

Московский физико-технический институт
Физтех-школа прикладной математики и информатики

МАТЕМАТИЧЕСКАЯ ЛОГИКА И ТЕОРИЯ АЛГОРИТМОВ
БИЛЕТЫ К ЭКЗАМЕНУ
II СЕМЕСТР

Лектор: *Мусатов Даниил Владимирович*



Автор: *Клуб Теха Лекций, Головки Денис*
Проект на Github

весна 2023

Содержание

Логика и арифметика.	2
1 Определения	2
1.1 Булевы функции, примеры. Двойственность.	2
1.2 Классы булевых функций: сохраняющие 0 и 1, монотонные, самодвойственные, линейные.	2
1.3 Пропозициональные формулы. Тавтологии. Конъюнктивные и дизъюнктивные нормальные формы.	2
1.4 Многочлены Жегалкина.	3
1.5 Аксиомы исчисления высказываний, <i>modus ponens</i> .	3
1.6 Логические выводы и выводимые формулы.	3
1.7 Резолюции.	4
1.8 Языки первого порядка: индивидуальные переменные, логические связки, кванторы, функциональные и предикатные символы, термы, атомарные формулы, формулы общего вида.	4
1.9 Интерпретация языка первого порядка. Оценка переменных. Общезначимые формулы.	5
1.10 Свободные и связанные вхождения переменных. Параметры формулы.	6
1.11 Выразимость предиката или функции в данной интерпретации.	6
1.12 Аксиомы исчисления предикатов, правила Бернаиса, правило обобщения.	7
1.13 Аксиомы равенства.	8
1.14 Теории, модели, нормальные модели.	8
1.15 Аксиомы арифметики Пеано.	8
1.16 Совместность, непротиворечивость, полнота теории.	9
2 Простые утверждения	10
2.1 Любую булеву функцию можно выразить формулой в КНФ или в ДНФ.	10
2.2 Замкнутость классов Поста относительно композиции.	10
2.3 Вывод формулы вида $A \rightarrow A$ в исчислении высказываний.	11
2.4 Теорема о корректности исчисления высказываний.	11
2.5 Сведение задачи о выполнимости произвольной формулы к задаче о выполнимости 3-КНФ.	11
2.6 Представление задачи о раскраске графа и задачи о расстановке ферзей на шахматной доске как задачи о выполнимости КНФ.	11
2.7 Теорема о корректности метода резолюций: из выполнимой КНФ нельзя вывести \perp .	12
2.8 Значение терма (формулы) первого порядка зависит только от значений его (её) параметров.	12
2.9 Выразимость свойств «равняться нулю», «равняться единице», «делиться нацело», «быть простым числом», «равняться наибольшему общему делителю», «равняться наименьшему общему кратному» в интерпретации $\langle \mathbb{N}, \cdot, = \rangle$.	13

2.10	Любую формулу первого порядка можно привести к предваренной нормальной форме.	13
2.11	Вывод правила обобщения в исчислении предикатов.	14
2.12	Вывод формулы вида $\exists x \forall y \varphi \rightarrow \forall y \exists x \varphi$ в исчислении предикатов.	14
2.13	Любое совместное множество формул первого порядка непротиворечиво.	14
2.14	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).	15
2.15	Выразимость в арифметике свойств «быть степенью двойки», «быть степенью четвёрки».	15
2.16	Множество предложений, выводимых в арифметике Пеано, перечислимо.	15
3	Вопросы из билетов	16
3.1	Теорема об однозначном представлении булевой функции многочленом Жегалкина.	16
3.2	Теорема о дедукции для исчисления высказываний.	16
3.3	Теорема о полноте исчисления высказываний.	17
3.4	Теорема о полноте метода резолюций: из невыполнимой КНФ всегда можно вывести \perp	19
3.5	Теорема о компактности для исчисления высказываний.	20
3.6	Устойчивость выразимых предикатов при автоморфизмах интерпретаций.	20
3.7	Теорема Гёделя о полноте исчисления предикатов: расширение любого непротиворечивого множества до полного и экзистенциально полного.	21
3.8	Теорема Гёделя о полноте исчисления предикатов: построение модели из замкнутых термов у любого непротиворечивого, полного и экзистенциально полного множества.	22
3.9	Представимость конечных последовательностей в арифметике при помощи β -функции Гёделя.	23
3.10	Арифметичность предикатов « n — степень шестёрки» и $n = 2^k$	23
3.11	Множество замкнутых формул, истинных в \mathbb{N} , неперечислимо. Первая теорема Гёделя о неполноте.	24
3.12	Теорема Тарского.	25
	Теория множеств.	26
4	Определения	26
4.1	Множество, основные теоретико-множественные операции, упорядоченная пара, декартово произведение.	26
4.2	Отображения и соответствия. Образ и прообраз. Инъекции, сюръекции, биекции. Композиция отображений. Возведение множества в степень множества.	26
4.3	Равномощность. Счётные и континуальные множества.	27
4.4	Бинарные отношения. Рефлексивность, транзитивность, (анти)симметричность и т. д. Отношения эквивалентности и отношения порядка.	27

4.5	Упорядоченное множество, линейно упорядоченное множество, фундированное множество, вполне упорядоченное множество.	28
4.6	Цепи в упорядоченных множествах. Верхние и нижние грани, максимальные и минимальные, наибольшие и наименьшие элементы.	28
4.7	Гомоморфизмы и изоморфизмы упорядоченных множеств.	28
4.8	Сложение и умножение упорядоченных множеств.	28
4.9	Начальные отрезки вполне упорядоченных множеств.	29
4.10	Предельные элементы вполне упорядоченных множеств.	29
4.11	Порядковые типы $\omega, \omega^k, \omega^\omega, \varepsilon_0$	29
4.12	Аксиома выбора.	29
4.13	Базис Гамеля.	29
5	Простые утверждения	30
5.1	Основные тождества про теоретико-множественные операции, декартово произведение, возведение множества в степень множества.	30
5.2	Равномощность — отношение эквивалентности.	31
5.3	Объединение и декартово произведение счётных множеств счётны.	31
5.4	В любом бесконечном множестве найдётся счётное подмножество.	31
5.5	Несчётность множества точек на отрезке.	31
5.6	Нефундированность прямого лексикографического порядка на конечных словах.	31
5.7	Любой начальный отрезок вполне упорядоченного множества, отличный от всего множества, представляется в виде $[0, a)$	31
5.8	Вполне упорядоченное множество неизоморфно своему начальному отрезку вида $[0, a)$ (вывод из леммы о монотонной функции).	32
5.9	Сумма и произведение фундированных множеств фундированы, вполне упорядоченных — вполне упорядочены.	32
5.10	Свойства сложения и умножения вполне упорядоченных множеств: ассоциативность, некоммутативность, (не)дистрибутивность, (не)монотонность.	32
5.11	Сравнимость любых двух множеств по мощности (вывод из теоремы Цермело и свойств вполне упорядоченных множеств).	33
5.12	Теорема о структуре: любой элемент вполне упорядоченного множества представляется как сумма предельного и конечного.	33
6	Вопросы из билетов	34
6.1	Эквивалентность фундированности, отсутствия бесконечно убывающей последовательности элементов и принципа трансфинитной индукции.	34
6.2	Лемма о монотонной функции из вполне упорядоченного множества в себя.	35
6.3	Теорема о структуре вполне упорядоченного множества: оно представляется как $\omega \cdot L + F$, где L — множество предельных элементов (кроме, возможно, наибольшего), F — конечное множество.	35
6.4	Теорема о трансфинитной рекурсии.	35
6.5	Сравнимость любых двух вполне упорядоченных множеств.	36
6.6	Теорема о вычитании вполне упорядоченных множеств.	37

6.7	Теорема о делении с остатком вполне упорядоченных множеств.	37
6.8	Теорема Цермело.	38
6.9	Лемма Цорна.	38
6.10	Любой частичный порядок можно дополнить до линейного.	38
6.11	Объединение двух бесконечных множеств равномощно одному из них.	39
6.12	Декартов квадрат бесконечного множества равномощен ему.	40
Вычислимость.		42
7	Определения	42
7.1	Машина Тьюринга.	42
7.2	Вычислимая функция.	43
7.3	Разрешимое множество.	43
7.4	Перечислимое множество.	43
7.5	Универсальная машина Тьюринга.	44
7.6	Универсальная вычислимая функция.	44
7.7	Главная универсальная вычислимая функция.	44
7.8	m -сводимость.	44
7.9	Арифметическая иерархия.	44
7.10	λ -термы, α -конверсии, β -редукции, нормальная форма.	45
7.11	Нумералы Чёрча.	46
7.12	Комбинатор неподвижной точки.	46
8	Простые утверждения	47
8.1	Композиция вычислимых функций вычислима.	47
8.2	Существование невычислимых функций, неразрешимых и перечислимых множеств (из соображений мощности).	47
8.3	Разрешимость любого конечного множества.	47
8.4	Перечислимость любого разрешимого множества.	47
8.5	Замкнутость классов разрешимых и перечислимых множеств относительно пересечения, объединения, декартова произведения и конкатенации, класса разрешимых относительно дополнения и разности.	47
8.6	Существование вычислимой в обе стороны биекции между \mathbb{N}^2 и \mathbb{N}	48
8.7	Подмножество разрешимого (перечислимого) множества не обязательно разрешимо (перечислимо), и наоборот.	48
8.8	Свойства m -сводимости: транзитивность, сводимость дополнений, разрешимость множества, m -сводимого к разрешимому, перечислимость множества, m -сводимого к перечислимому, сводимость разрешимого множества к любому нетривиальному.	48
8.9	Вложенность классов в арифметической иерархии.	49
8.10	Замкнутость классов арифметической иерархии относительно объединения и пересечения.	49
8.11	Дополнение языка из Σ_k лежит в Π_k , и наоборот.	49

8.12	Пример λ -терма, к которому можно применить β -редукцию только после α -конверсии.	49
8.13	Пример λ -терма, не имеющего нормальной формы	49
8.14	Построение комбинаторов сложения и умножения для нумералов Чёрча (с доказательством корректности).	49
9	Вопросы из билетов	51
9.1	Моделирование машины Тьюринга с несколькими лентами на машине Тьюринга с одной лентой.	51
9.2	Эквивалентность следующих утверждений: множество перечислимо, полухарактеристическая функция множества вычислима, множество является областью определения вычислимой функции, множество является проекцией разрешимого множества пар.	52
9.3	Теорема Поста: критерий разрешимости в терминах перечислимости множества и его дополнения.	53
9.4	Неразрешимость проблем самоприменимости и остановки.	53
9.5	Несуществование универсальной totally вычислимой функции.	54
9.6	Неперечислимость и некоперечислимость множества всюду определённых программ или множества программ с конечной областью определения (на выбор). . .	54
9.7	Существование главной универсальной вычислимой функции.	55
9.8	Теорема Райса–Успенского о неразрешимости нетривиальных свойств вычислимых функций.	55
9.9	Теорема Клини о неподвижной точке. Построение программы, на любом входе печатающей некоторый собственный номер.	56
9.10	Теорема об арифметической иерархии: $\Sigma_n \neq \Sigma_{n+1}$, $\Sigma_n \neq \Pi_n$	56
9.11	Теорема Чёрча–Россера (б/д). Единственность нормальной формы.	57
9.12	Построение комбинаторов логических значений, булевых функций, операций с парами, проверки на ноль для нумералов Чёрча (с доказательством корректности). .	58

Логика и арифметика.

1 Определения

1.1 Булевы функции, примеры. Двойственность.

Определение: Булева функция от n аргументов – это любое отображение $f : \{0,1\}^n \rightarrow \{0,1\}$.

Замечание: Число всевозможных комбинаций аргументов, равно 2^n , а количество булевых функций от n аргументов равно 2^{2^n} (для каждой перестановки аргументов есть два значения функции – это 0 или 1).

Определение: Булева функция f^* называется двойственной булевой функции f , если она получена из f инверсией всех аргументов и самой функции, то есть $f^*(x_1, \dots, x_n) = \neg f(\neg x_1, \dots, \neg x_n)$.

		AND	OR	XOR	Импл.	Эквив.	Штрих Шеффера	Стрелка Пирса
a	b	$a \wedge b$	$a \vee b$	$a \oplus b$	$a \rightarrow b$	$a \Leftrightarrow b$	$a b$	$a \downarrow b$
0	0	0	0	0	1	1	1	1
0	1	0	1	1	1	0	1	0
1	0	0	1	1	0	0	1	0
1	1	1	1	0	1	1	0	0

1.2 Классы булевых функций: сохраняющие 0 и 1, монотонные, самодвойственные, линейные.

- ▷ Класс T_0 функций, сохраняющих 0: $f \in T_0$, если $f(0, \dots, 0) = 0$
Принадлежат: 0, id , $a \wedge b$, $a \vee b$, $a \oplus b$
Не принадлежат: 1, $\neg a$
- ▷ Класс T_1 функций, сохраняющих 1: $f \in T_1$, если $f(1, \dots, 1) = 1$
Принадлежат: 1, id , $a \wedge b$, $a \vee b$, $a \rightarrow b$, $a \Leftrightarrow b$
Не принадлежат: 0, $\neg a$
- ▷ Класс M монотонных функций: $f \in M$, если $\forall i(a_i \leq b_i) \Rightarrow f(a_1, \dots, a_n) \leq f(b_1, \dots, b_n)$
Принадлежат: 0, 1, id , $a \wedge b$, $a \vee b$
Не принадлежат: $\neg a$, $a \oplus b$
- ▷ Класс S самодвойственных функций: $f \in S$, если $f(\bar{x}_1, \dots, \bar{x}_n) = \overline{f(x_1, \dots, x_n)}$
Принадлежат: id , $\neg a$, $(x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$
Не принадлежат: 0, 1, $a \wedge b$
- ▷ Класс L линейных функций: $f \in L$, если $f(x_1, \dots, x_n) = a_0 \oplus a_1 x_1 \oplus \dots \oplus a_n x_n$, $a_i \in \{0,1\}$
Принадлежат: 0, 1, id , $\neg a$, $a \Leftrightarrow b$, $a \oplus b$
Не принадлежат: $a \wedge b$

1.3 Пропозициональные формулы. Тавтологии. Конъюнктивные и дизъюнктивные нормальные формы.

Пропозициональные формулы определяются рекурсивно:

Определение: Если p – пропозициональная переменная (символ, обозначающий высказывание), то p есть формула. Если φ есть формула, то $\neg \varphi$ – также формула. Если φ и ψ являются формулами, то $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$ и $(\varphi \rightarrow \psi)$ также являются формулами.

Определение: Пусть $[\varphi](a_1, \dots, a_n)$ – значение формулы на наборе $\bar{a}(a_1, \dots, a_n)$.

1. $[p_i](\bar{a}) = a_i$
2. $[\neg\varphi](\bar{a}) = \text{neg}([\varphi](\bar{a}))$
3. $[\varphi \wedge \psi](\bar{a}) = \text{and}([\varphi](\bar{a}), [\psi](\bar{a}))$ и аналогично с *or*, *impl*

Определение: Литерал – переменная или отрицание переменной.

Определение: Конъюнкт – конъюнкция литералов (\wedge).

Определение: Дизъюнкт – дизъюнкция литералов (\vee).

Определение: КНФ – конъюнкция дизъюнктов. Пример: $f(x, y, z) = (x \vee y) \wedge (y \vee \neg z)$.

Определение: ДНФ – дизъюнкция конъюнктов. Пример: $f(x, y, z) = (x \wedge y) \vee (\neg y \wedge \neg z)$.

Определение: Тавтология – формула, истинная при всех значениях входящих в нее переменных. Пример: $((p \wedge q) \rightarrow p)$.

Определение: СКНФ (СДНФ) – КНФ (ДНФ), содержащая ровно одно вхождение каждой переменной в каждый дизъюнкт (конъюнкт). Пример СКНФ: $f(x, y, z) = (x \vee \neg y \vee z) \wedge (x \vee y \vee \neg z)$.

Теорема: Для любой булевой функции, не равной тождественной 1, \exists СКНФ, ее задающая.

Теорема: Для любой булевой функции, не равной тождественному 0, \exists СДНФ, ее задающая.

1.4 Многочлены Жегалкина.

Определение: Одночленом (моном) Жегалкина называется произведение (конъюнкция) различных переменных. Многочленом (полиномом) Жегалкина называется сумма (по mod 2) различных одночленов.

Базовые функции: а) $\neg x = x \oplus 1$ б) $x \wedge y = xy$ в) $x \vee y = x \oplus y \oplus xy$ г) $x \rightarrow y = 1 \oplus x \oplus xy$ д) $x \Leftrightarrow y = x \oplus y \oplus 1$.

Вычитание и сложение по сути одно и то же, поскольку все вычисления проходят по mod 2.

1.5 Аксиомы исчисления высказываний, modus ponens.

- $$\begin{aligned}
 A_1 &: A \rightarrow (B \rightarrow A); \\
 A_2 &: (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C)); \\
 A_3 &: A \wedge B \rightarrow A; \\
 A_4 &: A \wedge B \rightarrow B; \\
 A_5 &: A \rightarrow (B \rightarrow (A \wedge B)); \\
 A_6 &: A \rightarrow (A \vee B); \\
 A_7 &: B \rightarrow (A \vee B); \\
 A_8 &: (A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow ((A \vee B) \rightarrow C)); \\
 A_9 &: \neg A \rightarrow (A \rightarrow B); \\
 A_{10} &: (A \rightarrow B) \rightarrow ((A \rightarrow \neg B) \rightarrow \neg A); \\
 A_{11} &: A \vee \neg A.
 \end{aligned}$$

В качестве единственного правила вывода выступает modus ponens: $\frac{A \quad A \rightarrow B}{B}$. Эта запись означает, что если выведены формулы A и $A \rightarrow B$, то можно вывести B .

1.6 Логические выводы и выводимые формулы.

Определение: Вывод – конечная последовательность формул, каждая из которых либо является аксиомой, либо получается из ранее встретившихся по правилам вывода.

Определение: Формула называется выводимой, если она встречается в некотором выводе. Утверждение о том, что формула φ выводима в исчислении высказываний (ИВ), записывается так: $\vdash \varphi$.

Пример $\vdash A \rightarrow A$. Обозначим эту формулу B .

- | | |
|--|-------------|
| 1. $A \rightarrow B$ | (аксиома 1) |
| 2. $A \rightarrow (B \rightarrow A)$ | (аксиома 1) |
| 3. $(A \rightarrow (B \rightarrow A)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow A))$ | (аксиома 2) |
| 4. $(A \rightarrow B) \rightarrow (A \rightarrow A)$ | (2,3, MP) |
| 5. $A \rightarrow A$ | (1,4, MP) |

1.7 Резолюции.

Определение: Если $(A \vee x)$ и $(B \vee \neg x)$ одновременно истинны, то $(A \vee B)$ тоже истинно. Такое рассуждение называется правилом резолюции: $\frac{(A \vee x) \quad (B \vee \neg x)}{(A \vee B)}$

Определение: Дизъюнкт $(A \vee B)$ называется резольвентой дизъюнктов $(A \vee x)$ и $(B \vee \neg x)$.

Замечание: Резольвента дизъюнктов x и $\neg x$ – это пустой дизъюнкт, т.е. \perp .

Метод резолюций для проверки КНФ на выполнимость: Будем добавлять к набору дизъюнктов все возможные резольвенты.

Теорема: Метод резолюций всегда заканчивает свою работу, причём для невыполнимых КНФ выводится \perp , а для выполнимых не выводится. Таким образом, метод резолюций позволяет проверить выполнимость формулы.

1.8 Языки первого порядка: индивидные переменные, логические связки, кванторы, функциональные и предикатные символы, термы, атомарные формулы, формулы общего вида.

Если кванторы \forall и \exists могут стоять только по переменным, то говорят о языке первого порядка. Если же они могут стоять по более сложным объектам, таким как множества или функции, то говорят о языке второго порядка. Возможны и языки высших порядков.

Определение: Языки первого порядка – правила составления формул с кванторами, где кванторы берутся по отдельным объектам.

Алфавит языка первого порядка:

- ▷ Индивидная переменная (обычно буквы x, y, z, t, u, v, w) – символ формального языка, служащий для обозначения произвольного элемента.
- ▷ Сигнатура $\sigma = \langle P_1, \dots, P_k, f_1, \dots, f_m \rangle$ – набор предикатных и функциональных символов, обозначающих те или иные связи между объектами.

1. Предикат валентности N на множестве A – это функция $P : A^N \rightarrow \{0,1\}$.

Предикатный символ – символ, обозначающий предикат.

Например: $P^{(3)}, <^{(2)}, \subset^{(2)}, Prime^{(1)}$.

Предикатные символы нулевой валентности обычно не рассматривают.

2. Функция валентности N на множестве A – это функция $f : A^N \rightarrow A$.

Функциональный символ – символ алфавита, обозначающий функцию.

Например: $f^{(3)}, +^{(2)}, \cap^{(2)}, \sin^{(1)}$.

Функциональные символы валентности ноль – это константы: $11, \pi, e, \emptyset$.

- ▷ Символы логических операций: $\wedge, \vee, \neg, \rightarrow$
- ▷ Кванторы: \forall, \exists
- ▷ Служебные символы: скобки и запятые.

Определение: Терм – строка, рекурсивно построенная по следующим правилам:

1. Индивидуальная переменная есть терм;
2. Функциональный символ валентности ноль (т.е. $f^{(0)} = \text{const}$) есть терм;
3. Если $k > 0$, $f^{(k)}$ — функциональный символ валентности k , а t_1, \dots, t_k — термы, то $f^{(k)}(t_1, \dots, t_k)$ также терм.

Определение: Атомарной формулой называется выражение вида $P^{(k)}(t_1, \dots, t_k)$, где $k > 0$, t_1, \dots, t_k — термы, а $P^{(k)}$ — предикатный символ валентности k .

Определение: Формулой (первого порядка) называется строка, рекурсивно построенная по следующим правилам:

1. Атомарная формула является формулой;
2. Если φ и ψ являются формулами, то строки $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \rightarrow \psi)$, $\neg\varphi$ также являются формулами;
3. Если φ является формулой, а x — индивидуальная переменная, то $\exists x \varphi$ и $\forall x \varphi$ также являются формулами.

1.9 Интерпретация языка первого порядка. Оценка переменных. Общезначимые формулы.

Определение: Пусть фиксирована некоторая сигнатура σ . Чтобы задать интерпретацию сигнатуры σ , необходимо:

- ▷ указать некоторое непустое множество M , называемое носителем интерпретации;
- ▷ для каждого k -местного предикатного символа $P \in \sigma$ задана некоторая функция $[P] : M^k \rightarrow \{0, 1\}$;
- ▷ для каждого k -местного функционального символа $f \in \sigma$ задана некоторая функция $[f] : M^k \rightarrow M$;

Определение: Оценкой переменных называется функция $\pi : \text{Var} \rightarrow M$, где Var — множество индивидуальных переменных.

1. $[\varphi](\pi)$ — значение формулы φ на оценке π
2. $[t](\pi)$ — значение терма t на оценке π

Замечание: Множество Var заранее фиксировано, все термы и формулы строятся на его основе, а оценка задаёт значения всех переменных из этого множества.

Пусть фиксированы интерпретация I и оценка π . Тогда для каждого терма t должно возникнуть его значение, которое мы будем обозначать через $[t](\pi)$ (зависимость от интерпретации в явном виде писать не будем, поскольку она не будет меняться в дальнейших определениях, а оценка будет). Поскольку терм строился рекурсивно, его значение также будет определяться последовательно для всех шагов рекурсии.

- * Если $t = x$, где x — переменная, то $[t](\pi) = \pi(x)$
- * Если $t = c$, где c — функциональный символ валентности 0, то $[t](\pi) = [c]$
- * Если $t = f(t_1, \dots, t_k)$, то $[t](\pi) = [f]([t_1](\pi), \dots, [t_k](\pi))$

Значение формулы также определяется рекурсивно.

* Если $\varphi = P(t_1, \dots, t_k)$ – атомарная формула, то $[\varphi](\pi) = [P]([t_1](\pi), \dots, [t_k](\pi))$

* Если $\varphi = \neg\psi$, то $[\varphi](\pi) = \text{not}([\psi](\pi))$

* Если $\varphi = \psi \vee \gamma$, то $[\varphi](\pi) = \text{or}([\psi](\pi), [\gamma](\pi))$ (аналогично для \wedge, \rightarrow)

Замечание: Символы логических операций слева от знака равенства являются просто символами, а справа мы обозначаем соответствующую булеву функцию.

Наконец, перейдём к самому интересному – кванторам. Это единственный случай, где изменяется не только формула, значение которой определяется, но и оценка.

* Если $\varphi = \forall x\psi$, то $[\varphi](\pi) = \bigwedge_{m \in M} [\psi](\pi_{x \rightarrow m})$

* Если $\varphi = \exists x\psi$, то $[\varphi](\pi) = \bigvee_{m \in M} [\psi](\pi_{x \rightarrow m})$

$$\pi_{x \rightarrow m}(y) = \begin{cases} \pi(y), & y \neq x \\ m, & y = x \end{cases}$$

$$\bigwedge_{m \in M} Q_m = \begin{cases} 1, & \text{все } Q_m \text{ равны } 1 \\ 0, & \text{иначе} \end{cases}$$

$$\bigvee_{m \in M} Q_m = \begin{cases} 0, & \text{все } Q_m \text{ равны } 0 \\ 1, & \text{иначе} \end{cases}$$

Определение: Общезначимая формула – формула, истинная при любой интерпретации на любой оценке.

Пример 1: Для любой формулы φ формулы $\forall x \forall y \varphi \rightarrow \forall y \forall x \varphi$ и $\exists x \exists y \varphi \rightarrow \exists y \exists x \varphi$ общезначимы.

Пример 2: Для любой формулы φ общезначима формула $\exists x \forall y \varphi \rightarrow \forall y \exists x \varphi$. Обратная импликация общезначима не всегда.

1.10 Свободные и связанные вхождения переменных. Параметры формулы.

Определение: Говорят, что переменные, от которых не зависят значения формул, связаны некоторым оператором (\sum, \lim, \max или каким-нибудь ещё) и потому называются связанными (имеются в виду переменная i в выражении $\sum_{i=0}^n a^i$ и тому подобные), а остальные переменные свободны. Более корректно говорить не о связанных и свободных переменных, а о связанных и свободных вхождениях переменных.

Определение: Множество *параметров* терма t или формулы φ называется множеством $\text{Param}(t)$ (соотв., $\text{Param}(\varphi)$), определяемое рекурсивно таким образом:

- Если $t = x$, где x – переменная, то $\text{Param}(t) = \{x\}$;
- Если $t = c$, где c – константный символ, то $\text{Param}(t) = \emptyset$;
- Если $t = f(t_1, \dots, t_k)$, то $\text{Param}(t) = \bigcup_{i=1}^k \text{Param}(t_i)$;
- Если $\varphi = P(t_1, \dots, t_k)$, то $\text{Param}(\varphi) = \bigcup_{i=1}^k \text{Param}(t_i)$;
- Если $\varphi = \neg\psi$, то $\text{Param}(\varphi) = \text{Param}(\psi)$;
- Если $\varphi = (\psi \wedge \eta)$, $\varphi = (\psi \vee \eta)$ или $\varphi = (\psi \rightarrow \eta)$, то $\text{Param}(\varphi) = \text{Param}(\psi) \cup \text{Param}(\eta)$;
- Если $\varphi = \exists x\psi$ или $\varphi = \forall x\psi$, то $\text{Param}(\varphi) = \text{Param}(\psi) \setminus \{x\}$.

Иначе говоря, любое новое вхождение переменной добавляет её в список параметров, а навешивание квантора – исключает.

1.11 Выразимость предиката или функции в данной интерпретации.

Зафиксируем некоторую сигнатуру σ и её интерпретацию с носителем M .

Определение: Формула φ с параметрами x_1, \dots, x_m выражает предикат $P : M^m \rightarrow \{0,1\}$, если $\varphi(a_1, \dots, a_m) = 1 \Leftrightarrow P(a_1, \dots, a_m) = 1$.

Определение: Функция $f : M^n \rightarrow M$ называется выразимой, если существует формула φ от $n+1$ переменных, истинная на любой оценке π , такой что $\pi(x_1) = a_1, \dots, \pi(x_n) = a_n, \pi(x_{n+1}) = f(a_1, \dots, a_n)$, и ложная на любой другой оценке.

Пример 1: $x \geq y \Leftrightarrow \exists z : x = y + z$ в \mathbb{N} . Предикат \geq выразим в интерпретации $\langle \mathbb{N}, +, = \rangle$ и невыразим в интерпретации $\langle \mathbb{Z}, +, = \rangle$.

Пример 2: Пусть $\langle 2^A, \subset \rangle$: $x = y \Leftrightarrow (x \subset y \wedge y \subset x)$; $x = \emptyset \Leftrightarrow \forall y(x \subset y)$.

1.12 Аксиомы исчисления предикатов, правила Бернаиса, правило обобщения.

Аксиомы исчисления предикатов:

- ▷ $A_1 - A_{11}$ – аксиомы исчисления высказываний.
- ▷ $A_{12} : \forall x \varphi \rightarrow \varphi(t/x)$, где t/x – это корректная подстановка терма t в φ вместо свободных вхождений x .
- ▷ $A_{13} : \varphi(t/x) \rightarrow \exists x \varphi$.

Корректная подстановка означает, что терм t не содержит переменных, по которым стоят кванторы в φ .

Пример: Следствием из A_{12}, A_{13} является силлогизма: $\forall x \varphi \rightarrow \exists x \varphi$.

Правила вывода:

1. Modus ponens:

$$\frac{A \quad A \rightarrow B}{B}$$

2. 1-ое правило Бернаиса:

$$\frac{\varphi \rightarrow \psi}{\exists x \varphi \rightarrow \psi}$$

3. 2-ое правило Бернаиса:

$$\frac{\varphi \rightarrow \psi}{\varphi \rightarrow \forall x \psi}$$

4. Правило обобщения:

$$\frac{\varphi}{\forall x \varphi}$$

Пример Имеется формула:

$$\exists x \forall y \phi \rightarrow \forall y \exists x \phi.$$

Продемонстрируем ее вывод:

1. $\forall y \phi \rightarrow \phi$ (аксиома 12);
2. $\phi \rightarrow \exists x \phi$ (аксиома 13);
3. $\forall y \phi \rightarrow \exists x \phi$ (силлогизм);
4. $\exists x \forall y \phi \rightarrow \exists x \phi$ (первое правило Бернаиса);
5. $\exists x \forall y \phi \rightarrow \forall y \exists x \phi$ (второе правило Бернаиса).

1.13 Аксиомы равенства.

Определение: Пусть σ — произвольная сигнатура. Аксиомами равенства в сигнатуре σ будут формулы:

1. $\forall x (x = x)$ — аксиома рефлексивности,
2. $\forall x \forall y ((x = y) \rightarrow (y = x))$ — аксиома симметричности,
3. $\forall x \forall y \forall z (((x = y) \wedge (y = z)) \rightarrow (x = z))$ — аксиома транзитивности,

а также для каждого функционального символа сформулируем аксиому равенства, которая говорит, что его значение не меняется, если аргументы заменить на равные.

Пример: Для двухместного функционального символа f :

$$\forall x_1 \forall x_2 \forall y_1 \forall y_2 (((x_1 = x_2) \wedge (y_1 = y_2)) \rightarrow (f(x_1, y_1) = f(x_2, y_2)))$$

Для предикатных символов аксиомы равенства говорят, что истинный предикат остается истинным, если заменить аргументы на равные.

Определение: Формальная арифметика — это аксиоматическая теория, расширяющая исчисление предикатов с равенством.

1.14 Теории, модели, нормальные модели.

Рассмотрим сигнатуру σ .

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.

Пример: $P, \forall x R(x), \exists x \forall y P(x, y), \forall x Q(x) \rightarrow \neg(\forall x \exists y R(x, y))$

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

Определение: Интерпретация M сигнатуры σ называется нормальной, если предикат равенства интерпретируется как тождественное совпадение элементов носителя.

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

1.15 Аксиомы арифметики Пеано.

Стандартная интерпретация: \mathbb{N} , S — следующее число, $0, +, -, =$ понимаются как обычно.

Аксиомы связанные с порядком:

1. $\nexists x Sx = 0$
2. $\forall x \forall y (Sx = Sy \rightarrow x = y)$
3. Принцип индукции: $(\varphi(0) \wedge \forall x (\varphi(x) \rightarrow \varphi(Sx))) \rightarrow \forall x \varphi(x)$

Аксиомы, связанные с арифметическими действиями:

1. $\forall x x + 0 = x$
2. $\forall x \forall y x + Sy = S(x + y)$
3. $\forall x x \cdot 0 = 0$
4. $\forall x \forall y x \cdot Sy = x \cdot y + x$

Пример: Как вывести, что $2 + 2 = 4$? В нашем языке это означает, что $SS0 + SS0 = SSSS0$

1. $\forall x \forall y \ x + Sy = S(x + y)$ – аксиома
2. $SS0 + SS0 = S(SS0 + S0)$ – подстановка $x = SS0, y = S0$
3. $SS0 + S0 = S(SS0 + 0)$ – подстановка $x = SS0, y = 0$
4. $\forall x \ x + 0 = x$ – аксиома
5. $SS0 + 0 = SS0$ – подстановка $x = SS0$
6. $\forall x \forall y \ (x = y \rightarrow Sx = Sy)$ – аксиома равенства
7. $SS0 + 0 = SS0 \rightarrow S(SS0 + 0) = SSS0$ – подстановка $x = SS0 + 0, y = SS0$
8. $S(SS0 + 0) = SSS0$ – modus ponens
9. $SS0 + S0 = SSS0$ – по транзитивности
10. $S(SS0 + S0) = SSSS0$ – подстановка $x = S(SS0 + 0), y = SSS0$
11. $SS0 + SS0 = SSSS0$ – по транзитивности с 2.

1.16 Совместность, непротиворечивость, полнота теории.

Определение: Теория Γ называется совместной, если все формулы из Γ могут быть одновременно истинны в некоторой интерпретации.

Пример 1: $\{p \rightarrow q, q \rightarrow p, p \wedge q\}$ – совместно, так как все верны на $(1,1)$.

Пример 2: $\{\neg(p \rightarrow q), \neg(q \rightarrow p)\}$ – несовместно, тк первая формула верна только на $(1,0)$, а вторая – только на $(0,1)$.

Утверждение 1: $\Gamma = \{\varphi\} : \Gamma$ совместно $\Leftrightarrow \varphi$ выполнима.

Утверждение 2: $\Gamma = \{\varphi_1, \dots, \varphi_n\} : \Gamma$ совместно $\Leftrightarrow (\varphi_1 \wedge \dots \wedge \varphi_n)$ выполнима.

Определение: Теория Γ называется противоречивой, если из нее выводится некоторая формула φ и ее отрицание $\neg\varphi$, и непротиворечивой в противном случае.

Определение: Непротиворечивая теория Γ называется полной (в данной сигнатуре), если для любой замкнутой формулы этой сигнатуры либо $\Gamma \vdash \varphi$, либо $\Gamma \vdash \neg\varphi$.

2 Простые утверждения

2.1 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:

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

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, \dots, 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:

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

Можно заметить, что дизъюнкт $\bigvee_{i=1}^n p_i^{1-a_i}$ ложен на наборе (a_1, \dots, 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 $p \vee \neg p$. \square

2.2 Замкнутость классов Поста относительно композиции.

Определение: Композиция функций из множества F :

- ▷ Композиция порядка 0 – все проекторы, т.е. функции вида $pr_i(x_1, \dots, x_n) = x_i$.
- ▷ Композиция порядка $m + 1$ – функция вида $h(p_1, \dots, p_n) = f(g_1(p_1, \dots, p_n), \dots, g_k(p_1, \dots, p_n))$, где $f \in F$, f зависит от k аргументов, g_1, \dots, g_k – композиции порядка $\leq m$, хотя бы одно из них в точности m .

Определение: Замыканием класса Q называется класс $[Q]$, составленный из всех композиций любого уровня вложенности функций из класса Q .

Определение: Класс булевых функций Q называется замкнутым, если $Q = [Q]$.

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

- ▷ $[T_1] = T_1$: $h(1, \dots, 1) = f(g_1(1, \dots, 1), \dots, g_k(1, \dots, 1)) = f(1, \dots, 1) = 1$.
- ▷ $[T_0] = T_0$: аналогично T_1 .
- ▷ $[M] = M$: $\left\{ \begin{array}{c} x_1 \leq y_1 \\ \dots \\ x_n \leq y_n \end{array} \right\} \Rightarrow \left\{ \begin{array}{c} g_1(x_1, \dots, x_n) \leq g_1(y_1, \dots, y_n) \\ \dots \\ g_k(x_1, \dots, x_n) \leq g_k(y_1, \dots, y_n) \end{array} \right\} \Rightarrow$
 $f(g_1(x_1, \dots, x_n), \dots, g_k(x_1, \dots, x_n)) \leq f(g_1(y_1, \dots, y_n), \dots, g_k(y_1, \dots, y_n))$.
- ▷ $[S] = S$: $f(g_1(\neg p_1, \dots, \neg p_n), \dots, g_k(\neg p_1, \dots, \neg p_n)) = f(\neg g_1(p_1, \dots, p_n), \dots, \neg g_k(p_1, \dots, p_n)) =$
 $\neg f(g_1(p_1, \dots, p_n), \dots, g_k(p_1, \dots, p_n))$.
- ▷ $[L] = L$: Достаточно заметить, что при подстановке вместо переменных линейной функции каких-то других линейных функций, не могут появиться конъюнкции переменных в слагаемых. Поэтому при такой подстановке получается линейная функция.

2.3 Вывод формулы вида $A \rightarrow A$ в исчислении высказываний.

Доказательство приведено в определении 1.6.

2.4 Теорема о корректности исчисления высказываний.

Теорема: Если $\vdash \varphi$, то φ – тавтология.

▲ Любая аксиома есть тавтология. Проверяется непосредственно по таблице истинности. Правило МР тоже корректно: если A и $A \rightarrow B$ всегда истинны, то B тоже всегда истинно. Индукцией по номеру формулы в выводе доказывается, что все формулы в выводе тавтологичны, что и требовалось. ■

2.5 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: $(l_1 \vee x_1) \wedge (\neg x_1 \vee l_2 \vee x_2) \wedge \dots \wedge (\neg x_{k-2} \vee l_{k-1} \vee x_{k-1}) \wedge (\neg x_{k-1} \vee l_k)$, где переменные x_1, \dots, x_{k-1} 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 $i \geq j$ 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. ■

2.6 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 $(p_{i1} \vee p_{i2} \vee \dots \vee p_{i8})$.
 - 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 $\neg p_{ij}$).

2.7 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. $(x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee x_2) \vdash (x_2 \vee x_3)$
2. $(x_2 \vee x_3) \wedge (\neg x_2 \vee x_3) \vdash x_3$
3. $x_3 \wedge \neg x_3 \vdash \perp$

2.8 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 $\forall x \in \text{Param}(\varphi)$ (или $x \in \text{Param}(t)$) выполнено $\pi(x) = \rho(x)$, то $[\varphi](\pi) = [\varphi](\rho)$ (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 $t = f(t_1, \dots, t_k)$, то в силу $\text{Param}(t_i) \subset \text{Param}(t)$ по предположению индукции имеем $[t_i](\pi) = [t_i](\rho)$. Поэтому $[t](\pi) = [f]([t_1](\pi), \dots, [t_k](\pi)) = [f]([t_1](\rho), \dots, [t_k](\rho)) = [t](\rho)$;
- ▷ Если $\varphi = P(t_1, \dots, t_k)$, то рассуждение аналогично предыдущему;
- ▷ Если $\varphi = \neg\psi$, то $[\varphi](\pi) = \neg[\psi](\pi) = \neg[\psi](\rho) = [\varphi](\rho)$. Здесь предположение индукции использовано во втором равенстве;
- ▷ Если $\varphi = (\psi \wedge \gamma)$, то $[\varphi](\pi) = [\psi](\pi) \wedge [\gamma](\pi) = [\psi](\rho) \wedge [\gamma](\rho) = [\varphi](\rho)$. Здесь во втором равенстве использовано предположение индукции и вложения $\text{Param}(\psi) \subset \text{Param}(\varphi)$ и $\text{Param}(\gamma) \subset \text{Param}(\varphi)$. Случай $\varphi = (\psi \vee \gamma)$ и $\varphi = (\psi \rightarrow \gamma)$ разбираются аналогично;
- ▷ Если $\varphi = \exists x\psi$, то ключевое соображение состоит в следующем: если $\pi(y) = \rho(y)$ для всех $y \in \text{Param}(\psi) \setminus \{x\}$, то $\pi_{x \rightarrow m}(y) = \rho_{x \rightarrow m}(y)$ уже для всех $y \in \text{Param}(\psi)$, в том числе для $y = x$. Действительно, $\pi_{x \rightarrow m}(y) = \rho_{x \rightarrow m}(y) = m$, а для $y \neq x$ равенство есть по предположению. Поэтому $[\varphi](\pi) = \bigvee_{m \in M} [\psi](\pi_{x \rightarrow m}) = \bigvee_{m \in M} [\psi](\rho_{x \rightarrow m}) = [\varphi](\rho)$. Аналогичное рассуждение работает и для $\varphi = \forall x\psi$. ■

2.9 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:

- ▷ $x = 0 \Leftrightarrow \forall y \, x \cdot y = x$
- ▷ $x = 1 \Leftrightarrow \forall y \, x \cdot y = y$
- ▷ $x \dot{:} y \Leftrightarrow \exists z \, x = y \cdot z$
- ▷ $\text{Prime}(p) \Leftrightarrow (p \neq 1 \wedge \forall q(p \dot{:} q \rightarrow (q = 1 \vee q = p)))$
- ▷ $d = \text{НОД}(x, y) \Leftrightarrow (x \dot{:} d \wedge y \dot{:} d \wedge \forall k((x \dot{:} k \wedge y \dot{:} k) \rightarrow d \dot{:} k))$
- ▷ $d = \text{НОК}(x, y) \Leftrightarrow (d \dot{:} x \wedge d \dot{:} y \wedge \forall k((k \dot{:} x \wedge k \dot{:} y) \rightarrow k \dot{:} d))$

2.10 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: $\exists x A(x) \wedge \exists x B(x) \leftrightarrow \exists x A(x) \wedge \exists y B(y) \leftrightarrow \exists x (A(x) \wedge \exists y B(y)) \leftrightarrow \exists x \exists y (A(x) \wedge B(y)).$

2.11 Вывод правила обобщения в исчислении предикатов.

Правило обобщения:

$$\frac{\varphi}{\forall x \varphi}.$$

▲ Докажем правило обобщения:

1. φ (считаем, что уже вывели)
2. ψ (некоторая аксиома, не зависящая от x)
3. $\varphi \rightarrow (\psi \rightarrow \varphi)$ (Ах. 1)
4. $\psi \rightarrow \varphi$ (МР 1-3)
5. $\psi \rightarrow \forall x \varphi$ (2-ое правило Бернаиса)
6. $\forall x \varphi$ (МР 2-5) ■

2.12 Вывод формулы вида $\exists x \forall y \varphi \rightarrow \forall y \exists x \varphi$ в исчислении предикатов.

Доказательство приведено в определении [1.12](#).

2.13 Любое совместное множество формул первого порядка непротиворечиво.

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

2.14 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).

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: Из теоремы в сильной форме следует теорема в слабой форме.

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

2.15 Выразимость в арифметике свойств «быть степенью двойки», «быть степенью четвёрки».

Пусть задано $\langle \mathbb{N}, 0, S, +, \cdot, = \rangle$. Заметим, что $x \dot{:} y \Leftrightarrow \exists z x = y \cdot z$. Тогда x является степенью 2 $\Leftrightarrow \forall d(x \dot{:} d \rightarrow (d = 1 \vee d \dot{:} 2))$.

Аналогично, x является степенью 4 $\Leftrightarrow \exists y \forall d((y \cdot y = x) \wedge (y \dot{:} d \rightarrow (d = 1 \vee d \dot{:} 2)))$.

2.16 Множество предложений, выводимых в арифметике Пеано, перечислимо.

Определение: Множество называется перечислимым, если существует алгоритм, который печатает все элементы этого множества и только их.

▲ Пусть \mathcal{A} – система аксиом в арифметике Пеано. Мы можем алгоритмически перечислять конечные последовательности формул (например, в порядке возрастания суммы длин формул в такой последовательности). Для каждой последовательности формул можно проверить, является ли она выводом из \mathcal{A} . Если очередная последовательность формул оказывается выводом из \mathcal{A} , то мы добавляем последнюю формулу из этой последовательности к списку выводимых формул. Так мы рано или поздно перечислим каждую формулу, выводимую из данной системы аксиом, что и требовалось. ■

3 Вопросы из билетов

3.1 Теорема об однозначном представлении булевой функции многочленом Жегалкина.

Теорема (Жегалкина): Каждая булева функция единственным образом представляется в виде полинома Жегалкина.

▲ Заметим, что различных булевых функций от n переменных 2^{2^n} штук. При этом конъюнкций вида $x_{i_1} \dots x_{i_k}$ существует ровно 2^n , так как из n возможных сомножителей каждый или входит в конъюнкцию, или нет. В полиноме у каждой такой конъюнкции стоит 0 или 1, то есть существует 2^{2^n} различных полиномов Жегалкина от n переменных.

Теперь достаточно лишь доказать, что различные полиномы реализуют различные функции. Предположим противное. Тогда приравняв два различных полинома и перенеся один из них в другую часть равенства, получим полином, тождественно равный нулю и имеющий ненулевые коэффициенты. Тогда рассмотрим слагаемое с единичным коэффициентом наименьшей длины, то есть с наименьшим числом переменных, входящих в него (любой один, если таких несколько). Подставив единицы на места этих переменных и нули на места остальных, получим, что на этом наборе только одно это слагаемое принимает единичное значение, то есть нулевая функция на одном из наборов принимает значение 1. Противоречие. Значит, каждая булева функция реализуется полиномом Жегалкина единственным образом. ■

3.2 Теорема о дедукции для исчисления высказываний.

Теорема о дедукции: Пусть Γ, A – это $\Gamma \cup \{A\}$, тогда верно:

$$\frac{\Gamma \vdash A \rightarrow B}{\Gamma, A \vdash B} \quad \Downarrow$$

▲ (\Downarrow) Пусть $\Gamma \vdash A \rightarrow B$, тогда $\Gamma, A \vdash A, A \rightarrow B$. К выводу применим МР: $A, A \rightarrow B \vdash B$. Тогда по транзитивности $\Gamma, A \vdash B$.

(\Uparrow) Доказывается индукцией по длине вывода B из Γ, A

(1) Если этот вывод – длины 1, то B – аксиома или гипотеза (т.е. формула из Γ).

Если B – аксиома, то имеем вывод $A \rightarrow B$ (из \emptyset):

1. B (аксиома)
2. $B \rightarrow (A \rightarrow B)$ (аксиома A1)
3. $A \rightarrow B$ (1,2, МР)

(2) Если $B \in \Gamma$, то имеем такой же вывод $A \rightarrow B$ из Γ :

1. B (гипотеза)
2. $B \rightarrow (A \rightarrow B)$ (аксиома A1)
3. $A \rightarrow B$ (1,2, МР)

(3) Если $B = A$, то $A \rightarrow B = A \rightarrow A$. Но $\vdash A \rightarrow A$ (пример из определений 1.6).

(4) Предположим теперь, что $\Gamma, A \vdash B$ и утверждение (\Uparrow) верно для всех более коротких выводов, т.е. для всех C , если $\Gamma, A \vdash C$ и вывод C из Γ, A короче, чем вывод B , то $\Gamma \vdash A \rightarrow C$.

Покажем, что $\Gamma \vdash A \rightarrow B$. Рассмотрим вывод из Γ, A , который заканчивается формулой B . При этом B может оказаться аксиомой или гипотезой (тогда все предыдущие формулы для доказательства B не нужны). Но в этом случае $\Gamma \vdash A \rightarrow B$ по (1)–(3).

Остается случай, когда B получается по МР из формул $C, C \rightarrow B$, причем $\Gamma, A \vdash C$ и $\Gamma, A \vdash C \rightarrow B$ с более короткими доказательствами. По предположению индукции имеем:

(*) $\Gamma \vdash A \rightarrow C, A \rightarrow (C \rightarrow B)$.

С другой стороны,

(**) $A \rightarrow C, A \rightarrow (C \rightarrow B) \vdash A \rightarrow B$:

1. $A \rightarrow C$ (гипотеза)
2. $A \rightarrow (C \rightarrow B)$ (гипотеза)
3. $(A \rightarrow (C \rightarrow B)) \rightarrow ((A \rightarrow C) \rightarrow (A \rightarrow B))$ (аксиома A2)
4. $(A \rightarrow C) \rightarrow (A \rightarrow B)$ (2,3, MP)
5. $A \rightarrow B$ (1,4, MP)

Из (*), (**) по транзитивности получаем $\Gamma \vdash A \rightarrow B$. ■

3.3 Теорема о полноте исчисления высказываний.

Лемма 32 (базовая). *Имеют место следующие выводимости:*

$$\begin{array}{llll}
 A, B \vdash A \wedge B & A, B \vdash A \vee B & A, B \vdash A \rightarrow B & \\
 A, \neg B \vdash \neg(A \wedge B) & A, \neg B \vdash A \vee B & A, \neg B \vdash \neg(A \rightarrow B) & A \vdash \neg(\neg A) \\
 \neg A, B \vdash \neg(A \wedge B) & \neg A, B \vdash A \vee B & \neg A, B \vdash A \rightarrow B & \neg A \vdash \neg A \\
 \neg A, \neg B \vdash \neg(A \wedge B) & \neg A, \neg B \vdash \neg(A \vee B) & \neg A, \neg B \vdash A \rightarrow B &
 \end{array}$$

Поясним смысл леммы. Слева от знака выводимости стоят либо формулы A и B , либо их отрицания. Справа стоит более сложная формула, либо её отрицание в зависимости от того, что из двух верно, когда верны обе посылки. Можно сказать, что лемма моделирует вычисление значения по таблице истинности через выводимость.

Доказательство. Первая выводимость про конъюнкцию следует из пятой аксиомы, остальные получаются контрапозицией из третьей или четвёртой аксиом.

Первые три выводимости про дизъюнкцию следуют из шестой и седьмой аксиом. Последняя выводится так: добавим в список посылок $A \vee B$, далее по правилу разбора случаев нужно вывести противоречие и из $\neg A, \neg B, A$, и из $\neg A, \neg B, B$. В каждом из случаев противоречие есть прямо в списке посылок.

Первая, третья и четвёртая выводимости про импликацию следуют из первой и девятой аксиом. Вторая выводится так: добавим в список посылок $A \rightarrow B$, по modus ponens выводится B , а $\neg B$ уже есть в списке посылок. Значит, противоречие выведено, что и требовалось.

Первая выводимость про отрицание уже доказана, вторая тривиальна. □

Лемма 33 (основная). *Пусть A — формула, $x \in \{0, 1\}$. Через A^x обозначим формулу A , если $x = 1$, и формулу $\neg A$, если $x = 0$. Далее, пусть φ — формула от n переменных, выражающая функцию f . Тогда для всех формул A_1, \dots, A_n и значений x_1, \dots, x_n выполнено*

$$A_1^{x_1}, \dots, A_n^{x_n} \vdash \varphi(A_1, \dots, A_n)^{f(x_1, \dots, x_n)}.$$

Доказательство. Будем доказывать утверждение индукцией по построению формулы. В качестве базы можно было бы взять базовую лемму, но мы сделаем ещё один шаг назад. Пусть φ — переменная, т. е. $\varphi(A_1, \dots, A_n) = A_i$. В таком случае f — проектор, т. е. $f(x_1, \dots, x_n) = x_i$ и в правой части стоит просто одна из посылок.

Теперь докажем переход. Для разных связок он делается одинаково, возьмём для примера конъюнкцию. Таким образом, формула φ есть конъюнкция $\gamma \wedge \eta$, а функция f есть также конъюнкция функций g и h , но уже в смысле булевой функции, а не синтаксической связки. По предположению индукции имеем $A_1^{x_1}, \dots, A_n^{x_n} \vdash \gamma(A_1, \dots, A_n)^{g(x_1, \dots, x_n)}$ и $A_1^{x_1}, \dots, A_n^{x_n} \vdash \eta(A_1, \dots, A_n)^{h(x_1, \dots, x_n)}$. Далее, по базовой лемме имеем

$$\gamma(A_1, \dots, A_n)^{g(x_1, \dots, x_n)}, \eta(A_1, \dots, A_n)^{h(x_1, \dots, x_n)} \vdash (\gamma \wedge \eta)(A_1, \dots, A_n)^{(g \wedge h)(x_1, \dots, x_n)}.$$

Последняя формула есть $\varphi(A_1, \dots, A_n)^{f(x_1, \dots, x_n)}$. По правилу сечения получаем, что $A_1^{x_1}, \dots, A_n^{x_n} \vdash \varphi(A_1, \dots, A_n)^{f(x_1, \dots, x_n)}$, что и требовалось. Переходы для остальных связок доказываются аналогично. Таким образом, индуктивное утверждение доказано. \square

Определение 35. Множество пропозициональных формул Γ называется *совместным* (satisfiable, semantically consistent), если все формулы из Γ могут быть одновременно истинными на некотором наборе.

Определение 36. Множество пропозициональных формул Γ называется *противоречивым* (inconsistent), если из него выводится некоторая формула B и её отрицание, и *непротиворечивым* (consistent) в противном случае.

Теорема 37. *Множество Γ непротиворечиво тогда и только тогда, когда оно совместно.*

Прежде, чем доказывать эту теорему, покажем, как из неё следуют теоремы о корректности и полноте.

Утверждение 38. *Из теоремы 37 следуют теоремы о корректности и о полноте.*

Доказательство. Пусть формула φ выводима. В таком случае множество $\{\neg\varphi\}$ противоречиво: из него выводится как сама φ (она выводится из любого множества), так и $\neg\varphi$ (она есть в списке посылок). По контрапозиции к теореме 37 множество $\{\neg\varphi\}$ несовместно. Это означает, что ни на каком наборе $\neg\varphi$ не будет истинным. Поэтому φ , напротив, всюду истинно, т. е. φ — тавтология.

Пусть теперь φ — тавтология. В таком случае множество $\{\neg\varphi\}$ несовместно. По контрапозиции к теореме 37 оно будет противоречивым. Отсюда по правилу рассуждения от противного выводится $\neg\neg\varphi$, а по закону снятия двойного отрицания выводится и сама φ , что и требовалось. \square

Лемма 39. *Если $\Gamma \vdash A$ и на некотором наборе значений \mathbf{x} все формулы из Γ истинны, то и формула A на этом наборе истинна.*

Доказательство. Эта лемма аналогична теореме о корректности. Посмотрим на вывод формулы A . Каждая его формула либо является аксиомой и потому истинна на любом наборе, в том числе на \mathbf{x} , либо принадлежит Γ , и потому тоже истинна на \mathbf{x} , либо получена из двух более ранних по правилу modus ponens. В этом случае эти формулы истинны на \mathbf{x} по предположению индукции, и потому новая формула также истинна. \square

Теперь мы уже можем доказать, что любое совместное множество непротиворечиво. Действительно, пусть Γ совместно, но противоречиво. Тогда все формулы из Γ истинны на некотором наборе \mathbf{x} , но при этом $\Gamma \vdash B$ и $\Gamma \vdash \neg B$. По предыдущей лемме и B , и $\neg B$ должны быть истинны на наборе \mathbf{x} . Но это невозможно, поэтому совместное Γ противоречивым быть не может.

В обратную сторону доказательство посложнее. Идея его такова: сначала расширим произвольное непротиворечивое множество Γ до полного непротиворечивого множества Δ , а затем докажем, что Δ совместно.

Определение 40. Непротиворечивое множество Δ называется *полным* (complete), если для любой формулы φ выполнено либо $\Delta \vdash \varphi$, либо $\Delta \vdash \neg\varphi$.

Доказанная нами основная лемма позволяет упростить определение:

Лемма 41. *Непротиворечивое множество Δ полно тогда и только тогда, когда для любой переменной p выполнено либо $\Delta \vdash p$, либо $\Delta \vdash \neg p$.*

Доказательство. В одну сторону это верно, т. к. переменная является формулой. В другую сторону: для каждой переменной, входящей в формулу, выводится либо она, либо её отрицание. По основной лемме из этих литералов выводится либо φ , либо $\neg\varphi$. По правилу сечения получаем, что φ или $\neg\varphi$ выводится из Δ , что и требовалось. \square

Перейдём к основной линии доказательства.

Лемма 42. *Для любого непротиворечивого множества Γ найдётся полное непротиворечивое множество $\Delta \supset \Gamma$.*

Доказательство. Докажем для конечного или счётного числа переменных p_1, p_2, p_3, \dots . Доказательство для произвольного множества переменных также возможно, но лишь с использованием леммы Цорна.

Будем рассматривать все переменные по очереди. Если уже верно $\Gamma \vdash p_i$ или $\Gamma \vdash \neg p_i$, то ничего менять не будем. Иначе добавим в Γ переменную p_i в качестве формулы. Таким образом, получим семейство $\Gamma_0 \subset \Gamma_1 \subset \Gamma_2 \subset \dots$, где $\Gamma_0 = \Gamma$, а далее

$$\Gamma_k = \begin{cases} \Gamma_{k-1}, & \text{если } \Gamma_{k-1} \vdash p_i \text{ или } \Gamma_{k-1} \vdash \neg p_i, \\ \Gamma_{k-1} \cup \{p_k\}, & \text{иначе.} \end{cases}$$

Положим $\Delta = \bigcup_{k=0}^{\infty} \Gamma_k$. Покажем, что Δ искомо. Сначала докажем по индукции, что все Γ_k непротиворечивы. Действительно, Γ_0 непротиворечиво по определению. Далее, множество Γ_{k+1} либо совпадает с Γ_k и потому непротиворечиво, либо равно $\Gamma_k \cup \{p_{k+1}\}$. Если оно противоречиво, то по правилу рассуждения от противного $\Gamma \vdash \neg p_{k+1}$, но в этом случае Γ_{k+1} совпало бы с Γ_k . Значит, Γ_{k+1} непротиворечиво и переход индукции доказан.

Теперь покажем, что и само Δ непротиворечиво. Действительно, если бы противоречие вывелось, то в выводе было бы задействовано конечное число формул, ведь сам вывод — конечная последовательность формул. Но тогда все эти формулы содержались бы уже в Γ_k при достаточно большом k . А тогда само Γ_k было бы противоречивым, но это не так, как мы уже убедились.

Полнота Δ получается из того, что для каждой переменной выводится либо она, либо её отрицание. Таким образом, Δ непротиворечиво и полное, что и требовалось. \square

Лемма 43. *Всякое полное непротиворечивое множество Δ совместно.*

Доказательство. Найдём выполняющий набор следующим образом: для каждой переменной p , если $\Delta \vdash p$, положим $p = 1$, а если $\Delta \vdash \neg p$, положим $p = 0$. Покажем, что он в самом деле выполняющий. Действительно, пусть $\varphi \in \Delta$, но $\varphi = 0$ на этом наборе. В таком случае по основной лемме $\Delta \vdash \neg \varphi$. Но тогда Δ противоречиво: оно содержит φ , и из него выводится $\neg \varphi$. Поскольку Δ непротиворечиво, формула φ должна быть истинной на построенном наборе, что и требовалось. \square

Итак, произвольное непротиворечивое множество Γ расширено до Δ , которое оказалось совместным. Значит, исходное Γ также было совместным, что и требовалось в теореме о полноте. \square

3.4 Теорема о полноте метода резолюций: из невыполнимой КНФ всегда можно вывести \perp .

Теорема. Метод резолюций всегда заканчивает свою работу, причём для невыполнимых КНФ выводится \perp (полнота), а для выполнимых не выводится (корректность).

Доказательство. 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.

Для полноты мы докажем обратное свойство: если \perp не выводится, то КНФ выполнима. Будем строить выполняющий набор рекурсивно, поддерживая следующий инвариант: после i -го шага значения $x_1 = a_1, \dots, x_i = a_i$ выбраны так, что истинны все

дизъюнкты, содержащие только переменные x_1, \dots, x_i . Отсутствие \perp даёт нам базу индукции: выполнены все дизъюнкты, не зависящие ни от каких переменных (т. к. таких дизъюнктов нет). Переход: пусть уже заданы значения $x_1 = a_1, \dots, x_i = a_i$. Рассмотрим все дизъюнкты, зависящие от x_{i+1} и, возможно, каких-то из переменных x_1, \dots, x_i , но не переменных x_{i+2}, \dots, x_n . Некоторые из них уже истинны благодаря выбору предыдущих значений. Исключим их из рассмотрения. Если в оставшиеся входит только литерал x_{i+1} , то положим $x_{i+1} = 1$, инвариант будет соблюлён. Если в оставшиеся входит только литерал $\neg x_{i+1}$, то положим $x_{i+1} = 0$, и инвариант тоже будет соблюлён. Осталось исключить случай, когда в какой-то дизъюнкт входит x_{i+1} , а в какой-то другой $\neg x_{i+1}$. Действительно, пусть такие дизъюнкты нашлись: $D_1 = (x_{i+1} \vee D'_1)$ и $D_0 = (\neg x_{i+1} \vee D'_0)$, где D'_1 и D'_0 зависят только от x_1, \dots, x_i . По предположению D'_0 и D'_1 должны быть ложны на значениях $x_1 = a_1, \dots, x_i = a_i$, иначе мы бы исключили D_0 или D_1 . Но резольвентой D_0 и D_1 будет дизъюнкт $(D'_0 \vee D'_1)$, который тоже должен быть ложен при $x_1 = a_1, \dots, x_i = a_i$. Но тогда предположение индукции нарушено. Значит, последний случай невозможен, и потому исходная формула выполнима. \square

3.5 Теорема о компактности для исчисления высказываний.

Теорема: Пусть любое конечное подмножество множества Γ совместно. Тогда и всё множество Γ совместно.

▲ Если всё множество Γ несовместно, то оно противоречиво. Но тогда в нём есть конечное противоречивое подмножество. Но тогда оно несовместно, что противоречит условию. ■

3.6 Устойчивость выразимых предикатов при автоморфизмах интерпретаций.

Пусть имеется некоторая сигнатура σ и интерпретация этой сигнатуры, носителем которой является множество M .

Определение: Взаимно однозначное отображение $\alpha : M \rightarrow M$ называется *автоморфизмом* интерпретации, если все функции и предикаты, входящие в интерпретацию, устойчивы относительно α . При этом k -местный предикат P называется *устойчивым* относительно α , если

$$P(\alpha(m_1), \dots, \alpha(m_k)) \Leftrightarrow P(m_1, \dots, m_k)$$

для любых элементов $m_1, \dots, m_k \in M$. Далее, k -местная функция f называется устойчивой относительно α , если

$$f(\alpha(m_1), \dots, \alpha(m_k)) = \alpha(f(m_1, \dots, m_k)).$$

Теорема: Любой предикат, выразимый в данной интерпретации, устойчив относительно её автоморфизмов.

▲ Пусть π — некоторая оценка, то есть отображение, ставящее в соответствие всем индивидуальным переменным некоторые элементы носителя. Через $\alpha \circ \pi$ обозначим оценку, которая получится, если к значению каждой переменной применить отображение α ; другими словами, $\alpha \circ \pi(\xi) = \alpha(\pi(\xi))$ для любой переменной ξ .

Первый шаг состоит в том, чтобы индукцией по построению терма t доказать такое утверждение: значение терма t при оценке $\alpha \circ \pi$ получается применением α к значению терма t при оценке π : $[t](\alpha \circ \pi) = \alpha([t](\pi))$.

Для переменных это очевидно, а шаг индукции использует устойчивость всех функций интерпретации относительно α . Теперь индукцией по построению формулы φ легко доказать такое утверждение: $[\varphi](\alpha \circ \pi) = [\varphi](\pi)$.

Мы не будем выписывать эту проверку; скажем лишь, что взаимная однозначность α используется, когда мы разбираем случай кванторов. (В самом деле, если с одной стороны изоморфизма берётся какой-то объект, то взаимная однозначность позволяет взять соответствующий ему объект с другой стороны изоморфизма.) ■

3.7 Теорема Гёделя о полноте исчисления предикатов: расширение любого непротиворечивого множества до полного и экзистенциально полного.

Определение: Множество Γ замкнутых формул в сигнатуре называется теорией.

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

Определение: Теория Γ называется совместной, если все формулы из Γ могут быть одновременно истинны в некоторой интерпретации.

Определение: Теория Γ называется противоречивой, если из нее выводится некоторая формула φ и ее отрицание $\neg\varphi$, и непротиворечивой в противном случае.

Теорема Гёделя о полноте исчисления предикатов: Если φ общезначима, то она выводима в исчислении предикатов. Пользуясь данной терминологией, можно сформулировать теорему, из которой будет следовать теорема Гёделя.

Теорема: Если теория непротиворечива, то она совместна (имеет модель).

Доказательство: 1. Мы хотим расширить не противоречивую Γ так, чтобы она была полной (если φ - замкнутая формула, то $\Gamma \vdash \varphi$ или $\Gamma \vdash \neg\varphi$) и экзистенциально полной (т.е. если $\Gamma \vdash \exists x\varphi$, то $\Gamma \vdash \varphi(t/x)$, где t - замкнутый терм).

Теория Γ в сигнатуре σ называется полной, если для любой замкнутой формулы ϕ этой же сигнатуры выполнено либо $\Gamma \vdash \phi$, либо $\Gamma \vdash \neg\phi$

Теорема о пополнении: Любую непротиворечивую теорию Γ можно расширить до полной непротиворечивой теории Δ .

Доказательство (для счётной сигнатуры). Пусть $\phi_1, \dots, \phi_n, \dots$ - нумерация всех замкнутых формул в сигнатуре σ . Будем строить рекурсивную цепочку: $\Gamma_0 = \Gamma$.

$$\Gamma_{i+1} = \begin{cases} \Gamma_i \cup \phi_{i+1}, & \text{если это непротиворечивая теория} \\ \Gamma_i \cup \neg\phi_{i+1}, & \text{иначе} \end{cases}$$

Если обе теории противоречивы, то и Γ_i противоречиво - доказывается аналогично ИВ

$$\Delta = \bigcup_{i=0}^{\infty} \Gamma_i$$

Проблема с нехваткой констант: может быть так, что $\Gamma \vdash \exists x \phi$, но неверно $\Gamma \vdash \phi(t/x)$ ни для какого замкнутого терма t . Тогда получится, что $\phi(t/x)$ не будет верна в модели из замкнутых термов, а тогда и формула $\exists x \phi$ не будет там верна.

Вводится дополнительное требование: теория Γ называется экзистенциально полной в сигнатуре σ , если для любой формулы ϕ , такой что $\Gamma \vdash \exists x \phi$, также $\Gamma \vdash \phi(t/x)$ для какого-то замкнутого терма t

Теорема: любую пару (Γ, σ) , т.ч. теория Γ непротиворечива в сигнатуре σ , можно расширить до пары (Δ, τ) , т.ч. теория Δ непротиворечива и экзистенциально полна в сигнатуре τ

Доказательство: вновь рассмотрим подряд все формулы с 1 параметром $\phi_1, \dots, \phi_n, \dots$. Положим $\Gamma_0 = \Gamma$, $\sigma_0 = \sigma$

Если $\Gamma_i \vdash \exists x \phi_{i+1}$, то $\sigma_{i+1} = \sigma_i \cup \{c_{\phi_{i+1}}\}$, $\Gamma_{i+1} = \Gamma_i \cup \{\phi_{i+1}(c_{\phi_{i+1}}/x)\}$

Нужно доказать, что при такой процедуре не пропадёт непротиворечивость

Пусть Γ_{i+1} противоречива. Тогда $\Gamma_i \vdash \neg\phi_{i+1}(c_{\phi_{i+1}}/x)$

Но если в выводе противоречия заменить $c_{\phi_{i+1}}$ на "свежую" переменную z (т.е. не участвовавшую в выводе), то вывод останется корректным.

Т.е. $\Gamma_i \vdash \neg\phi_{i+1}(z/x)$. Отсюда по правилу обобщения $\Gamma_i \vdash \forall z \neg\phi_{i+1}(z/x)$

Поэтому (упр. - проверить детали) $\Gamma_i \vdash \forall x \neg\phi_{i+1}(x)$

С другой стороны, $\Gamma_i \vdash \exists x \phi_{i+1}$, поэтому само Γ_i противоречиво

Теперь $\Delta = \bigcup \Gamma_i$, $\tau = \bigcup \sigma_i$

Δ также будет непротиворечивым, т.к. противоречие выводится из конечного множества формул

<p>Проблема : при пополнении может утратиться экзистенциальная полнота. В теорию добавляются новые формулы, становятся выводимыми новые формулы вида $\exists x \phi$, для некоторых из них может нарушаться условие</p> <p>С другой стороны, при экзистенциальном пополнении может утратиться полнота. В сигнатуре появляются новые символы, условие полноты распространяется на новые формулы, для которых может быть неверным.</p> <p>Чтобы решить эту проблему, нужно сделать счётное число раундов пополнения и экзистенциального пополнения, и объединить все получившиеся теории и сигнатуры.</p> <p>Результат будет непротиворечивым, полным и экзистенциально полным.</p> <p>Непротиворечивость : как обычно, противоречие выводится из конечного числа формул, на каком – то конечном этапе все они уже добавлены.</p> <p>Полнота : пусть дана формула в объединённой сигнатуре. Формула зависит от конечного числа символов, на каком – то этапе они все уже добавлены в сигнатуру. На следующем раунде пополнения эта формула будет рассмотрена.</p> <p>Экзистенциальная полнота : пусть дана формула вида $\exists x \phi$, выводимая из объединённой теории. В выводе используется конечное число формул, все они уже лежат в теории на каком-то этапе. На следующем раунде экзистенциального пополнения будет добавлена нужная константа.</p>	
<p>Идея доказательства теоремы о полноте : если в сигнатуре есть константные символы, то в языке есть замкнутые термы, т.е. термы, не зависящие от переменных. Им должны соответствовать какие-то элементы носителя модели. Самое простое – все эти элементы будут разными, функции будут определяться тривиальным образом, т.е. функция f из термов t_1, \dots, t_k делает терм $f(t_1, \dots, t_k)$.</p> <p>Проблема с этим планом : константных символов может и вообще не быть, или быть недостаточно для того, чтобы все формулы из теории были выполнены</p> <p>Другая проблема : а как, собственно, определять предикаты?</p> <p>Идея решения : чтобы избавиться от первой проблемы, добавляем новые константные символы, а для решения второй проблемы пополняем теорию, чтобы любая замкнутая формула была доказуема или опровержима, что позволит определить значения предикатов на замкнутых термах</p> <p>(Предикат от замкнутых термов является замкнутой формулой и потому подпадает под условие.</p> <p>Решение одной проблемы усугубляет другую, и наоборот, поэтому нужно сделать счётное число исправлений</p>	

Лемма 9. Любую непротиворечивую теорию можно расширить до непротиворечивой, полной и экзистенциально полной теории.

Доказательство было приведено выше.

3.8 Теорема Гёделя о полноте исчисления предикатов: построение модели из замкнутых термов у любого непротиворечивого, полного и экзистенциально полного множества.

Лемма 10.

Любая непротиворечивая, полная, экзистенциально полная теория совместна, то есть имеет модель.

<p>Последняя лемма : любая полная, непротиворечивая и экзистенциально полная теория Γ имеет модель из замкнутых термов.</p> <p>Носитель – все замкнутые термы</p> $[f](t_1, \dots, t_k) = f(t_1, \dots, t_k)$ $[P](t_1, \dots, t_k) = \begin{cases} 1, & \text{если } \Gamma \vdash P(t_1, \dots, t_k) \\ 0, & \text{иначе} \end{cases}$ <p>Нужно доказать, что если $\Gamma \vdash \phi$, то ϕ истинно в этой модели</p> <p>Можно считать, что ϕ замкнуто (иначе напомним \forall по правилу обобщения)</p> <p>Для замкнутых в силу полноты Γ будем доказывать следующее:</p> <p>Если $\Gamma \vdash \phi$, то ϕ истинна в модели, а если $\Gamma \vdash \neg \phi$, то ϕ ложна в модели</p> <p>Индукция по логической глубине формулы.</p> <p>Если ϕ атомарная, то по определению $[P]$</p> <p>Если $\phi = \neg \psi$, то для ψ всё доказано, для ϕ тоже получается.</p> <p>Если $\phi = (\psi \wedge \xi)$ или для другой связки, то из утверждений для ψ и ξ всё выводится</p> <p>Если $\phi = \exists x \psi$, то по экзистенциальной полноте $\Gamma \vdash \psi(t/x)$, это более простая формула, поэтому $\psi(t/x)$ истинна в модели, поэтому $\exists x \psi$ тоже истинна в модели</p> <p>С другой стороны, если $\exists x \psi$ истинна в модели, то $\psi(t/x)$ истинна в модели, по предположению индукции $\Gamma \vdash \psi(t/x)$, поэтому $\Gamma \vdash \exists x \psi$</p> <p>$\forall x \psi$ можно заменить на $\neg \exists x \neg \psi$ как с точки зрения выводимости, так и с точки зрения истинности</p> <p>Все формулы исходного Γ_0 будут лежать в Γ и потому быть выводимыми, так что мы построили действительно модель исходной теории</p>	
---	--

3.9 Представимость конечных последовательностей в арифметике при помощи β -функции Гёделя.

Лемма 1:

$\forall n \quad \forall c \quad \exists b > c$ такое, что $b + 1, 2b + 1, \dots, nb + 1$ - взаимно просты.

Рассмотрим $b = n!$.

Тогда возьмем произвольные различные k и m от 1 до n . $\gcd(kb + 1, mb + 1) = d > 1 \Rightarrow (k - m)b$ делится на d .

Значит т.к. $b = n!$ и $k - m < n$, получаем, что любой простой делитель числа $(k - m)b$ должен быть строго меньше n .

$\forall d$ есть простой делитель $p < n$.

$mb + 1$ делится на p .

$mb + 1 - m \cdot n!$ делится на $p \Rightarrow d = 1$

Лемма 2.

$\forall (x_1, \dots, x_n) \quad \exists a, b \quad \forall i : a \equiv x_i \pmod{b_i + 1}$

Док-во:

Выберем по Лемме 1 $b > \max\{x_i\}$.

Тогда нужное a найдётся по китайской теореме об остатках: Если натуральные числа a_1, \dots, a_n попарно взаимно просты, то для любых r_1, \dots, r_n таких, что $0 \leq r_i < a_i$ при всех $i : 0, \dots, n$ найдется число, которое при делении на a_i дает остаток r_i при всех i . Более того, если найдутся два таких числа, то они будут сравнимы по модулю $a_1 \cdot \dots \cdot a_n$.

Положим $\beta(a, b, i) = a \pmod{bi + 1}$

β арифметична: $r = x \pmod{q} \Leftrightarrow r < q$ и $\exists s : x = sq + r$.

3.10 Арифметичность предикатов « n — степень шестёрки» и $n = 2^k$.

Определение: Предикат $P : \mathbb{N}^k \rightarrow \{0, 1\}$ называется *арифметичным*, если он выразим в стандартной интерпретации арифметики $\langle \mathbb{N}, +, \cdot, = \rangle$. Функция $f : \mathbb{N}^k \rightarrow \mathbb{N}$ называется *арифметичной*, если арифметичен предикат $P_f : \mathbb{N}^{k+1} \rightarrow \{0, 1\}$, где $P_f(x, y) = 1 \Leftrightarrow f(x) = y$.

Степень шестерки

Степень шестерки можно выразить с использованием квантора по конечному множеству

$$\exists D(x \in D \wedge \forall y \in D(y = 1 \vee (y : 6 \wedge \frac{y}{6} \in D)))$$

У нас есть $x, \frac{x}{6}, \frac{x}{36}, \frac{x}{216}, \dots, 1$. Этакый мешок с числами. И если в нем есть x , то есть и $\frac{x}{6}$ и т.д., а остановиться это все может только на единице. Соответственно, если x - не степень шестерки, то возникнет не единица, и оба условия будут нарушены.

Через обычные предикаты эта функция выражается с помощью кодирования Смаллиана. Оно лучше применимо для описания конечных множеств. В чем суть:

Берем и вводим предикат $S(a, b, x)$, которые отвечает следующим свойствам:

1 $\forall a, b \{x : S(a, b, x) = 1\}$ - конечно

2 Для любого конечного S найдутся такие a и b , что $S = \{x : S(a, b, x) = 1\}$

Теперь записанную нами формулу $\exists D \dots x \in D \dots$ можно переписать следующим образом:

$$\exists a, \exists b (S(a, b, x) \wedge \forall y (S(a, b, y) \rightarrow (y = 1 \vee (y : 6 \wedge \exists z (y = 6 \cdot z \wedge S(a, b, z))))))$$

Что поменялось? Заменяли $\exists D$ на $\exists a, \exists b$. И $x \in D$ на $S(a, b, x)$, получили формулу первого порядка

Степень двойки

$x = 2^k$ можно выразить с использованием квантора по конечной последовательности

$$\exists \{a_i\} (a_0 = 1 \wedge a_k = x \wedge \forall i \in [0; k-1] a_{i+1} = a \cdot a_i)$$

Через обычные предикаты это выражается с использованием β -функции Гёделя.

Тут вводится арифметическая функция $\beta(a, b, i)$ со следующим свойством:

$$\forall [x_0, \dots, x_n] \text{ найдутся такие } a, b, \text{ что } \forall i \in [0, n] x_i = \beta(a, b, i)$$

Теперь в формуле, которая имеет вид $\exists \{x_i\} \dots x_j \dots$ можно заменить на такую:
 $\exists a \exists b \dots \beta(a, b, j) \dots$

Применим полученные знания к нашему предикату и получим:

$$x = 2^k \iff \exists a, b (\beta(a, b, 0) = 1 \wedge \beta(a, b, k) = x \wedge \forall i \in [0, \dots, k-1] \beta(a, b, i+1) = 2 \cdot \beta(a, b, i))$$

3.11 Множество замкнутых формул, истинных в \mathbb{N} , неперечислимо. Первая теорема Гёделя о неполноте.

Опр Множество $A \subset \mathbb{N}^k$ называется *арифметическим*, если существует арифметическая формула α с параметрами x_1, \dots, x_k , которая его представляет в следующем смысле: $\langle n_1, \dots, n_k \rangle$ принадлежит множеству A тогда и только тогда, когда формула α истинна при значениях параметров $x_1 = n_1, \dots, x_k = n_k$.

Любое перечислимое множество арифметично

Лемма1

Всякое арифметическое множество лежит в классе Σ_n или Π_n для некоторого n (и, естественно, для всех больших n).

▲ Формулу, задающую арифметическое множество, приведём к предварённой нормальной форме (вынеся кванторы наружу). Ясно, что бескванторная часть задаёт разрешимое множество, поэтому исходное множество принадлежит какому-то из классов Σ_n или Π_n . Можно и не использовать предварённой нормальной формы, а применить индукцию по длине формулы и сослаться на то, что пересечение, объединение и дополнение, а также проекция не выводят за пределы арифметической иерархии (объединения всех классов Σ_n и Π_n). ■

Рассмотрим теперь множество T , элементами которого являются все истинные арифметические формулы без параметров (точнее, их номера в какой-то вычислимой нумерации всех формул — это значит, что по формуле можно алгоритмически получить её номер и наоборот).

Лемма2

Любое арифметическое множество m -сводится к множеству T .

▲ Пусть A — произвольное арифметическое множество. Пусть $\alpha(x)$ — формула с одной переменной, которая выражает принадлежность множеству A . Это означает, что $\alpha(n)$ истинно при тех и только тех n , которые принадлежат A . Тогда вычислимая функция $n \rightarrow$ (номер формулы, которая является результатом подстановки константы n в $\alpha(x)$) m -сводит A к T . ■

Первая теорема Гёделя о неполноте

Множество T арифметических истин неперечислимо.

▲ Это следует из того, что если бы T было перечислимо, оно было бы арифметично, что противоречит теореме Тарского ■

Множество замкнутых формул, истинных в N , неперечислимо

Если множество перечислимо, то оно лежит в арифметической иерархии, что противоречит теореме Тарского

3.12 Теорема Тарского.**Теорема Тарского**

Истинность арифметической формулы нельзя выразить арифметическим выражением. То есть не существует формулы $\text{True}(x)$, которая истинна тогда и только тогда, когда формула с номером x истинна. (Множество T не арифметично.)

▲ Если бы T было арифметическим, то оно лежало бы в некотором конкретном классе. Поскольку всякое арифметическое множество сводится к T , то все арифметические множества лежали бы в этом классе. Но мы знаем, что множества из более высоких классов иерархии тоже арифметичны, но в Σ_n не лежат. ■

Теория множеств.

4 Определения

4.1 Множество, основные теоретико-множественные операции, упорядоченная пара, декартово произведение.

1. *Множеством* называется произвольный набор (совокупность, класс, семейство) каких-либо объектов. Объекты, входящие во множество, называются его *элементами*. Если объект x является элементом множества A , то говорят, что x принадлежит A , и пишут $x \in A$.
2. Множество A является *подмножеством* множества B , если любой элемент множества A также принадлежит множеству B . Обозначение: $A \subset B$.
3. Множества A и B *равны*, если одновременно $A \subset B$ и $B \subset A$. Обозначение: $A = B$.
4. Для задания *упорядоченной пары* нужно задать неупорядоченную и первый элемент в ней. Например, по упрощённому определению Куратовского: $(a, b) = \{a, \{a, b\}\}$.
5. *Кортежем* длины 0 называется пустое множество. Если уже задан $T = (a_1, \dots, a_n)$ – кортеж длины n , то $(a, a_1, \dots, a_n) = \{a, \{a, T\}\}$ есть кортеж длины $n + 1$. Так можно получить ещё одно определение упорядоченной пары: $(a, b) = \{a, \{a, \{b, \emptyset\}\}\}$.
6. *Декартовым произведением* множеств A и B называется множество упорядоченных пар $A \times B = \{(a, b) \mid a \in A, b \in B\}$. *Декартовой степенью* A^n множества A называется множество кортежей длины n из элементов A .
 - ▷ *Объединением* A и B называется множество $A \cup B = \{x \mid x \in A \text{ или } x \in B\}$.
 - ▷ *Пересечением* A и B называется множество $A \cap B = \{x \mid x \in A \text{ и } x \in B\}$.
 - ▷ *Разностью* A и B называется множество $A \setminus B = \{x \mid x \in A \text{ и } x \notin B\}$.
 - ▷ *Симметрической разностью* A и B называется множество $A \triangle B = (A \setminus B) \cup (B \setminus A)$.
 - ▷ *Дополнением* множества A называется множество $A = \{x \mid x \notin A\}$.

4.2 Отображения и соответствия. Образ и прообраз. Инъекции, сюръекции, биекции. Композиция отображений. Возведение множества в степень множества.

1. *Соответствием* между множествами A и B называют произвольное подмножество декартова произведения $F \subset A \times B$.
2. *Отображением* из множества A в множество B называется однозначное соответствие между A и B , т. е. такое соответствие, что для любого $a \in A$ найдётся ровно одно $b \in B$, соответствующее a .
3. Соответствие F называется *инъективным*, если для любых $a_1 \neq a_2$ множества $F(a_1)$ и $F(a_2)$ не пересекаются. Инъективное отображение называется *инъекцией*.

4. Соответствие F называется *сюръективным*, если любой элемент B соответствует хотя бы одному элементу A , т. е. любой $b \in B$ лежит в $F(a)$ для некоторого $a \in A$. Сюръективное отображение называется *сюръекцией*.
5. *Биекцией* называется отображение, являющееся одновременно инъекцией и сюръекцией.
6. Пусть $F : A \rightarrow B$ – соответствие, а $S \subset A$. *Образ* S – это множество $F(S) = \bigcup_{s \in S} F(s) \subset B$.
7. Пусть $F : A \rightarrow B$ – соответствие, а $T \subset B$. *Прообраз* T – это множество $F^{-1}(T) = \{a \mid F(a) \cap T \neq \emptyset\} \subset A$.
8. Пусть $F : A \rightarrow B$ и $G : B \rightarrow C$ – соответствия. Тогда их *композицией* $G \circ F$ называется соответствие $H : A \rightarrow C$, определенное правилом: $c \in H(a)$ тогда и только тогда, когда найдется b , такое что одновременно $c \in G(b)$ и $b \in F(a)$.
9. Пусть A и B – два множества. Тогда множеством B^A называется множество всех отображений из A в B .

4.3 Равномощность. Счётные и континуальные множества.

1. Множества A и B называются *равномощными*, если существует биекция $A \rightarrow B$. Обозначение: $A \cong B$.
2. Множество A называется *счётным*, если оно равномощно множеству \mathbb{N} .
3. Множество A называется *континуальным*, если оно равномощно множеству \mathbb{R} .

4.4 Бинарные отношения. Рефлексивность, транзитивность, (анти)симметричность и т. д. Отношения эквивалентности и отношения порядка.

Определение: *Бинарным отношением* на множестве A называется любое подмножество $R \subset A \times A$.

Классификация отношений:

1. рефлексивные $\forall x \, xRx$ $(= \leq \vdots \subset \cong)$
 2. антирефлексивные $\forall x \, \neg(xRx)$ $(<)$
 3. симметричные $\forall x, y \, xRy \rightarrow yRx$ $(= \cong \text{ mod } \parallel)$
 4. антисимметричные $\forall x, y \, (xRy \wedge yRx) \rightarrow (x = y)$ $(< \leq \vdots \subset)$
 5. транзитивные $\forall x, y, z \, (xRy \wedge yRz) \rightarrow xRz$ $(= < \vdots \subset \cong)$
 6. антитранзитивные $\forall x, y, z \, (xRy \wedge yRz) \rightarrow \neg(xRz)$ $(\perp \text{ на плоскости})$
 7. евклидово (правое) $\forall x, y, z \, (xRy \wedge xRz) \rightarrow yRz$ $(\text{нетранзитивное } R = \{(1,2), (2,2), (2,3), (3,2), (3,3)\})$
- отношение эквивалентности: *рефлексив.* + *симметрич.* + *транзитив.*
 - отношение нестрогого (частичного) порядка: *рефлексив.* + *антисимметрич.* + *транзитив.*
 - отношение строгого (частичного) порядка: *антирефлексив.* + *антисимметрич.* + *транзитив.*
 - отношение (нестрогого) предпорядка: *рефлексив.* + *транзитив.*

4.5 Упорядоченное множество, линейно упорядоченное множество, фундированное множество, вполне упорядоченное множество.

Определение: Упорядоченным множеством называется пара (A, \leq_A) – множество и отношение порядка на нем.

Определение: Частично упорядоченное множество называется *линейно упорядоченным*, если любые два элемента в нем сравнимы.

Определение: Частично упорядоченное называется *фундированным*, если в любом его непустом подмножестве есть минимальный элемент.

Пример

✓ $\langle \mathbb{N}, \leq \rangle$, $\langle \mathbb{N} + \mathbb{N}, \leq \rangle$, $\langle \mathbb{N}, | \rangle$ с заданным тривиально порядком – фундированные.

× \mathbb{Z} , $[0, 1]$ – не фундированные.

Определение: Фундированное линейно упорядоченное множество называется *вполне упорядоченным*, а соответствующий порядок – полным.

Пример

× Множество всех конечных слов из букв латинского алфавита.

× $[0, 1]$, $\langle \mathbb{N}, | \rangle$.

✓ \mathbb{N} .

4.6 Цепи в упорядоченных множествах. Верхние и нижние грани, максимальные и минимальные, наибольшие и наименьшие элементы.

Определение: Подмножество частично упорядоченного множества называется *цепью*, если любые два его элемента сравнимы.

Определение: Элемент $a \in M$ называется *минимальным*, если $b \leq a$ только при $b = a$. Элемент $a \in M$ называется *наименьшим*, если $\forall b \in M : a \leq b$. Аналогично вводятся понятия *максимального* и *наибольшего* элементов.

Определение: *Верхней гранью* множества A называется такой элемент M , что $\forall x \in A : x \leq M$.

Определение: *Нижней гранью* множества A называется такой элемент m , что $\forall x \in A : x \geq m$.

4.7 Гомоморфизмы и изоморфизмы упорядоченных множеств.

Определение: Гомоморфизмом упорядоченных множеств называется функция $f : A \rightarrow B$, такая что

$$x \leq_A y \Leftrightarrow f(x) \leq_B f(y).$$

Определение: Изоморфизмом упорядоченных множеств называется функция $f : A \rightarrow B$, являющаяся гомоморфизмом и биекцией.

4.8 Сложение и умножение упорядоченных множеств.

$\langle A, \leq_A \rangle + \langle B, \leq_B \rangle = \langle C, \leq_C \rangle$, где $C = A \sqcup B$, $x \leq_C y$, если <div style="display: inline-block; vertical-align: middle; border-left: 1px solid black; padding-left: 5px;"> $\begin{cases} x, y \in A, x \leq_A y \\ x, y \in B, x \leq_B y \\ x \in A, y \in B \end{cases}$ </div>
$\langle A, \leq_A \rangle \cdot \langle B, \leq_B \rangle = \langle C, \leq_C \rangle$, где $C = A \times B$, $(x_1, y_1) \leq_C (x_2, y_2)$, если <div style="display: inline-block; vertical-align: middle; border-left: 1px solid black; padding-left: 5px;"> $\begin{cases} y_1 \leq_B y_2 \\ y_1 = y_2, x_1 \leq_A x_2 \end{cases}$ </div>

4.9 Начальные отрезки вполне упорядоченных множеств.

Определение: Пусть S – ВУМ. Подмножество $A \subset S$ называется *начальным отрезком*, если $\forall x \forall y ((x \leq y \wedge y \in A) \rightarrow x \in A)$.

Примеры

$$\checkmark [0, a] = \{x \mid x \leq a\}.$$

$$\checkmark [0, a) = \{x \mid x < a\}.$$

$$\checkmark \text{Всё } S.$$

4.10 Предельные элементы вполне упорядоченных множеств.

Определение: В любом ВУМ у любого элемента a , кроме максимального, есть единственный непосредственно следующий за ним (элемент $a + 1$), т.е. такой $c > a$, что не существует такого b , что $a < b < c$.

Определение: *Предельным элементом* ВУМ называется элемент, не являющийся непосредственно следующим ни для какого другого элемента.

4.11 Порядковые типы $\omega, \omega^k, \omega^\omega, \varepsilon_0$.

Определение: Неформально *ординалом* (порядковым числом или порядковым типом) называется класс эквивалентности вполне упорядоченных множеств по отношению изоморфности. Формально ординалом называется транзитивное множество, каждый элемент которого также транзитивен.

Будем обозначать 0 – порядковый тип пустого множества, 1 – порядковый тип множества из одного элемента, k – порядковый тип линейного порядка на k -элементном множестве (такие ординалы называются конечными), ω – порядковый тип множества натуральных чисел \mathbb{N} со стандартным порядком.

Рассмотрим порядковый тип ω . Следующим за ним будет $\omega + 1$, потом $\omega + 2, \dots, \omega + \omega = \omega \cdot 2, \omega \cdot 2 + 1, \dots, \omega \cdot 3, \dots, \omega \cdot \omega = \omega^2$. Далее идут $\omega^2 + 1, \dots, \omega^2 + \omega, \dots, \omega^2 \cdot 2, \dots, \omega^3, \dots, \omega^\omega, \dots, \omega^{\omega+1}, \dots, \omega^{\omega^\omega}, \dots, \varepsilon_0 = \omega^{\omega^{\omega^{\dots}}}$ (ω раз).

ε_0 – минимальный ординал, такой что $\varepsilon_0 = \omega^{\varepsilon_0}$.

4.12 Аксиома выбора.

Пусть задано некоторое множество A . Тогда существует функция $\varphi : 2^A \setminus \{A\} \rightarrow A$ такая, что $\forall S \subset A : \varphi(S) \in S$.

4.13 Базис Гамеля.

Базис Гамеля в \mathbb{R} над \mathbb{Q} это такой набор действительных чисел, что любое другое действительное число представляется как конечная линейная комбинация элементов базиса с рациональными коэффициентами, при этом никакая нетривиальная конечная линейная комбинация элементов базиса с рациональными коэффициентами не равна 0 .

5 Простые утверждения

5.1 Основные тождества про теоретико-множественные операции, декартово произведение, возведение множества в степень множества.

Утверждение 10. Для операций над множествами выполнены следующие тождества:

- а) Коммутативность: $A \cup B = B \cup A$, $A \cap B = B \cap A$, $A \Delta B = B \Delta A$;
- б) Ассоциативность: $(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$, $(A \Delta B) \Delta C = A \Delta (B \Delta C)$;
- в) Дистрибутивность: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
- г) Идемпотентность: $A \cup A = A$, $A \cap A = A$;
- д) Аннигиляция: $A \setminus A = A \Delta A = \emptyset$;
- е) Законы де Моргана: $\overline{(A \cup B)} = \bar{A} \cap \bar{B}$, $\overline{(A \cap B)} = \bar{A} \cup \bar{B}$.

Доказательство. Каждое из тождеств можно доказывать при помощи кругов Эйлера

Определение: Множества A и B эквивалентны, если для каждого элемента A есть элемент B , задающий тот же кортеж, и наоборот. Будем обозначать такую эквивалентность как $A \sim B$.

Свойства:

1. $A^n \sim A \times A \times \dots \times A$ – по определению.
2. $(A \times B) \times C \sim A \times (B \times C)$:
 $A \times B = \{(a, b) : a \in A, b \in B\}$;
 $(A \times B) \times C = \{((a, b), c) : a \in A, b \in B, c \in C\} \sim \{(a, (b, c)) : a \in A, b \in B, c \in C\} = A \times (B \times C)$.
3. $A \times \{\emptyset\} \sim A$.
4. $A^{n+k} \sim \underbrace{(A \times A \times \dots \times A)}_n \underbrace{(A \times A \times \dots \times A)}_k \sim \underbrace{A \times A \times \dots \times A}_{n+k} \sim A^n \times A^k$.
5. $(A^n)^m \sim A^{nm}$.

Свойства:

1. $(A \times B)^C \sim A^C \times B^C$.
2. $A^{B \cup C} \sim A^B \times A^C$, если B и C не пересекаются.
3. $(A^B)^C \sim A^{B \times C}$.

Доказательство:

1. Пусть $F \in (A \times B)^C$. Это значит, что $F : C \rightarrow A \times B$. То есть каждому элементу $c \in C$ сопоставлена некоторая пара $(a, b) \in A \times B$. Вместо этого ему можно сопоставить отдельно элементы $a \in A$ и $b \in B$. Получится два отображения, первое отображает c в a , а второе – c в b , то есть пара отображений $(F_1, F_2) \in A^C \times B^C$.
2. Вторая эквивалентность означает, что определить функцию на несвязном объединении двух множеств это то же самое, что определить её на каждом из этих множеств по отдельности.
3. Третья эквивалентность означает, что функция двух аргументов есть то же самое, что отображение первого аргумента в функцию, зависящую от второго аргумента.

5.2 Равномощность — отношение эквивалентности.

Утверждение 7. При всех A, B и C выполнены утверждения:

- а) $A \cong A$ (рефлексивность \cong);
- б) Если $A \cong B$, то $B \cong A$ (симметричность \cong);
- в) Если $A \cong B$ и $B \cong C$, то $A \cong C$ (транзитивность \cong).

Доказательство. В первом пункте в качестве биекции нужно взять id_A , во втором — обратную биекцию, в третьем — композицию биекций. \square

5.3 Объединение и декартово произведение счётных множеств счётны.

Утверждение: Пусть A — счётное множество, а $b \notin A$. Тогда $A \cup \{b\}$ тоже счётно.

Доказательство: Формально, пусть $\alpha : \mathbb{N} \rightarrow A$ — биекция. Тогда определим биекцию $\beta : \mathbb{N} \rightarrow (A \cup \{b\})$ так: $\beta(0) = b$ и $\beta(n) = \alpha(n-1)$ для $n > 0$.

Утверждение: Если A счётно, а B конечно, то $A \cup B$ тоже счётно.

Утверждение: Если A и B суть счётные множества, то $A \cup B$ тоже счётно.

Доказательство: Ясно, что $A \cup B = A \cup (B \setminus A)$. Если множество $B \setminus A$ конечно, то утверждение следует из предыдущего. Иначе $B \setminus A$ счётно.

Таким образом, утверждение достаточно доказать для непересекающихся A и B . В этом случае пусть $\alpha : \mathbb{N} \rightarrow A$ и $\beta : \mathbb{N} \rightarrow B$ суть биекции. Тогда построим биекцию $\gamma : \mathbb{N} \rightarrow A \cup B$ по правилу: $\gamma(2k) = \alpha(k)$, а $\gamma(2k+1) = \beta(k)$.

Утверждение: Декартово произведение двух счётных множеств $A \times B$ счётно.

Доказательство: В самом деле, по определению декартово произведение есть множество всех упорядоченных пар вида $\langle a, b \rangle$, в которых $a \in A$ и $b \in B$. Разделим пары на группы, объединив пары с одинаковой первой компонентой (каждая группа имеет вид $\{a\} \times B$ для какого-то $a \in A$). Тогда каждая группа счётна, поскольку находится во взаимно однозначном соответствии с B (пара определяется своим вторым элементом), и групп столько же, сколько элементов в A , то есть счётное число.

5.4 В любом бесконечном множестве найдётся счётное подмножество.

Так как A бесконечно, в нем существует элемент a_0 , причем $A \setminus a_0$ также бесконечно. Значит, в нем найдется a_1 . Продолжая набирать элементы, получим множество $A_1 = \{a_0, a_1, \dots\}$, $A_1 \subset A$.

5.5 Несчётность множества точек на отрезке.

Ясно, что любые два отрезка равномощны, так что рассмотрим отрезок $[0, 1]$. Докажем несчётность интервала $(0, 1)$, из чего будет несчётность отрезка.

Рассмотрим биекцию $f(x) = \text{tg}(\pi(x - \frac{1}{2}))$.

5.6 Нефундированность прямого лексикографического порядка на конечных словах.

Нефундированность следует из существования бесконечно убывающей цепочки. Например, можно рассмотреть последовательность: $b > ab > aab > \dots$

5.7 Любой начальный отрезок вполне упорядоченного множества, отличный от всего множества, представляется в виде $[0, a)$.

Теорема: Если S — ВУМ, A — начальный отрезок S , $A \neq S$, то $A = [0, a)$.

Доказательство. Рассмотрим $\bar{A} = S \setminus A$. Так как $\bar{A} \neq \emptyset$, то по свойству фундированности $\exists y = \min \bar{A}$, тогда покажем, что $A = [0, y)$. $[0, y) \subset A$, так как если $x \in [0, y)$ и $x \notin A$, то $x < y$ и $x \in \bar{A} \Rightarrow y \neq \min \bar{A}$, противоречие. $A \subset [0, y)$, так как если $x \in A$ и $x \notin [0, y)$, то (поскольку это ЛУМ) $x \geq y \Rightarrow$ (по определению начального отрезка) получаем, что $y \in A$ противоречие. \square

5.8 Вполне упорядоченное множество неизоморфно своему начальному отрезку вида $[0, a)$ (вывод из леммы о монотонной функции).

Теорема : вполне упорядоченное множество не может быть изоморфно своему собственному начальному отрезку

Доказательство. Пусть изоморфно. Тогда $f : A \rightarrow [0, a)$ — изоморфизм.

Он сохраняет порядок, поэтому если $x < y$, то $f(x) < f(y)$.

По теореме о монотонной функции получаем $f(x) \geq x$. В частности, $f(a) \geq a$, с другой стороны, $f(a) \in [0, a)$, поэтому $f(a) < a$, противоречие.

5.9 Сумма и произведение фундированных множеств фундированы, вполне упорядоченных — вполне упорядочены.

Сложение упорядоченных множеств:

$$\langle A, \leq_A \rangle + \langle B, \leq_B \rangle = \langle C, \leq_C \rangle$$

$$C = A \sqcup B$$

$$x \leq_C y, \text{ если } \begin{cases} x, y \in A, x \leq_A y \\ x, y \in B, x \leq_B y \\ x \in A, y \in B \end{cases}$$

Теорема : сумма фундированных множеств фундирована, сумма вполне упорядоченных вполне упорядочена

Доказательство через Φ : пусть $S \subset C$. Если $S \cap A \neq \emptyset$, то есть $\min(S \cap A)$ с точки зрения \leq_A . Он же будет $\min S$ с точки зрения \leq_C

Если же $S \cap A = \emptyset$, то $S = S \cap B$, есть $\min(S \cap B)$ с точки зрения \leq_B . Он же будет $\min S$ с точки зрения \leq_C

Умножение упорядоченных множеств

$$\langle A, \leq_A \rangle \cdot \langle B, \leq_B \rangle = \langle C, \leq_C \rangle$$

$$C = A \times B$$

$$(a_1, b_1) \leq_C (a_2, b_2), \text{ если } \begin{cases} b_1 <_B b_2 \\ b_1 = b_2, a_1 \leq_A a_2 \end{cases}$$

Теорема : произведение фундированных множеств фундировано, произведение вполне упорядоченных вполне упорядочено

Доказательство через БС' : пусть $(a_0, b_0) \geq_C (a_1, b_1) \geq_C (a_2, b_2) \geq_C \dots$

Тогда $b_0 \geq_B b_1 \geq_B b_2 \geq_B b_3 \dots$. По БС' для B получаем $\exists N \forall n > N b_n = b_N$. В частности $\forall n > N b_n = b_{n+1}$.

Значит, $\forall n > N a_n \geq_A a_{n+1}$. Получаем нестрогую убывающую последовательность в A , по БС' получаем $\exists M \forall m > M a_m = a_M$. Т.е. $\forall m > M (a_m, b_m) = (a_M, b_M)$. Т.е. верна БС' для C .

5.10 Свойства сложения и умножения вполне упорядоченных множеств: ассоциативность, некоммутативность, (не)дистрибутивность, (не)монотонность.

Верны ассоциативность и правая дистрибутивность: $A \cdot (B + C) \simeq A \cdot B + A \cdot C$. Коммутативность и левая дистрибутивность неверны: $1 + \omega = \omega \neq \omega + 1$, $2 \cdot \omega = \omega \neq \omega \cdot 2$, $(1 + 1) \cdot \omega = \omega \neq 1 \cdot \omega + 1 \cdot \omega$.

Условие монотонности звучит так: если $A < B$ ($A \lesssim B$), то верно ли, что для всех C истинно $A + C < B + C$, $C + A < C + B$, $A \cdot C < B \cdot C$, $C \cdot A < C \cdot B$ (то же для \lesssim вместо $<$)?

При $A < B$ верно $C + A < C + B$, $A + C \lesssim B + C$, $C \cdot A < C \cdot B$ (при непустом C), $A \cdot C \lesssim B \cdot C$. При $A \lesssim B$ все неравенства верны с \lesssim .

5.11 Сравнимость любых двух множеств по мощности (вывод из теоремы Цермело и свойств вполне упорядоченных множеств).

Теорема о сравнимости вполне упорядоченных множеств.

Пусть A и B — вполне упорядоченные множества. Тогда одно из них изоморфно начальному отрезку другого.

Более того, выполнено одно из трёх: $A \simeq B$, $A \simeq [0, b)$, $b \in B$, $B \simeq [0, a)$, $a \in A$.

Идея доказательства: если одно из множеств пустое, то утверждение очевидно.

Иначе в каждом из них есть минимальный элемент(0). Сопоставим эти элементы друг другу.

Если в одном из множеств больше ничего нет, то утверждение доказано.

Иначе в каждом есть минимальный ненулевой элемент(1). Сопоставим их друг другу.

Так будем продолжать: каждый раз либо одно из множеств закончилось и утверждение доказано, либо будем наращивать изоморфизм.

Сравнимость любых двух множеств по мощности

По теореме Цермело для любого множества существует равномощное ему ВУМ. Пусть даны A, B , а A', B' соответствующие им ВУМы, удовлетворяющие теореме Цермело. Тогда из теоремы о сравнимости ВУМов A' и B' сравнимы по мощности, значит, и также сравнимы по мощности.

5.12 Теорема о структуре: любой элемент вполне упорядоченного множества представляется как сумма предельного и конечного.

Теорема: Для любого элемента a вполне упорядоченного множества найдётся предельный элемент b и натуральное число k , такое что $a = \underbrace{S(S(\dots(S(b))\dots))}_{k \text{ раз}}$.

Доказательство: Нужно брать непосредственно предыдущий, пока не придём к предельному. Прийти обязаны, иначе будет бесконечно убывающая последовательность.

6 Вопросы из билетов

6.1 Эквивалентность фундированности, отсутствия бесконечно убывающей последовательности элементов и принципа трансфинитной индукции.

Мы будем работать с частично упорядоченным множеством (A, \leq) и для краткости будем его просто называть множеством A .

Теорема: Три определения фундированного множества эквивалентны друг другу:

1. Множество A называется фундированным, если в любом непустом подмножестве A есть минимальный элемент.
2. Множество A называется фундированным, если для него выполняется принцип невозможности бесконечного спуска: не существует бесконечной строго убывающей последовательности $x_1 > x_2 > x_3 > \dots$.
3. Множество A называется фундированным, если для него выполняется принцип трансфинитной индукции: для любого свойства $\varphi(x)$ верно условие:

$$\forall x (\forall y < x \varphi(y) \rightarrow \varphi(x)) \Rightarrow \forall x \varphi(x).$$

▲ $(1 \Rightarrow 2)$ Предположим, что 2 определение неверно, и в множестве есть бесконечная убывающая цепь $x_1 > x_2 > \dots$. Но тогда в множестве $B = \{x_1, x_2, \dots\}$ нет минимального элемента, что противоречит определению 1.

$(2 \Rightarrow 1)$ Теперь предположим, что определение 1 не выполнено. Это значит, что в A есть непустое подмножество B , в котором нет минимального элемента. Поскольку $B \neq \emptyset$, то $\exists x_1 \in B$. Мы предположили, что в B нет минимальных элементов. В частности, $x_1 \neq \min$, то $\exists x_2 < x_1$. Поскольку $x_2 \neq \min$, то $\exists x_3 < x_2$ и так далее, получим бесконечно убывающую последовательность. Это противоречит определению 2.

$(1 \Rightarrow 3)$ Снова предположим, что для некоторого A выполнено определение 1. Нам нужно доказать, что для данного множества выполнен также и принцип индукции. Пусть для какого-то свойства $\varphi(x)$ верен “шаг индукции”:

$$\forall x (\forall y < x \varphi(y) \rightarrow \varphi(x)).$$

Мы хотим показать, что в таком случае свойство $\varphi(x)$ верно для всех элементов $x \in A$. Предположим противное – пусть для некоторых x свойство $\varphi(x)$ ложно. Выберем среди всех таких x минимальный (определение фундированности гарантирует, что среди всех элементов x для которого $\varphi(x)$ ложно, есть хотя бы один минимальный). Тогда для данного x_{\min} свойство $\varphi(x_{\min})$ ложно, а для всех элементов y меньших x_{\min} свойство $\varphi(y)$ истинно. Получаем противоречие с предположением индукции (т.е. $1 \rightarrow 0$).

$(3 \Rightarrow 1)$ Теперь предполагаем, что для A выполнен принцип индукции. Нам нужно проверить, что $\forall B \subset A \mid B \neq \emptyset$ есть хотя бы один минимальный элемент. Пусть в некотором $B \subset A$ минимального элемента нет. Мы должны доказать, что данное B пусто. Для этого мы рассмотрим свойство $\varphi(x) : \varphi(x)$ истинно $\Leftrightarrow x \notin B$. Для данного свойства верно:

$$\forall x (\forall y < x \varphi(y) \rightarrow \varphi(x)).$$

(если все элементы $y < x$ не лежат в B , то и x не лежит в B , иначе x был бы минимальным элементом B) По принципу индукции заключаем, что свойство $\varphi(x)$ истинно для всех $x \in A$. Это значит, что в B нет ни одного элемента — это подмножество пусто. ■

6.2 Лемма о монотонной функции из вполне упорядоченного множества в себя.

Лемма: Пусть A – вполне упорядоченное множество, а $f : A \rightarrow A$ – строго монотонная функция ($x > y \Rightarrow f(x) > f(y)$). Тогда $\forall x f(x) \geq x$.

▲ Докажем через принцип невозможности бесконечного спуска:

Пусть для какого-то x верно $f(x) < x$. Тогда по строгой монотонности выполнено:

$$f(f(x)) < f(x), f(f(f(x))) < f(f(x)), \dots$$

Следовательно, образуется бесконечно убывающая последовательность

$$x > f(x) > f(f(x)) > f(f(f(x))) > \dots$$

Это противоречит фундированности A , значит, $\forall x f(x) \geq x$. ■

6.3 Теорема о структуре вполне упорядоченного множества: оно представляется как $\omega \cdot L + F$, где L – множество предельных элементов (кроме, возможно, наибольшего), F – конечное множество.

▲ Пусть P – множество предельных элементов нашего ВУМа. Заметим, что P – ВУМ (как подмножество ВУМа). Рассмотрим элемент $x \in P$. Пусть $Sx = y$ (следующий элемент). Построим биекцию между ω и $[x, y)$. Числу n из ω поставим в соответствие число $\underbrace{SS \dots S}_{n \text{ раз}} x$. Очевидно, что

это инъекция ($x + n = x + m \Leftrightarrow n = m$).

Докажем, что это сюръекция. Рассмотрим элемент t лежащий в $[x, y)$. Бесконечно уменьшать его на 1 (то есть брать предыдущий) нельзя по одному из эквивалентных определений фундированности \Rightarrow существует предельный элемент k (у которого нет предыдущего), такой что $S \dots Sk = t$. k лежит в $[x, y)$, но единственный предельный элемент, лежащий в этом множестве – это $x \Rightarrow k = x \Rightarrow t = S \dots Sk$ будет получен.

Повторим такие действия для всех x (кроме наибольшего). Затем возможны 2 случая

1. В исходном ВУМе нет наибольшего элемента. Тогда аналогично прошлым шагам строим изоморфизм между ω и оставшимися элементами. Получаем, что наш ВУМ равен $\omega \cdot P$.
2. В исходном ВУМе есть наибольший элемент. Тогда осталось лишь конечное число нерассмотренных элементов. Докажем это.

Обозначим наибольший элемент всего ВУМа как a . По определению фундированности, мы не сможем бесконечно брать предыдущий элемент \Rightarrow существует k – предельный, такой что $a = \underbrace{S \dots S}_{m \text{ раз}} k$. $k \geq x$, но x – наибольший из предельных элементов $\Rightarrow k = x \Rightarrow |[x, a]| = m + 1$.

Построим биекцию между этим отрезком и множеством $F = [0; m]$.

Таким образом, получаем, что наше ВУМ равномощно $\omega \cdot L + F$, где L – множество предельных элементов кроме, возможно, наибольшего, а F – конечное множество. ■

6.4 Теорема о трансфинитной рекурсии.

Теорема. Пусть A – вполне упорядоченное множество, B – произвольное множество. Пусть имеется некоторое рекурсивное правило (отображение F , которое ставит в соответствие элементу $x \in A$ и функции $g : [0, x) \rightarrow B$ некоторый элемент B). Тогда $\exists!$ функция $f : A \rightarrow B$: $f(x) = F(x, f|_{[0, x)}) \forall x \in A$. (здесь $f|_{[0, x)}$ обозначает ограничение функции f на начальный отрезок $[0, x)$)

▲ Идея доказательства: значение f на минимальном элементе определено однозначно, так как предыдущих значений нет (сужение $f|_{[0, 0)}$ пусто). Тогда и на следующем элементе значение

функции f определено однозначно, поскольку на предыдущих (точнее, единственном предыдущем) функция f уже задана, и т. д.

Строгое док-во:

1. Утверждение о произвольном $a \in A$: существует и единственно отображение f отрезка $[0, a]$ в множество B , для которого рекурсивное определение (равенство, приведённое в условии) выполнено при всех $x \in [0, a]$.

Пусть отображение $f : [0, a] \rightarrow B$, обладающее указанным свойством – "корректное". Таким образом, мы хотим доказать, что $\forall a \in A \exists!$ корректное отображение отрезка $[0, a]$ в B . Поскольку мы рассуждаем по индукции, можно предполагать, что для всех $c < a$ это утверждение выполнено, то есть существует и единственно корректное отображение $f_c : [0, c] \rightarrow B$. (Корректность f_c означает, что при всех $d \leq c$ значение $f_c(d)$ совпадает с предписанным по рекурсивному правилу.)

Рассмотрим отображения f_{c_1} и f_{c_2} для двух различных $c_1 < c_2$. Отображение f_{c_2} определено на большем отрезке $[0, c_2]$. Если ограничить f_{c_2} на меньший отрезок $[0, c_1]$, то оно совпадёт с f_{c_1} , поскольку ограничение корректного отображения на меньший отрезок корректно (это очевидно), а мы предполагали единственность на отрезке $[0, c_1]$.

Таким образом, все отображения f_c согласованы друг с другом (принимают одинаковое значение, если определены одновременно). Объединив их, мы получаем некоторое единое отображение h , определённое на $[0, a)$. Применив к a и h рекурсивное правило, получим некоторое значение $b \in B$. Доопределим h в точке a , положив $h(a) = b$. Получится отображение $h : [0, a] \rightarrow B$; легко понять, что оно корректно.

Чтобы завершить индуктивный переход, надо проверить, что на отрезке $[0, a]$ корректное отображение единственно. В самом деле, его ограничения на отрезки $[0, c]$ при $c < a$ должны совпадать с f_c , поэтому осталось проверить однозначность в точке a – что гарантируется рекурсивным определением (выражающим значение в точке a через предыдущие). На этом индуктивное доказательство заканчивается.

2. Осталось лишь заметить, что для разных a корректные отображения отрезков $[0, a]$ согласованы друг с другом (сужение корректного отображения на меньший отрезок корректно, применяем единственность) и потому вместе задают некоторую функцию $f : A \rightarrow B$, удовлетворяющую рекурсивному определению. Существование доказано; единственность тоже понятна, так как ограничение этой функции на любой отрезок $[0, a]$ корректно и потому однозначно определено, как мы видели. ■

6.5 Сравнимость любых двух вполне упорядоченных множеств.

Теорема. Если A и B – ВУМы, то верно ровно одно из трёх:

1. $A \simeq B$;
2. $A \simeq [0, b)$, $b \in B$;
3. $B \simeq [0, a)$, $a \in A$.

▲

1. Покажем, что 2 и 3 не могут быть выполнены одновременно. $A \simeq [0, b)$, $B \simeq [0, a) \Rightarrow$ начальный отрезок B изоморфен начальному отрезку начального отрезка A , а начальный отрезок начального отрезка так же является начальным отрезком. Получили что A *изоморфно своему начальному отрезку*, что невозможно по следствию, противоречие. Аналогичными рассуждениями можно понять, что 1 и 2, 1 и 3 тоже не могут быть выполнены одновременно. Таким образом, понимаем, что не больше одного из этих пунктов может быть выполнено.

2. Покажем, что хотя бы один из этих пунктов будет выполнен (будем использовать трансфинитную рекурсию): постепенно построим функцию с аргументами в A и значениями в B . Строим функцию $g : A \rightarrow B \cup \{\perp\}$, где \perp – специальный символ неопределённости (любую частично

определённую функцию можно переделать во всюду определённую, если добавить специальный символ неопределённости)

Строим функцию рекурсивно: $g(a) = \{\min\{y \in B : y \neq g(x) \text{ для } x < a\}\}$ (1), если это множество не пусто, иначе - \perp .

Корректность определения: *функция g существует и единственна*. Скажем, что $g|_{[0,a)} : [0,a) \rightarrow B \cup \{\perp\}$ корректна, если она удовлетворяет соотношению (1). Докажем по трансфинитной индукции, что $g|_{[0,a)}$ существует и единственна. Пусть $\forall x < a$ $g|_{[0,x)}$ существует и единственна. Тогда при $x < a$ $g|_{[0,x)}(x)$ определено однозначно.

Пусть $a < c$. Тогда $g|_{[0,a)}$ и $g|_{[0,c)}$ совпадают на $[0,a)$ (ввиду однозначности). Можно рассмотреть $g : A \rightarrow B \cup \{\perp\}$, которая продолжает все $g|_{[0,a)}$. Если в множестве A есть максимальный элемент, то он не попадёт ни в один из полуинтервалов, но он ровно один, и для него всё доопределяется по (1). Если же максимального элемента нет, то нужно всё объединить.

I. $\exists a : g(a) = \perp \Rightarrow$ при всех $c > a$ $g(c) = \perp$

Если $g(c) = \perp$, то пусть $a = \min\{x | g(x) = \perp\}$. Тогда $B \simeq [0, a)$. Доказывается, что при $x < a$ начальный отрезок $[0, x) \simeq [0, g(x))$, g - изоморфизм. Пусть при $y < x$ $[0, y) \simeq [0, g(y))$.

инъекция: $y_1 < y_2 < x \Rightarrow g(y_2) = \min\{z \in B : z \neq g(x) \text{ для } x < y_2\} \Rightarrow g(y_1) \neq g(y_2)$

сюръекция: $z < g(x) \Rightarrow z = g(v)$ при $v < x$

Сохранение порядка: $y_1 < y_2 < x \Rightarrow g(y_1) < g(y_2)$. По написанному выше $g(y_1) \neq g(y_2)$. Но $g(y_2)$ не может быть меньше, чем $g(y_1)$, иначе бы получилось, что до $g(y_1)$ есть какие-то пустые места, и $g(y_1)$ бы определилось не так, как оно определилось, а занято было бы то пустое место.

II. $\nexists a : g(a) = \perp$:

- все значения в B принимаются. Тогда $A \simeq B$

- не все значения в B принимаются. Тогда $b = \min\{y | y \neq g(x), x \in A\}$, и $A \simeq [0, b)$ ■

6.6 Теорема о вычитании вполне упорядоченных множеств.

Теорема. $\alpha \leq \beta \Rightarrow \exists! \gamma : \alpha + \gamma = \beta$ (с точностью до изоморфизма).

▲ Наше $\alpha \simeq [0, b)$ (см. предыдущий билет), тогда $\exists \gamma = \beta \setminus ([0, b))$

Докажем единственность. Пусть есть $\gamma_1 < \gamma_2 \Rightarrow \alpha + \gamma_1 < \alpha + \gamma_2 \Rightarrow$ они не могут оба равняться β . Противоречие. ■

6.7 Теорема о делении с остатком вполне упорядоченных множеств.

Теорема $\forall \alpha, \beta \quad \exists! \gamma, \delta : \delta < \alpha$ и $\alpha = \beta \cdot \gamma + \delta$, где $\alpha, \beta, \gamma, \delta$ – ВУМы.

Доказательство:

1) Существование.

Рассмотрим ζ такое, что заведомо $\beta \zeta > \alpha$ (например, подойдет $\zeta = \alpha + 1$).

Это значит, что α равняется некоторому начальному отрезку $\beta \zeta$. Этот начальный отрезок представляется в виде $[0; q)$, $q \in \beta \zeta$ и потому $q = (b, g)$, $b \in \beta$, $g \in \zeta$

$\alpha \in [0; q) \Rightarrow \alpha = (s, t)$: либо $t < g$, а s любое из β , либо $t = g$, $s < b$.

Для каждого $t < g$ получаем экземпляр β , порядок на этих экземплярах взят с $[0; g)$

В итоге : $\gamma = [0; g)$, $\delta = [0; b)$

2) Единственность.

Если $\gamma_1 = \gamma_2$, то аналогично единственности вычитания. Если $\gamma_1 < \gamma_2$, то $\gamma_1 + 1 \leq \gamma_2$ и поэтому $\beta \cdot \gamma_1 + \delta_1 < \beta \cdot \gamma_1 + \beta = \beta \cdot (\gamma_1 + 1) \leq \beta \cdot \gamma_2 \leq \beta \cdot \gamma_2 + \delta_2$.

6.8 Теорема Цермело.

Теорема Цермело: Любое множество можно вполне упорядочить, то есть у любого множества есть равномощное ему вполне упорядоченное множество.

▲ Пусть φ – функция из аксиомы выбора для множества A . Назовем корректным фрагментом ВУМ $\langle S, \leq_S \rangle$, где $S \subset A$ и $\forall x \in S \ x = \varphi(\{y | y <_S x\})$.

По теореме о сравнении из двух корректных фрагментов один изоморфен начальному отрезку другого (так как они оба ВУМы). Покажем, что он не только изоморфен, но и равен начальному отрезку другого.

Пусть это не так. Тогда пусть x – минимальный элемент, в котором изоморфизм f дал не то значение. Тогда начальный отрезок $[0; x)$ лежит в обоих корректных фрагментах, а значит $x = \varphi([0; x)) = f(x)$ – противоречие.

Легко заметить, что объединение корректных фрагментов – это корректный фрагмент, так как если x лежит в объединении, то x лежит в каком-то из корректных фрагментов, а значит равенство $x = \varphi([0; x))$ сохраняется в объединении.

Объединим все корректные фрагменты (множество всех корректных фрагментов существует так как оно является подмножеством множества упорядоченных подмножеств A). Предположим, что мы получили $B \subset A, B \neq A$. Но тогда мы можем дополнить объединение элементом $\varphi(B)$ и получить корректный фрагмент, больший объединения всех корректных фрагментов – противоречие $\Rightarrow B = A \Rightarrow$ мы смогли вполне упорядочить A . ■

6.9 Лемма Цорна.

Лемма Цорна: Пусть Z – частично упорядоченное множество, в котором всякая цепь имеет верхнюю границу. Тогда в этом множестве есть максимальный элемент, и, более того, для любого элемента $a \in Z$ существует элемент $b \geq a$, являющийся максимальным в Z .

▲ Пусть дан произвольный элемент a . Предположим, что не существует максимального элемента, большего или равного a . Это значит, что для любого $b \geq a$ найдётся $c > b$. Тогда $c > a$ и потому найдётся $d > c$ и т. д. Продолжая этот процесс достаточно долго, мы исчерпаем все элементы Z и придём к противоречию.

Проведём рассуждение аккуратно. Возьмём вполне упорядоченное множество I достаточно большой мощности (большей, чем мощность Z , например 2^Z). Построим строго возрастающую функцию $f : I \rightarrow Z$ по трансфинитной рекурсии. Её значение на минимальном элементе I будет равно a . Предположим, что мы уже знаем все её значения на всех элементах, меньших некоторого i . В силу монотонности эти значения попарно сравнимы, а значит, образуют цепь. Поэтому существует их верхняя граница s , которая, в частности, больше или равна a . Возьмём какой-то элемент $t > s$ и положим $f(i) = t$; по построению монотонность сохранится. Тем самым I равномощно части Z , что противоречит его выбору.

В этом рассуждении, формально говоря, есть пробел: мы одновременно определяем функцию по трансфинитной рекурсии и доказываем её монотонность с помощью трансфинитной индукции. Наше рекурсивное определение имеет смысл, лишь если уже построенная часть функции монотонна. Формально говоря, можно считать, что следующее значение не определено, если уже построенный участок не монотонен, и получить функцию, определённую на всём I или на начальном отрезке. Если она определена на некотором начальном отрезке, то она монотонна на нём по построению, поэтому следующее значение тоже определено – противоречие ■

6.10 Любой частичный порядок можно дополнить до линейного.

Применение леммы Цорна: любой частичный порядок можно дополнить до линейного.

Если P – отношение частичного порядка, то существует S – отношение линейного порядка, т.ч. $P \subset S$. В качестве A рассмотрим множество отношений порядка. Упорядочение на A – вложение как подмножества. Это упорядочение соответствует условию леммы Цорна: у любой цепи есть верхняя грань, а именно объединение всех элементов цепи.

Нужно доказать, что в объединении получится порядок:

Рефлексивность : наследуется из каждого элемента цепи

Антисимметричность : если в итоговом порядке $a < b$ и $b < a$, то для каких-то порядков из цепи $a \leq_i b, b \leq_j a$:

Если $j > i$, то $a \leq_j b$. Из антисимметричности \leq_j , Получаем $a = b$.

Транзитивность : аналогично, если $a \leq b$ и $b \leq c$, то $a \leq_i b$ и $b \leq_j c$, отсюда $a \leq_j b, b \leq_j c$, откуда $a \leq_j c$ и потому $a \leq c$

По лемме Цорна есть максимальный элемент. Нужно доказать, что он линеен. Т.е. если какие-то 2 элемента не сравнимы, то порядок можно продолжить.

Пусть a и b несравнимы. Тогда построим новый порядок $x \leq' y$, если $\left[\begin{array}{l} x \leq y \\ x \leq a, b \leq y \end{array} \right]$

Докажем, что \leq' является порядком.

Рефлексивность : наследуется из \leq .

Антисимметричность : 4 случая:

Если $x \leq y$ и $y \leq x$, то $x = y$ по антисимметричности \leq .

Если $x \leq y, y \leq a, b \leq x$, то $b \leq a$, что противоречит предположению.

Остальные два случая аналогичны.

Транзитивность:

Если $x \leq y, y \leq a, b \leq z$, то $x \leq a, b \leq z \Rightarrow x \leq' z$.

Если $x \leq a, b \leq y, y \leq a, b \leq z$, то $b \leq a$, что невозможно.

Получаем, что все 3 свойства верны. Т.е. нелинейный порядок можно дополнить, поэтому максимальный элемент является линейным.

6.11 Объединение двух бесконечных множеств равномощно одному из них.

Вспомогательная теорема. Формулировка: Если A бесконечно, то множество $A \times N$ равномощно A .

Доказательство: Вполне упорядочим множество A . Мы уже знаем, что всякий элемент множества A однозначно представляется в виде $z + n$, где z – предельный элемент (не имеющий непосредственно предыдущего), а n – натуральное число. Это означает, что A равномощно $B \times N$, где B – множество предельных элементов. (Тут есть небольшая трудность – последняя группа элементов конечна, если в множестве есть наибольший элемент. Но мы уже знаем, что добавление конечного или счётного множества не меняет мощности, так что этим можно пренебречь.) Теперь утверждение теоремы очевидно: $A \times N$ равномощно $(B \times N) \times N$, то есть $B \times (N \times N)$ и тем самым $B \times N$ (произведение счётных множеств счётно), то есть A .

По теореме Кантора-Бернштейна отсюда следует, что промежуточные мощности (в частности, $|A| + |A|$, а также любое произведение A и конечного множества) совпадают с $|A|$.

Формулировка: Сумма двух бесконечных мощностей равна их максимуму.

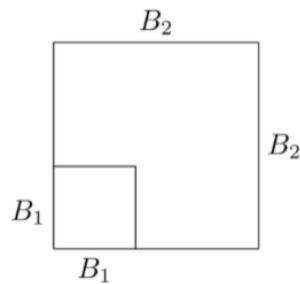
Доказательство: Прежде всего напомним, что любые две мощности сравнимы. Пусть, скажем, $|A| \leq |B|$. Тогда $|B| \leq |A| + |B| \leq |B| + |B| \leq |B| \times N \leq |B|$ (последнее неравенство – утверждение предыдущей теоремы). Остаётся воспользоваться теоремой Кантора-Бернштейна и заключить, что $|B| = |A + B|$.

$B \preceq A, A \preceq A \cup B \preceq A \times 0, 1 \preceq A \times N \preceq A$.

6.12 Декартов квадрат бесконечного множества равномошен ему.

Доказательство: Заметим, что для счётного множества мы это уже знаем. Поэтому в A есть подмножество, равномошное своему квадрату. Рассмотрим семейство всех таких подмножеств вместе с соответствующими биекциями. Элементами этого семейства будут пары (B, f) , где B – подмножество A , а $f : B \rightarrow B \times B$ – взаимно однозначное соответствие. Введём на этом семействе частичный порядок: $(B_1, f_1) \leq (B_2, f_2)$, если $B_1 \subset B_2$ и ограничение отображения f_2 на B_1 совпадает с f_1 .

Свойства операций над мощностями

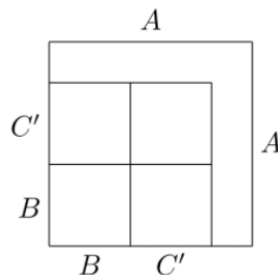


Отображение f_1 — взаимно однозначное соответствие между малым квадратом и его стороной; f_2 добавляет к нему взаимно однозначное соответствие между $B_2 \setminus B_1$ и «уголком» $(B_2 \times B_2) \setminus (B_1 \times B_1)$.

Теперь применим лемму Цорна. Для этого нужно убедиться, что любое линейно упорядоченное (в смысле описанного порядка) множество пар указанного вида имеет верхнюю границу. В самом деле, объединим все первые компоненты этих пар; пусть B — их объединение. Как обычно, согласованность отображений (гарантируемая определением порядка) позволяет соединить отображения в одно. Это отображение (назовём его f) отображает B в $B \times B$. Оно будет инъекцией: значения $f(b')$ и $f(b'')$ при различных b' и b'' различны (возьмём большее из множеств, которым принадлежат b' и b'' ; на нём f является инъекцией по предположению). С другой стороны, f является сюръекцией: для любой пары $(b', b'') \in B \times B$ возьмём множества, из которых произошли b' и b'' , выберем из них большее и вспомним, что мы имели взаимно однозначное соответствие между ним и его квадратом.

По лемме Цорна в нашем частично упорядоченном множестве существует максимальный элемент. Пусть этот элемент есть (B, f) . Мы знаем, что f есть взаимно однозначное соответствие между B и $B \times B$ и потому $|B| = |B| \times |B|$. Теперь есть две возможности. Если B равномошно A , то $B \times B$ равномошно $A \times A$ и всё доказано. Осталось рассмотреть случай, когда B не равномошно A , то есть имеет меньшую мощность (большей оно иметь не может, будучи подмножеством). Пусть C — оставшаяся часть A , то есть $A \setminus B$.

Тогда $|A| = |B| + |C| = \max(|B|, |C|)$, следовательно, C равномошно A и больше B по мощности. Возьмём в C часть C' , равномошную B , и положим $B' = B + C'$.



Продолжение соответствия с B на $B' = B + C'$.

Обе части множества B' равномощны B . Поэтому $B' \times B'$ разбивается на 4 части, каждая из которых равномощна $B \times B$, и, следовательно, равномощна B (т.к. $C', (B' \times B'), (B \times B)$ равномощны B). В итоге мы получаем большую пару (B', f') , что противоречит утверждению леммы Цорна о максимальнойности. Таким образом, этот случай невозможен.

Вычислимость.

7 Определения

7.1 Машина Тьюринга.

Определение: Формальное определение *машины Тьюринга* – это кортеж $(\Sigma, \Gamma, Q, q_1, q_a, q_r, \delta)$, где

Σ – конечное непустое множество – входной алфавит, типично $\{0,1\}$.

Γ – конечное непустое множество, включающее в себя Σ , как подмножество, а также, по меньшей мере, еще пустой символ (бланк, пробел) – ленточный алфавит.

Q – конечное множество, не пересекающееся с Γ – множество внутренних состояний.

$q_1 \in Q$ – начальное состояние.

$q_a \in Q$ – принимающее состояние.

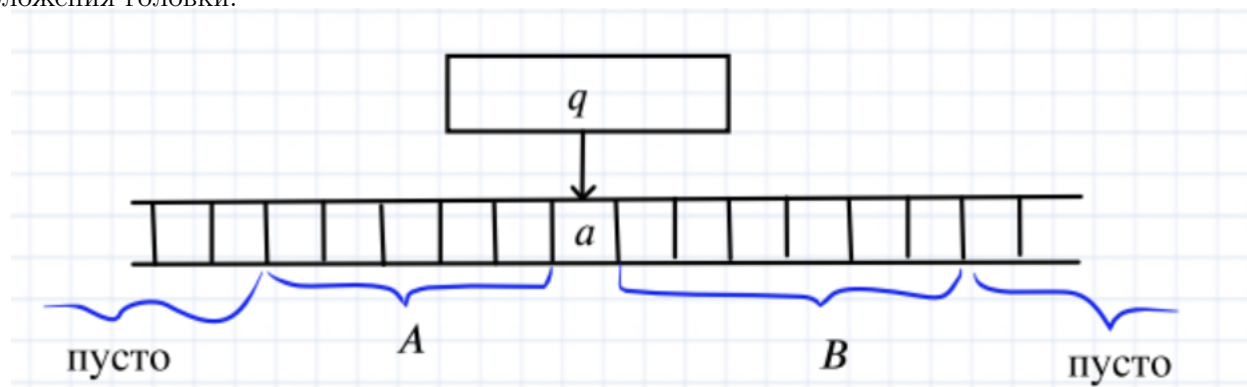
$q_r \in Q$ – отвергающее состояние.

δ – функция перехода. $\delta : Q \times \Gamma \rightarrow Q \times \Gamma \times \{L, R, N\}$, где L – перемещение влево, R – вправо, N – никуда.

Для задач с текстовым или числовым ответом вместо q_r, q_a рассматривают одно q_0 .

Определение: *Конфигурация машины Тьюринга* – данные о содержимом ленты, положении указателя и состоянии управляющего блока.

Начальная конфигурация: на ленте написан вход, машина в состоянии q , указывает на первый символ входа. У каждой конфигурации есть однозначно определяемая следующая. Если состояние завершающее, конфигурация уже не меняется. Иначе производится замена символа, состояния и положения головки.



AqaB

Вычислением на машине Тьюринга называется последовательность конфигураций, каждая из которых непосредственно следует из предыдущей по правилам этой машины.

Пример смены конфигураций

Если, например, $B = bB'$, и $\delta(q,a) = (s,c,R)$, то следующая конфигурация за $AqaB$ будет $AcsbB'$
 Если $B = \epsilon$ и $\delta(q,a) = (s,c,R)$, то следующая конфигурация будет $Acs\#$ ($\#$ – бланк)

q,s – состояния

7.2 Вычислимая функция.

Определение: Функция $f : \{0,1\}^* \rightarrow \{0,1\}^*$ называется *вычислимой*, если для некоторой машины Тьюринга выполнено:

- 1 Если $f(x)$ определена, то существует вычисление, которое начинается с q_1x и заканчивается $q_0f(x)$.
- 2 Если $f(x)$ не определена, то машина Тьюринга не остановится.

Примеры

6. Пусть $\Sigma = \{0, 1\}$. Опишите машины, вычисляющие функции:

- а) $f(x) = x$,
- б) $f(x) = 0$,
- в) нигде не определённую.

Ответы:

- а) $q_10 \rightarrow q_00N, q_11 \rightarrow q_01N, q_1\# \rightarrow q_0\#N$
- б) $q_10 \rightarrow q_1\#R, q_11 \rightarrow q_1\#R, q_1\# \rightarrow q_00N$
- в) $q_10 \rightarrow q_10N, q_11 \rightarrow q_11N, q_1\# \rightarrow q_1\#N$

7.3 Разрешимое множество.

Определение: Множество $A \subset \{0,1\}^*$ называется *разрешимым*, если для некоторой машины Тьюринга выполнено:

- 1 Если $x \in A$, то существует вычисление на этой машине, которое начинается с q_1x и заканчивается q_a .
- 2 Если $x \in \bar{A}$, то существует вычисление на этой машине, которое начинается с q_1x и заканчивается q_r .

7.4 Перечислимое множество.

Будем рассматривать машину, у которой вместо завершающих состояний есть команды печати в поток вывода: печать 0, печать пробела. Результатом работы такой машины будет конечная или бесконечная цепочка слов, разделённых пробелами.

Определение: Множество называется *перечислимым*, если существует печатающая машина, такая что:

Если $x \in A$, то x встречается в потоке вывода.

Если $x \notin A$, то x не встречается в потоке вывода.

Примеры

- ✓ Пустое множество является перечислимым.
- ✓ Область значений/Область определения любой вычислимой функции – перечислимое множество.
- × $\{n|U(n, x) \text{ определено при всех } x\}$ – неперечислимо.

7.5 Универсальная машина Тьюринга.

Определение: *Универсальная машина Тьюринга* – это некоторая машина, которая получает на вход описание другой машины и вход для нее, а возвращает результат ее работы.

$$U(\langle M \rangle, x) = M(x).$$

7.6 Универсальная вычислимая функция.

Определение: Функция $u : \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$ называется *универсальной вычислимой функцией*, если:

- 1 u вычислима, как функция от двух аргументов.
- 2 Если $f : \{0,1\}^* \rightarrow \{0,1\}^*$ – вычислимая функция одного аргумента, то $\exists p \forall x u(p, x) = f(x)$.

7.7 Главная универсальная вычислимая функция.

Определение: $U : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ – *главная универсальная вычислимая функция*, если

- 1 U вычислима.
- 2 U универсальна, т.е. для любой вычислимой $f : \mathbb{N} \rightarrow \mathbb{N}$ найдется p такое, что $\forall x f(x) = U(p, x)$ (говорят, что p – это номер функции f).
- 3 U главная, т.е. для любой вычислимой $V : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ найдется всюду определенная вычислимая $s : \mathbb{N} \rightarrow \mathbb{N}$, такая что $\forall p \forall x V(p, x) = U(s(p), x)$.

Интуитивный смысл: U – универсальный компилятор, V – какой-то вычислимый. Первый аргумент V – “программа”, второй – “данные”, s – “автоматический транслятор”, переделывающие программу для V в программу для U .

7.8 m -сводимость.

Определение: Говорят, что A *m -сводится* к B , если существует всюду определенная вычислимая функция $f : \mathbb{N} \rightarrow \mathbb{N}$, такая что $x \in A \Leftrightarrow f(x) \in B$. Обозначение: $A \leq_m B$.

7.9 Арифметическая иерархия.

Определение: Говорят, что множество A принадлежит классу Σ_n , если существует такое разрешимое множество $R \in \mathbb{N}^{k+1}$, что

$$x \in A \Leftrightarrow \exists y_1 \forall y_2 \exists y_3 \dots Qy_n [(x, y_1, \dots, y_k) \in R].$$

Аналогично, говорят, что A принадлежит классу Π_n , если существует такое разрешимое множество $R \in \mathbb{N}^{k+1}$, что

$$x \in A \Leftrightarrow \forall y_1 \exists y_2 \forall y_3 \dots Qy_n [(x, y_1, \dots, y_k) \in R].$$

Согласно этому определению, $\Sigma_0 = \Pi_0$ (классы Σ_0 и Π_0 совпадают с классом всех разрешимых множеств).

Σ_1 – перечислимые, Π_1 – коперечислимые

▲ S перечисливо \Leftrightarrow для некоторого разрешимого R верно $(x \in S \Leftrightarrow \exists y (x, y) \in R)$, Q коперечисливо \Leftrightarrow для некоторого разрешимого R верно $(x \in S \Leftrightarrow \forall y (x, y) \in R)$.

Примеры

1 T – множество всюду определенных функций.

$p \in T \Leftrightarrow \forall n \exists k (U(p, n) \text{ останавливается за } k \text{ шагов})$ – разрешимое свойство $\Rightarrow T \in \Pi_2$.

2 FD – множество функций с конечной областью определения.

$p \in FD \Leftrightarrow \exists N \forall n \forall k (n > N \Rightarrow U(p, n) \text{ останавливается за } k \text{ шагов})$ – разрешимое свойство $\Rightarrow FD \in \Sigma_2$.

7.10 λ -термы, α -конверсии, β -редукции, нормальная форма.

Определение: λ -терм строится по индукции:

1 Переменная является λ -термом.

2 (Операция аппликации): Если M и N суть лямбда-термы, то (MN) – тоже лямбда-терм.

Смысл: в функцию M вместо переменного подставляем N .

3 (Операция λ -абстракции): Если M – терм, а x – переменная, то $(\lambda x.M)$ – тоже терм. Смысл: выражение M теперь рассматривается как функция от x .

Определение: α -конверсия – это замена связанной переменной. $\lambda x.M \rightarrow \lambda z.M(z/x)$

Ограничение: не должно возникать конфликтов имен. Переменные из M не должны попадать под действие λ -квантора.

Пример

✓ $\lambda x.xy \rightarrow \lambda z.zy$ – так можно.

✓ $\lambda x.xy(\lambda x.xy) \rightarrow \lambda z.zy(\lambda x.xy)$ – и так можно.

× $\lambda x.xy \rightarrow \lambda y.yy$ – а вот так нельзя.

× $\lambda x.x(\lambda y.xy) \rightarrow \lambda y.y(\lambda y.yy)$ – и так тоже нельзя! Тут переменная, полученная после замены, попала под воздействие уже имеющегося квантора.

Определение: β -редукция – это замена аргумента функции на какое-то значение. $(\lambda x.M)N \rightarrow M(N/x)$

Ограничение: не должно возникать конфликтов имен. В N не должно быть переменных, по которым стоят λ -кванторы в M

Пример

✓ $\sin x$ при $x = 2$ равен $\sin 2$.

× $(\lambda x.(x\lambda y.xy))y \rightarrow y\lambda y.yy$ – так нельзя.

Определение: Говорят, что терм M находится в *нормальной форме*, если к нему нельзя применить β -редукцию даже после нескольких α -конверсий

Говорят, что N – нормальная форма M , если $M = N$ и N находится в нормальной форме.

Не у всех термов есть нормальная форма.

Пример

$\Omega = (\lambda x.xx)(\lambda x.xx)$

7.11 Нумералы Чёрча.

Определение:

Формально, число k соответствует преобразованию функции f в ее k -ую итерацию:

$$\begin{aligned}\bar{0} &= \lambda f x. x \\ \bar{1} &= \lambda f x. f x \\ \bar{2} &= \lambda f x. f(fx) \\ &\vdots \\ \bar{n} &= \lambda f x. f(f \dots f(fx)) \dots - n \text{ раз } f.\end{aligned}$$

7.12 Комбинатор неподвижной точки.

Определение: Комбинатором называется замкнутый λ -терм (без свободных переменных).

Говорят, что комбинатор G представляет функцию $g : \mathbb{N}^k \rightarrow \mathbb{N}$, если для любых n_1, \dots, n_k выполнено:

$$G\bar{n}_1\bar{n}_2 \dots \bar{n}_k = \overline{g(n_1, \dots, n_k)}.$$

Если g не определена, то у $G\bar{n}_1\bar{n}_2 \dots \bar{n}_k$ нет нормальной формы.

Пример

1 Inc – прибавление 1. Inc $\bar{n} = \bar{n} + 1$:

$$Inc = \lambda n f x. f(n f x)$$

2 Add – сложение. Add $\bar{n}\bar{m} = \overline{n + m}$:

$$Add = \lambda m n f x. m f(n f x)$$

3 Mult – умножение:

$$Mult = \lambda m n f x. m(n f)x$$

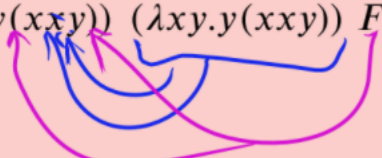
4 Exp – возведение в степень:

$$Exp = \lambda m n f x. n m f x$$

Определение: Y – комбинатор неподвижной точки, если для любого F верно $YF = F(YF)$.

Пример

Пример : $Y = (\lambda x y. y(xxy))(\lambda x y. y(xxy))$

$$YF = (\lambda x y. y(xxy)) (\lambda x y. y(xxy)) F$$


$$= F((\lambda x y. y(xxy))(\lambda x y. y(xxy)) F) = F(YF)$$

8 Простые утверждения

8.1 Композиция вычислимых функций вычислима.

Пусть машина M_f вычисляет функцию f , а машина M_g — функцию g . Тогда функцию $f(g(x))$ можно вычислить машиной M_g , которая вместо своего конечного состояния переходит в начальное состояние машины M_f (при этом для самой машины M_f нужны новые состояния, не пересекающиеся с состояниями M_g).

8.2 Существование невычислимых функций, неразрешимых и неперечислимых множеств (из соображений мощности).

Невычислимая

Функции, о которых идет речь, представляют собой функции, заданные и принимающие значения в множестве слов в алфавите A . Ясно, что множество слов в алфавите A счетно. Следовательно, рассматривается множество всех функций, заданных на счетном множестве и принимающих значения в счетном же множестве. Как известно, это множество имеет мощность континуума. С другой стороны, поскольку множество всевозможных машин Тьюринга счетно, то множество функций, вычислимых по Тьюрингу, также счетно. Континуальная мощность строго больше счетной. Следовательно, существуют функции, не вычисляемые по Тьюрингу.

Неразрешимое и неперечислимое множество

Алгоритмов (и поэтому разрешимых/перечислимых подмножеств натурального ряда) счётное число, а всех подмножеств натурального ряда несчётное число. Значит, из соображения мощности найдутся неразрешимые и неперечислимые множества.

8.3 Разрешимость любого конечного множества.

Алгоритм разрешения любого конечного множества S содержит таблицу элементов множества S , вход сравнивается по очереди со всеми элементами таблицы. В случае совпадения выдаем 1, иначе 0.

8.4 Перечислимость любого разрешимого множества.

По определению разрешимого множества, существует такая машина, что если $x \in A$, то существует вычисление, начинающееся в q_1x и заканчивающееся в q_a . Это значит, что для этой машины все $x \in A$ встречаются в потоке вывода. Значит, множество A перечислимо.

8.5 Замкнутость классов разрешимых и перечислимых множеств относительно пересечения, объединения, декартова произведения и конкатенации, класса разрешимых относительно дополнения и разности.

Пересечение и объединение перечислимых множеств – перечислимое множество

Если X и Y перечисляются алгоритмами A и B , то их объединение перечисляется алгоритмом, который параллельно выполняет по шагам A и B и печатает всё, что печатают A и B . С пересечением немного сложнее – результаты работы A и B надо накапливать и сверять друг с другом; что появится общего – печатать.

Пересечение, объединение, дополнение разрешимых множеств – разрешимое множество

Пересечение, объединение, дополнение – это просто композиция соответствующей характеристической функции и булевой функции.

- ▷ Для дополнения достаточно рассмотреть тот же алгоритм, что и для разрешения множества A . Вместо единицы печатать 0, вместо 0 – единицу.

▷ $\chi_{A \cup B}(x) = \chi_A \vee \chi_B$ – вычислима.

▷ $\chi_{A \cap B}(x) = \chi_A \wedge \chi_B$ – вычислима.

8.6 Существование вычислимой в обе стороны биекции между \mathbb{N}^2 и \mathbb{N} .

$$(x, y) \mapsto (2x + 1)2^y$$

Это биекция – очевидно, так как любое число представимо таким образом, причем разным числам соответствуют разные представления, и для любого числа вида $(2x + 1)2^y$ найдется число из \mathbb{N} . Опишем алгоритм вычисления:

⇒ Очевидно, такая функция вычислима, как функция от двух аргументов.

⇐ Делим число на 2, пока оно четно. Получаем отсюда y . Потом вычитаем один, делим на 2, получаем x .

Таким образом, построенная биекция вычислима в обе стороны, а значит, подходит под условие.

8.7 Подмножество разрешимого (перечислимого) множества не обязательно разрешимо (перечислимо), и наоборот.

Подмножество разрешимого/перечислимого множества может быть неразрешимо/неперечислимо. Любое множество, в том числе неразрешимое/неперечислимое, является подмножеством \mathbb{N} , которое разрешимо/перечислимо.

Подмножество неразрешимого/неперечислимого множества может быть разрешимо/перечислимо. Достаточно в любом множестве выбрать конечное подмножество, тогда оно разрешимо/перечислимо.

8.8 Свойства m -сводимости: транзитивность, сводимость дополнений, разрешимость множества, m -сводимого к разрешимому, перечислимость множества, m -сводимого к перечислимому, сводимость разрешимого множества к любому нетривиальному.

Основные свойства m -сводимости :

0) Рефлексивность $A \leq_m A$.

1) Транзитивность : $A \leq_m B, B \leq_m C \Rightarrow A \leq_m C$.

Это следует из того, что композиция вычислимых функций вычислима

$$x \in A \Leftrightarrow f(x) \in B \Leftrightarrow g(f(x)) \in C$$

2) Сводимость к разрешимому : $A \leq_m B, B$ разрешимо $\Rightarrow A$ разрешимо

$$x \in A \Leftrightarrow f(x) \in B \Leftrightarrow R(f(x)) = 1$$

$R \circ f$ вычислимо и будет программой, разрешающей A

3) Сводимость к перечислимому : $A \leq_m B, B$ перечислимо $\Rightarrow A$ перечислимо

Например, как выше, но в качестве R нужно взять программу, вычисляющую полухарактеристическую функцию

$$4) \text{ Сводимость дополнений : } A \leq_m B \Leftrightarrow \bar{A} \leq_m \bar{B}$$

$$x \in \bar{A} \Leftrightarrow \neg(x \in A) \Leftrightarrow \neg(f(x) \in B) \Leftrightarrow f(x) \in \bar{B} \text{ (т.е. годится та же самая функция)}$$

5) сводимость разрешимых множеств

Если A разрешимо, а B и \bar{B} непусты, то $A \leq_m B$

$$\text{Если есть } b_0 \in B \text{ и } b_1 \in \bar{B}, \text{ то рассмотрим } f(x) = \begin{cases} b_0, & x \in A \\ b_1, & x \in \bar{A} \end{cases}$$

8.9 Вложенность классов в арифметической иерархии.

$$\Sigma_k \subset \Sigma_{k+1}, \Sigma_k \subset \Pi_{k+1}, \Pi_k \subset \Sigma_{k+1}, \Pi_k \subset \Pi_{k+1}.$$

▲ Добавляем нужный квантор по фиктивной переменной. Например, $\exists y(x, y) \in R \Leftrightarrow \exists y \forall z(x, y, z) \in R \times \mathbb{N} \Leftrightarrow \forall t \exists y(x, y, t) \in R \times \mathbb{N}$ (из Σ_1 в Π_2, Σ_2). ■

8.10 Замкнутость классов арифметической иерархии относительно объединения и пересечения.

Пусть $A, B \in \Sigma_k$. Тогда:

$$\begin{aligned} x \in A &\Leftrightarrow \exists y_1 \forall y_2 \dots \exists y_k(x, y_1, \dots, y_k) \in R \\ x \in B &\Leftrightarrow \exists z_1 \forall z_2 \dots \exists z_k(x, z_1, \dots, z_k) \in Q \\ x \in A \cap B &\Leftrightarrow (\exists y_1 \forall y_2 \dots \exists y_k(x, y_1, \dots, y_k) \in R) \vee (\exists z_1 \forall z_2 \dots \exists z_k(x, z_1, \dots, z_k) \in Q) \Leftrightarrow \\ &\quad \exists(y_1, z_1) \forall(y_2, z_2) \dots \exists(y_k, z_k)((x, y_1, \dots, y_k) \in R \wedge (x, z_1, \dots, z_k) \in Q), \end{aligned}$$

что является разрешимым свойством следующего кортежа: $((x, (y_1, z_1), \dots, (y_k, z_k)))$.
Значит, $A \cap B \in \Sigma_k$. Для объединения аналогично.

8.11 Дополнение языка из Σ_k лежит в Π_k , и наоборот.

Докажем, что дополнение языка из Σ_k лежит в Π_k , обратное утверждение доказывается аналогично. По определению, множество A принадлежит классу Σ_n , если существует такое разрешимое множество $R \in \mathbb{N}^{k+1}$, что

$$x \in A \Leftrightarrow \exists y_1 \forall y_2 \exists y_3 \dots Q y_n[(x, y_1, \dots, y_k) \in R].$$

Рассмотрим дополнение \bar{A} к множеству A . Возьмем отрицание условия из определения:

$$x \in \bar{A} \Leftrightarrow \forall y_1 \exists y_2 \forall y_3 \dots \bar{Q} y_n[(x, y_1, \dots, y_k) \in \bar{R}].$$

Так как дополнение разрешимого множества разрешимо, то \bar{R} разрешимо, значит мы получили, что \bar{A} принадлежит классу Π_k по определению, что и требовалось.

8.12 Пример λ -терма, к которому можно применить β -редукцию только после α -конверсии.

$$(\lambda x y. x) y \xRightarrow{\alpha} (\lambda x t. x) y \xRightarrow{\beta} \lambda t. y$$

8.13 Пример λ -терма, не имеющего нормальной формы

$$(\lambda x. x x)(\lambda x. x x)$$

8.14 Построение комбинаторов сложения и умножения для нумералов Чёрча (с доказательством корректности).

Add – сложение.

$$\begin{aligned} Add \ \overline{m} \overline{n} &= (\lambda m n f x. m f(n f x)) \overline{m} \overline{n} = (\lambda n f x. \overline{m} f(n f x)) \overline{n} = (\lambda n f x. (\lambda g y. \underbrace{g(g \dots (g y) \dots)}_m) f(n f x)) \overline{n} = \\ &= (\lambda n f x. (\lambda y. \underbrace{f(f \dots (f y) \dots)}_m)(n f x)) \overline{n} = \lambda f x. (\lambda y. \underbrace{f(f \dots (f y) \dots)}_m)(\overline{n} f x) = \\ &= \lambda f x. (\lambda y. \underbrace{f(f \dots (f y) \dots)}_m)(\lambda g t. \underbrace{g(g \dots (g t) \dots)}_n) f x = \lambda f x. (\lambda y. \underbrace{f(f \dots (f y) \dots)}_m)(\underbrace{f(f \dots (f x) \dots)}_n) = \end{aligned}$$

$$\lambda f x. \underbrace{(f(f \dots (f x) \dots))}_{m+n} = \overline{m} + \overline{n}.$$

Mult – умножение:

$$\begin{aligned} Mult \ \overline{m} \overline{n} &= (\lambda m n f x. m(n f) x) \overline{m} \overline{n} = (\lambda n f x. \overline{m}(n f) x) \overline{n} = (\lambda n f x. (\lambda g y. \underbrace{g(g \dots (g y) \dots))}_m)(n f) x \overline{n} \\ &= \lambda f x. (\lambda g y. \underbrace{g(g \dots (g y) \dots))}_m)(\overline{n} f) x = \lambda f x. (\lambda y. \underbrace{\overline{n} f(\overline{n} f \dots (\overline{n} f y) \dots))}_m) x = \\ &\lambda f x. (\lambda y. \overline{n} f(\overline{n} f \dots \overline{n} f(\lambda g t_1. \underbrace{g(g \dots (g t_1) \dots))}_n) f y) \dots) x \\ &= \lambda f x. (\lambda y. \underbrace{\overline{n} f(\overline{n} f \dots \overline{n} f(\underbrace{f(f \dots (f y) \dots))}_m) \dots)}_{m-1} \dots) x = \lambda f x. (\lambda y. \underbrace{\overline{n} f(\overline{n} f \dots \overline{n} f}_{m-2}(\underbrace{f(f \dots (f y) \dots)}_{n+n})) \dots) x = \\ &\dots = \\ &\lambda f x. (\lambda y. \underbrace{(f(f \dots (f y) \dots))}_{n*m} \dots) x = \lambda f x. \underbrace{f(f \dots (f x) \dots)}_{n*m} = \overline{m} * \overline{n}. \end{aligned}$$

9 Вопросы из билетов

9.1 Моделирование машины Тьюринга с несколькими лентами на машине Тьюринга с одной лентой.

Машина Тьюринга (МТ) состоит из:

- бесконечной в две стороны ленты, в ячейках которой могут быть записаны символы алфавита A (некоторого конечного множества);
- головки, которая может двигаться вдоль ленты, обозревая в каждый данный момент времени одну из ячеек;
- оперативной памяти, которая имеет конечный размер (другими словами, состояние оперативной памяти — это элемент некоторого конечного множества, которое называется множеством состояний МТ Q);
- таблицы переходов (или программы), которая задаёт функцию.

У **многоленточных** машин не одна лента, а несколько (фиксированное число для конкретной машины). На каждой ленте есть своя головка. За такт работы головки могут перемещаться по всем лентам. Действие на такте работы зависит как от состояния машины, так и от всего набора символов, которые видят головки машины на всех лентах.

Чтобы задать машину с h лентами, нужно указать:

- алфавит A , в котором выделен пустой символ Λ ;
- множество состояний Q , в котором выделено начальное состояние q_0 ;
- таблицу переходов, которая теперь является функцией вида $\delta : A^h \times Q \rightarrow A^h \times Q \times \{-1, 0, +1\}^h$ (первый аргумент — символы, которые машина видит на ленте; последний — команды движения для головок на каждой ленте);
- выделить среди лент ленту входа и ленту результата (возможно, что это одна и та же лента).

h -МТ M **вычисляет** функцию $f : B^* \rightarrow B^*$ (где B — подмножество алфавита машины, не содержащее пустого символа), если для каждого w из области определения функции f результат работы M равен $f(w)$, а для каждого w не из области определения f машина M не останавливается на входе w .

Любая функция, вычисляемая на многоленточной МТ, вычислима и на одноленточной машине.

Докажем, построив для произвольной h -МТ искомую одноленточную. Если описывать конфигурации h -МТ M_h в виде матрицы конфигурации размера $h \times N$, то каждый столбец такой матрицы может находиться в конечном числе состояний: не более $(A \cdot (Q + 1))^h$, где A — размер алфавита, а Q — количество состояний.

Моделирующая машина M_1 использует расширенный алфавит из $A + (A \cdot (Q + 1))^h$ (пустой символ и символы, отвечающие различным столбцам матрицы конфигурации). Она поддерживает описание матрицы конфигурации машины M_h в этом алфавите и изменяет его, моделируя работу M_h по тактам.

Поскольку действия M_h на каждом такте работы зависят от её состояния и символов под головками на каждой ленте, машина M_1 поддерживает также и эту информацию, записывая её в «оперативную память». Т.е. состояния M_1 представляются парами («управляющее состояние», «оперативная память»).

Такт работы машины M_h моделируется машиной M_1 в два этапа. На первом этапе машина M_1 просматривает все непустые ячейки на своей ленте слева направо и определяет, какие символы расположены под текущими положениями головок машины M_h .

На втором этапе M_1 изменяет содержимое своей ленты в соответствии с таблицей переходов машины M_h .

Более детальное описание устройства M_1 :

- Алфавит машины M_1 — $A' = A \cup (A \times (Q \cup \Lambda))^h$;
- Пустой символ тот же, что и у моделируемой машины M_h ;
- Машина M_1 является последовательным соединением трёх машин: M_s , M_w , M_f .

1. M_s . Первая машина M_s подготавливает содержимое ленты к двухэтапному моделированию тактов работы машины M_h . Машина M_s просматривает ячейки входного слова. Первый символ a_1 она заменяет на $((a_1, q_0), (\Lambda, q_0), \dots, (\Lambda, q_0))$ (это первый столбец матрицы начальной конфигурации M_h), а каждый последующий символ входа a на $((a, \Lambda), (\Lambda, \Lambda), \dots, (\Lambda, \Lambda))$ (это остальные столбцы матрицы начальной конфигурации — напомним, что в начальной конфигурации все ленты, кроме входной, пусты). Обнаружив пустой символ Λ , машина M_s возвращается в крайнее левое положение и останавливается.

2. M_w . Вторая машина M_w моделирует такты работы M_h описанным выше способом. Она проходит непустые ячейки ленты два раза. При движении слева направо машина M_w «запоминает» символы под головками машины M_h по следующему правилу: если в очередном столбце матрицы конфигурации машины M_h на i -й позиции находится пара (a, q) , $q \in Q$, то i -я головка расположена над символом a . К концу первого прохода в оперативной памяти M_w содержится полная информация о символах под головками и состоянии M_h , что однозначно определяет строчку таблицы переходов M_h , которую нужно применить на данном такте. Если такой строчки нет, то M_w заканчивает работу.

На втором проходе найденная строчка таблицы переходов M_h используется для обновления матрицы конфигурации. Информация о символах на лентах M_h обновляется по следующему правилу: если в очередном столбце матрицы конфигурации машины M_h на i -й позиции находится пара (a, q) , $q \in Q$, то столбец меняется так, чтобы в этой позиции было написано пара (a', q) , где a' — символ, который M_h записывает на i -ую ленту. Те пары в столбце, которые соответствуют ячейкам, над которыми нет головки, не изменяются.

Кроме того, нужно обновить информацию о положениях головок соответственно текущей команде движения. Для этого машина M_w переписывает вторые компоненты пар, из которых состоит столбец матрицы конфигурации M_h (т.е. текущий столбец матрицы). Движение по каждой ленте может быть как влево, так и вправо. Поэтому для выполнения этого действия M_w перемещается из текущего положения на шаг вправо, записывая в этот столбец новые положения головок, и на шаг влево, выполняя аналогичное действие. При выполнении этих действий машина M_w может выйти за пределы рабочей зоны (матрицы конфигурации). Тогда она оказывается над пустым символом, который заменяется на подходящий столбец, описывающий пустые символы и положения головок машины M_h .

3. M_f . По завершении работы M_w начинает работу третья машина M_f , которая восстанавливает на ленте состояние ленты результата машины M_h . Она проходит по всем ячейкам рабочей зоны и заменяет столбец матрицы конфигурации на символ из алфавита A машины M_h , если головка M_h на ленте результата не находится в этом столбце. Затем она возвращается в ту ячейку, которая соответствует положению головки на ленте результата машины M_h , и производит ту же замену. После этого M_f останавливается с чувством выполненного долга.

9.2 Эквивалентность следующих утверждений: множество перечислимо, полухарактеристическая функция множества вычислима, множество является областью определения вычислимой функции, множество является проекцией разрешимого множества пар.

Теорема. Следующие утверждения для непустого $S \subset \mathbb{N}$ эквивалентны:

1) S перечислимо (существует печатающая машина, такая, что $\forall x \in S$ x встречается в потоке вывода, $\forall x \notin S$ x не встречается в потоке вывода);

2) Полухарактеристическая функция множества (равная 0 на элементах S и не определённая вне S) вычислима;

3) S - область определения вычислимой функции (если существует алгоритм, её вычисляющий, то есть такой алгоритм A , что $\forall f(n)$ определённых для некоторого n алгоритм A остановится на входе n и напечатает $f(n)$, иначе - не остановится на входе n);

4) S - проекция разрешимого (существует алгоритм, который по любому натуральному n определяет, принадлежит ли оно множеству) множества пар.

▲ (1) \Rightarrow (2). Запускаем эту печатающую машину. Если она выдаёт x , то значение полухарактеристической функции 1, иначе - \perp .

(2) \Rightarrow (3). S - область определения характеристической функции, описанной ранее.

(3) \Rightarrow (1). Пусть S - область определения вычислимой функции f , вычисляемой алгоритмом B . Тогда есть алгоритм, перечисляющий A : параллельно запускать B на входах $0, 1, 2, \dots$, делая всё больше шагов (1 шаг на входах 0 и 1 , 2 шага - на входах $0, 1, 2$, и т.д.); напечатать все номера, на которых B остановился.

(1) \Rightarrow (4). $S = \{x | \exists n(x, n) \in B\}$ - проекция множества $B = \{(x, n) : x \text{ в первых } n \text{ шагах алгоритма, перечисляющего } S\}$

(4) \Rightarrow (1). for ($x=0$; $++x$)
for ($y=0$; $y \leq x$; $++y$)
 {if($(x, y) \in B$) cout << x ;
 if($(y, x) \in B$) cout << y ; } ■

9.3 Теорема Поста: критерий разрешимости в терминах перечислимости множества и его дополнения.

Теорема: A разрешимо $\Leftrightarrow A$ и \bar{A} перечислимы

▲ \Rightarrow : A можно перечислить даже по возрастанию. Запустим цикл по $n = 0, 1, \dots$. Если $n \in A$ (вычислимо по определению разрешимого множества), то выводим n . Дополнение разрешимого множества также разрешимо (возьмем характеристическую функцию A и поменяем местами значения 0 и 1), поэтому оно тоже перечислимо

\Leftarrow : Покажем как построить характеристическую функцию для A . Запускаем цикл по $n = 1, 2, \dots$

1. Возвращаем 1, если x было перечислено в A на n -ом шаге
2. Возвращаем 0, если x было перечислено в \bar{A} на n -ом шаге

Для любого x что-то будет выведено, так как оно лежит либо в A , либо в \bar{A} и в силу их перечислимости будет перечислено на каком-то шаге $\Rightarrow A$ - разрешимо ■

9.4 Неразрешимость проблем самоприменимости и остановки.

Пусть U - универсальная вычислимая функция

Проблема самоприменимости: по входу p нужно понять, определено ли $U(p, p)$.

Утверждение: это неразрешимая проблема, т.е. множество $\{p | U(p, p) \text{ определено}\}$ неразрешимо.

▲ Предположим, что это множество разрешимо. Тогда вычислима функция

$$d'(x) = \begin{cases} U(x, x) + 1 & U(x, x) \text{ определено} \\ 1 & U(x, x) \text{ не определено} \end{cases}$$

Тогда так как d' вычислима, то по определению $U \exists p \forall x d'(x) = U(p, x)$. Рассмотрим $U(p, p)$. Предположим, что она определена, тогда $U(p, p) = d'(p) = U(p, p) + 1$ - противоречие. Если предположим, что она не определена, получим $U(p, p) = d'(p) = 1$ - тоже противоречие \Rightarrow это множество неразрешимо ■

Лемма: Область определения вычислимой функции перечислима

▲ Построим полухарактеристическую функцию. Запустим $f(x)$ и если оно остановится, вернем 1. Это и будет полухарактеристической функцией области определения (1 - если $f(x)$ определена, \perp - если не определена) \Rightarrow область определения перечислима ■

Замечание: Множество из проблемы самоприменимости перечислимо, как область определения вычислимой функции $d(x) = U(x, x)$

Проблема остановки (останова): по входу (p, k) нужно понять, определено ли $U(p, k)$.

Утверждение: эта проблема тоже неразрешима

▲ Пусть это не так и проблема разрешима. Тогда бы разрешима проблема самоприменимости, так как она является частным случаем проблемы остановки (при $k = p$). Получили противоречие \Rightarrow эта проблема неразрешима ■

9.5 Несуществование универсальной totally вычислимой функции.

Определение: $U : \{0,1\}^* \times \{0,1\}^* \Rightarrow \{0,1\}^*$ называется *универсальной totally вычислимой функцией*, если

1. U вычислима и всюду определена
2. Если f — всюду определённая вычислимая функция одного аргумента, то $\exists p \forall x U(p, x) = f(x)$

Теорема: Универсальной totally вычислимой функции не существует

▲ Предположим, что такая функция существует. Тогда рассмотрим функцию $d(x) = U(x, x)$ - всюду определена и вычислима. Тогда функция $d'(x) = U(x, x) + 1$ также всюду определена и вычислима. Значит, по определению универсальной totally вычислимой функции $\exists p \forall x U(p, x) = d'(x)$. Рассмотрим $U(p, p) = d'(p) = U(p, p) + 1$ - противоречие \Rightarrow такой функции не существует ■

Замечание: Для обычных универсальных вычислимых функций такого противоречие не возникает, так как равенство $U(p, p) = U(p, p) + 1$ верно, если $U(p, p)$ не определена

9.6 Неперечислимость и некоперечислимость множества всюду определённых программ или множества программ с конечной областью определения (на выбор).

▲ Пусть это множество перечислимо (обозначим его как A). Решим с его помощью проблему самоприменимости (см. билет 3.4). Пусть F - исследуемая функция, имеющая номер n в какой-то главной универсальной вычислимой функции. Тогда

$$F'(x) = \begin{cases} x & \text{если } F(n) \text{ не завершилось за } x \text{ шагов} \\ \perp & \text{иначе не определена} \end{cases}$$

Значит F' всюду определена $\Leftrightarrow F(n)$ не останавливается. Пусть F' имеет номер m . Тогда:

1. Запустить и сразу остановить $F(n)$
2. Прodelать ещё 1 шаг в работе $F(n)$. Если $F(n)$ остановилось, вывести 1
3. Вывести перечисляющем алгоритмом ещё один элемент множества A . Если он равен m (то есть $F'(x) \in A$, а значит всюду определена) вывести 0
4. Вернуться ко второму шагу

Так как F или самоприменима, или несамоприменима (ее номер либо лежит в множестве из проблемы самоприменимости, либо нет), то или 1 или 2 шаг когданибудь выведет результат, значит проблема самоприменимости решена, противоречие.

Коперечислимость решается аналогично, только $F'(x) = F(n)$ (получается F' не всюду определена (то есть лежит в дополнении к A) $\Leftrightarrow F(n)$ не останавливается). Нам остается только заменить в нашем алгоритме третий шаг: будем перечислять \bar{A} . ■

9.7 Существование главной универсальной вычислимой функции.

Теорема 1: Существует вычислимая функция двух аргументов, являющаяся универсальной функцией для класса вычислимых функций одного аргумента.

▲ Запишем все программы, вычисляющие функции одного аргумента, в вычислимую последовательность p_0, p_1, \dots (например, в порядке возрастания их длины). Положим $U(i, x)$ равным результату работы i -ой программы на входе x . Тогда функция U и будет искомой вычислимой универсальной функцией. ■

Теорема 2: Существует главная универсальная функция.

▲ Заметим сначала, что существует вычислимая функция трёх аргументов, универсальная для класса вычислимых функций двух аргументов, то есть такая функция T , что при фиксации первого аргумента среди функций $T_n(u, v) = T(n, u, v)$ встречаются все вычислимые функции двух аргументов.

Такую функцию можно построить так. Фиксируем некоторую вычислимую нумерацию пар, то есть вычислимое взаимно однозначное соответствие $(u, v) \leftrightarrow [u, v]$ между $\mathbb{N} \times \mathbb{N}$ и \mathbb{N} ; число $[u, v]$, соответствующее паре (u, v) , мы будем называть номером этой пары.

Если теперь R — двуместная вычислимая универсальная функция для вычислимых одноместных функций (существует по теореме 1), то вычислимая функция T , определённая формулой $T(n, u, v) = R(n, [u, v])$, будет универсальной для вычислимых двуместных функций. В самом деле, пусть F — произвольная вычислимая функция двух аргументов. Рассмотрим вычислимую одноместную функцию f , определённую соотношением $f([u, v]) = F(u, v)$. Поскольку R универсальна, найдётся число n , для которого $R(n, x) = f(x)$ при всех x . Для этого n выполнены равенства $T(n, u, v) = R(n, [u, v]) = f([u, v]) = F(u, v)$. Итак, универсальная функция трёх аргументов построена.

Теперь используем её для определения главной универсальной функции U двух аргументов. Положим $U([n, u], v) = T(n, u, v)$ и проверим, что функция U будет главной. Для любой вычислимой функции V двух аргументов можно найти такое n , что $V(u, v) = T(n, u, v)$ (так как T — универсальна) для всех u и v . Тогда $V(u, v) = U([n, u], v)$ для всех u и v и потому функция s , определённая формулой $s(u) = [n, u]$, удовлетворяет требованиям из определения главной универсальной функции. ■

9.8 Теорема Райса–Успенского о неразрешимости нетривиальных свойств вычислимых функций.

Теорема Райса–Успенского: Пусть $A \subset \mathcal{F}$ — произвольное нетривиальное свойство вычислимых функций (нетривиальность означает, что есть как функции, ему удовлетворяющие, так и функции, ему не удовлетворяющие, то есть что множество A непусто и не совпадает со всем \mathcal{F}). Пусть U — главная универсальная функция. Тогда не существует алгоритма, который по U -номеру вычислимой функции проверял бы, обладает ли она свойством A . Другими словами, множество $S_A = \{n | U_n \in A\}$ неразрешимо.

▲ Пусть $\zeta(x)$ — нигде не определённая функция. Без ограничения общности $\zeta \in \bar{A}$ (иначе получим неразрешимость \bar{A} , которая влечёт неразрешимость A)

Пусть $\xi(x)$ — какая-то функция из A . Пусть K — какое-то перечислимое неразрешимое множество (например, из проблемы самоприменимости)

Рассмотрим

$$V(n, x) = \begin{cases} \xi(x) & n \in K \\ \zeta(x) & n \in \bar{K} \end{cases}$$

Тогда V — вычислимая функция. Программа, вычисляющая V : запустить перечисление K , ожидать появления n . Если появилось, вернуть $\xi(x)$.

По определению главной универсальной вычислимой функции (ГУВФ) существует всюду определённая s , такая что $\forall n \forall x V(n, x) = U(s(n), x)$

1. Если $n \in K$, то $V(n, x) = \xi(x) = U(s(n), x) \Rightarrow s(n)$ — номер функции из A
2. Если $n \in \bar{K}$, то $U(s(n), x) = \zeta(x)$, т.е. $s(n)$ — номер функции из \bar{A} .

Получаем $n \in K \Leftrightarrow s(n) \in S_a$. При этом s вычислима и всюду определена, так что ситуация подходит под определение m -сводимости (см. определения) $\Rightarrow K \leq_m S_a$. Так как K неразрешимо, то и S_a неразрешимо ■

9.9 Теорема Клини о неподвижной точке. Построение программы, на любом входе печатающей некоторый собственный номер.

Теорема Клини о неподвижной точке: Пусть U — ГУВФ, h — всюду определённая вычислимая функция. Тогда существует p , т.ч. при всех x верно $U(p, x) = U(h(p), x)$

▲ Пусть $V(x, y) := U(U(x, x), y)$. В силу главности U существует вычислимая всюду определённая s , такая что $\forall x, y V(x, y) = U(s(x), y)$.

Рассмотрим $t(x) = h(s(x))$ — вычислима и всюду определена как композиция вычислимых всюду определённых. Значит $\exists p \forall x t(x) = U(p, x)$. Тогда

$$\begin{aligned} U(s(p), y) &= V(p, y) = U(U(p, p), y) = U(t(p), y) = U(h(s(p)), y) \Rightarrow U(s(p), y) = U(h(s(p)), y) \Rightarrow \\ &\Rightarrow s(p) - \text{неподвижная точка} \blacksquare \end{aligned}$$

Замечание: в условии некоторый собственный номер означает какой-то свой номер в ГУВФ (какой-то так как у каждой функции бесконечное количество номеров)

Утверждение: Пусть $U(n, x)$ — главная вычислимая универсальная функция для класса всех вычислимых функций одного аргумента. Тогда существует такое число p , что $U(p, x) = p$ для любого x .

▲ Рассмотрим $V(n, x) = n$. Так как U — ГУВФ, то существует вычислимая всюду определённая функция s такая что $U(s(n), x) = V(n, x)$. Тогда по теореме Клини о неподвижной точке существует p такое что $\forall x U(p, x) = U(s(p), x) = V(p, x) = p$ ■

9.10 Теорема об арифметической иерархии: $\Sigma_n \neq \Sigma_{n+1}, \Sigma_n \neq \Pi_n$.

Опр *Классы арифметической иерархии*

Говорят, что множество A принадлежит классу Σ_n , если существует такое разрешимое множество $R \in \mathbb{N}^{k+1}$, что

$$x \in A \iff \exists y_1 \forall y_2 \exists y_3 \dots Q y_n [(x, y_1, \dots, y_k) \in R]$$

Аналогично, говорят, что A принадлежит классу Π_n , если существует такое разрешимое множество $R \in \mathbb{N}^{k+1}$, что

$$x \in A \iff \forall y_1 \exists y_2 \forall y_3 \dots Q y_n [(x, y_1, \dots, y_k) \in R]$$

Согласно этому определению, $\Sigma_0 = \Pi_0$ (классы Σ_0 и Π_0 совпадают с классом всех разрешимых множеств)

Σ_1 - перечислимые, Π_1 - коперечислимые

Теорема 1. Для любого n в классе Σ_n существует множество, универсальное для всех множеств класса Σ_n . (Его дополнение будет универсальным в классе Π_n .)

Говоря о дополнении к Π_n , Σ_n множеству, мы имеем в виду дополнение из множества всех множеств, выражаемых через n предикатов.

Говоря об универсальном множестве из класса Σ_n , мы имеем в виду множество пар натуральных чисел, которое принадлежит классу Σ_n и среди сечений которого встречаются все множества натуральных чисел, принадлежащие классу Σ_n .

▲ Для класса Σ_1 (перечислимых множеств) существование универсального множества мы уже обсуждали (билет 3.extra6.1). С его помощью можно построить универсальные множества и для более высоких классов иерархии. (Начинать надо с первого уровня, так как на «нулевом» уровне не существует универсального разрешимого множества.)

По определению свойства класса Π_2 имеют вид $\forall y \exists z R(x, y, z)$, где R — некоторое разрешимое свойство. Но их можно эквивалентно определить и как свойства вида $\forall y P(x, y)$, где P — некоторое перечислимое свойство. Теперь уже видно, как построить универсальное множество класса Π_2 . Возьмём универсальное перечислимое свойство $U(n, x, y)$, из которого фиксацией различных n получаются все перечислимые свойства пар натуральных чисел. Тогда из свойства $T(n, x) = \forall y U(n, x, y)$ при различных натуральных n получаются все Π_2 -свойства натуральных чисел. С другой стороны, само свойство T по построению принадлежит классу Π_2 .

Дополнение к универсальному Π_2 -множеству будет, очевидно, универсальным Σ_2 -множеством — так как отрицание чего-либо меняет все кванторы на противоположные, благодаря чему и само множество, и все его сечения по такому свойству также принадлежат Σ_2 — значит, это универсальное Σ_2 -множество.

Аналогично можно действовать и для Σ_n - и Π_n -множеств. ■

Теорема 2. Универсальное Σ_n -множество не принадлежит классу Π_n . Аналогичным образом, универсальное Π_n -множество не принадлежит классу Σ_n .

▲ Рассмотрим универсальное Σ_n -свойство $T(m, x)$. По определению это означает, что среди его сечений (получающихся, если зафиксировать m) есть все Σ_n -свойства. Пусть T принадлежит классу Π_n . Тогда его диагональ, свойство $D(x) = T(x, x)$, также лежит в Π_n (например, потому, что $D \leq_m T$), а её отрицание, свойство $\neg D(x)$, принадлежит классу Σ_n . Но этого не может быть, так как $\neg D$ отлично от всех сечений свойства T (оно отличается от m -го сечения в точке m), а T универсально. ■

Если $\Sigma_n = \Sigma_{n+1}$, то $\Pi_{n+1} = \Pi_n$ (как отрицание Σ_n и Σ_{n+1}). Т.к. $\Sigma_n \subset \Pi_{n+1} = \Pi_n$, а $\Pi_n \subset \Sigma_{n+1} = \Sigma_n$, то $\Sigma_{n+1} = \Pi_{n+1}$, что противоречит теореме выше. Основная теорема доказана.

9.11 Теорема Чёрча-Россера (б/д). Единственность нормальной формы.

Теорема 9.1 (Чёрча-Россера (б/д)). Если для некоторого λ -терма A имеется два варианта редукции $A \rightarrow B$ и $A \rightarrow C$, то существует такой λ -терм D , что $B \rightarrow D$ и $C \rightarrow D$.

Определение 9.1. Термы M и N называются равными, если существует такой терм T , что M сводится (некоторым количеством α и β редукций) к T и N сводится к T .

Определение 9.2. Говорят, что терм M находится в нормальной форме, если к нему нельзя применить β -редукцию даже после нескольких α -конверсий.

Говорят, что N — нормальная форма терма M , если $M = N$ и N в нормальной форме.

Следствие 1 (из теоремы Чёрча-Россера). У каждого λ -терма есть не более одной нормальной формы.

Доказательство. Предположим, что у терма A две нормальные формы: B и C (то есть $A \rightarrow B$ и $A \rightarrow C$). По теореме Чёрча-Россера существует такой D , что $B \rightarrow D$ и $C \rightarrow D$. Но по определению B и C – λ -термы, к которым нельзя применить β -редукцию. Противоречие. \square

Замечание. Не у всех λ -термов есть нормальная форма. Например, $\Omega = (\lambda x.xx)(\lambda x.xx)$ редуцируется сам в себя.

9.12 Построение комбинаторов логических значений, булевых функций, операций с парами, проверки на ноль для нумералов Чёрча (с доказательством корректности).

Определение 9.3. *Комбинатором* называется замкнутый λ -терм (без свободных переменных).

Представление логических значений и булевых функций

Пусть

$$False = \lambda xy.y (= \bar{0})$$

$$True = \lambda xy.x$$

Получается, что

$$True M N = M$$

$$False M N = N$$

Тогда логические функции выражаются следующим образом:

$$And = \lambda pq.pqp$$

$$Or = \lambda pq.ppq$$

$$Not = \lambda p.p False True$$

Доказательство. *

$$1) And = \lambda pq.pqp$$

Если $p = 0$, то $p \wedge q = 0 = p$

Если $p = 1$, то $p \wedge q = q$

$$2) Or = \lambda pq.ppq$$

Если $p = 0$, то $p \vee q = q$

Если $p = 1$, то $p \vee q = 1 = p$

$$3) Not = \lambda p.p False True$$

Если $p = False$, то $False False True = True$ Если $p = True$, то $True False True = False$ \square

Представление арифметических операций на нумералах Чёрча

1) Inc – прибавление единицы ($Inc \bar{n} = \overline{n+1}$)

$$Inc = \lambda nfx.f(nfx)$$

Доказательство. $Inc \bar{n} = (\lambda nfx.f(nfx))\bar{n} = \lambda fx.f(\bar{n}fx) = \lambda fx.f(\lambda gy.\underbrace{g(g(g(\dots)))}_{n \text{ раз}})fx) =$

$$\lambda fx.\underbrace{f(f(f(\dots(f(fx))\dots)))}_{n+1 \text{ раз}} = \overline{n+1} \quad \square$$

2) *Add* – сложение

$$Add = \lambda mnfx.mf(nfx)$$

Доказательство. *

$$Add \bar{m} \bar{n} = (\lambda mnfx.mf(nfx)) \bar{m} \bar{n} = \lambda fx.\bar{m}f(\bar{n}fx) = \lambda fx.(\underbrace{\lambda gy.g(g(g(...)))}_{m\text{раз}})\underbrace{f(f(f(...)))}_{n\text{раз}} = \lambda fx.\underbrace{f(f(f(...)))}_{m+n\text{раз}} = \overline{m+n} \quad \square$$

3) *Mult* – умножение

$$Mult = \lambda mnfx.m(nf)x$$

Доказательство аналогично.

Проверка на ноль для нумералов Чёрча

$$IsZero = \lambda n.n(\lambda x.False)True$$

Проверим для нуля:

$$IsZero\bar{0} = \bar{0}(\lambda x.False)True = True$$

Любое число, кроме нуля представимо в виде: $\overline{n+1}$. Проверим *IsZero* для таких чисел:

$$IsZero(\overline{n+1}) = \overline{n+1}(\lambda x.False)True = (\lambda fx.f(...))(\lambda x.False)True = ((\lambda x.False)(...)) = False$$