d \,\vdots\, 2))$

16) Множество предложений, выводимых в арифметике Пеано, перечислимо.

1. Проверяем – аксиома или нет
2. Перебираем все последовательности формул с данными переменными
   - если не является выводом из прошлых, то делаем "continue"
   - если является, то делаем "cout"