1. Логика и арифметика

1.0 Определения

1) Булевы функции, примеры. Двойственность.

Определение: Булевая функция от n аргументов - это функция $f : \{0,1\}^n \to \{0,1\}$.

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: Булевая функция f^* называется двойственной булевой функции f, если она получена из f инвверсией всех аргументов и самой функции, то есть
$f^*(x_1, \ldots, x_n) = \neg f(\neg x_1, \ldots, \neg x_n)$

		AND	OR	XOR	Импл.	Эквив.	Штрих Шеффера	Стрелка Пирса	f^*
a	b	$a \wedge b$	$a \vee b$	$a \oplus b$	$a \to b$	$a \Leftrightarrow b$	$a \mid b$	$a \downarrow b$	$\neg(\neg a \downarrow \neg b)$
0	0	0	0	0	1	1	1	1	1
0	1	0	1	1	1	0	1	0	1
1	0	0	1	1	0	0	1	0	1
1	1	1	1	0	1	1	0	0	0

2) Классы булевых функций

- Класс T_0 функций, сохраняющих 0: $f \in T_0$, если $f(0, \ldots, 0) = 0$
  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 $f(1, \ldots, 1) = 1$
  Принадлежат: $1,\ id,\ a \wedge b,\ a \vee b,\ a \to b,\ a \Leftrightarrow b$
  Не принадлежат: $0,\ \neg a$

- Класс M монотонных функций: $f \in M$, если $\forall i(a_i \leqslant b_i) \Rightarrow f(a_1, \ldots, a_n) \leqslant f(b_1, \ldots, b_n)$
  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 $f(\overline{x_1}, \ldots, \overline{x_n}) = \overline{f(x_1, \ldots, x_n)}$
  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 $f(x_1, \ldots, x_n) = a_0 \oplus a_1 x_1 \oplus \cdots \oplus a_n x_n, a_i \in \{0,1\}$
  Принадлежат: $0,\ 1,\ id,\ \neg a,\ a \Leftrightarrow b,\ a \oplus b$
  Не принадлежат: $a \wedge b$

3) Пропозициональные формулы, КНФ и ДНФ

Построение формул:

1. Переменная – это формула
2. ϕ – формула $\Rightarrow\ \neg\phi$ – формула
3. ϕ, ψ – формулы $\Rightarrow\ (\phi \vee \psi), (\phi \wedge \psi), (\phi \to \psi)$ – формулы

Определение: $[\phi](a_1, \ldots, a_n)$ – значение формулы на наборе $\bar{a}(a_1, \ldots, a_n)$

1. $[p_i](\bar{a}) = a_i$

2. $[\neg\phi](\bar{a}) = neg([\phi](\bar{a}))$

3. $[\phi \wedge \psi](\bar{a}) = and([\phi](\bar{a}), [\psi](\bar{a}))$ и аналогично с $or, impl$

Определение: Литерал – переменная/формула вида $\neg p$, где p - переменная
Определение: Конъюнкт – конъюнкция литералов ($\wedge$)
Определение: Дизъюнкт – дизъюнкция литералов ($\vee$)
Определение: КНФ – конъюнкция дизъюнктов - $f(x, y, z) = (x \vee y) \wedge (y \vee \neg z)$
Определение: ДНФ – дизъюнкция конъюнктов - $f(x, y, z) = (x \wedge y) \vee (\neg y \wedge \neg z)$
Определение: Тавтология – формула, истинная при всех значениях входящих в нее переменных. Например, $((p \wedge q) \to p)$.
Важные функции: 1) $a \vee \neg a \equiv 1$ 2) $a \wedge \neg a \equiv 0$

СКНФ/СДНФ (Совершенные):

1. в ней нет одинаковых простых дизъюнкций (у СКНФ) и конъюнкций (у СДНФ);

2. каждая простая дизъюнкция (у СКНФ) и конъюнкция (у СДНФ) полная.

Например, 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.

4) Многочлены Жегалкина

Определение: Многочленом Жегалкина называется полином с коэффициентами вида 0 и 1, где в качестве произведения берётся конъюнкция, а в качестве сложения исключающее или: $P = a_{000\ldots000} \oplus a_{100\ldots0} x_1 \oplus a_{010\ldots0} x_2 \oplus \dots \oplus a_{00\ldots01} x_n \oplus a_{110\ldots0} x_1 x_2 \oplus \dots \oplus a_{00\ldots011} x_{n-1} x_n \oplus \dots \oplus a_{11\ldots1} x_1 \ldots x_n$
Базовые функции: а) $\neg p = p \oplus 1$ б) $p \vee q = p \oplus q \oplus pq$
в) $p \wedge q = pq$ в) $p \to q = 1 \oplus p \oplus pq$
Вычитание и сложение по сути одно и то же, поскольку все вычисления проходят по mod 2.

5) Аксиомы исчисления высказываний, modus ponens

Теорема (корректности): Любая выводимая формула есть тавтология.
Теорема (полноты): Любая тавтология выводима.
Одним из возможных вариантов (гильбертовской) аксиоматизации логики высказываний является следующая система аксиом:
$A_1 : A \to (B \to A)$;
$A_2 : (A \to (B \to C)) \to ((A \to B) \to (A \to C))$;
$A_3 : A \wedge B \to A$;
$A_4 : A \wedge B \to B$;
$A_5 : A \to (B \to (A \wedge B))$;
$A_6 : A \to (A \vee B)$;
$A_7 : B \to (A \vee B)$;
$A_8 : (A \to C) \to ((B \to C) \to ((A \vee B) \to C))$;
$A_9 : \neg A \to (A \to B)$;
$A_{10} : (A \to B) \to ((A \to \neg B) \to \neg A)$;
$A_{11} : A \vee \neg A$.
вместе с единственным правилом: $\frac{A \quad A \to B}{B}$ (Modus ponens). Эта запись означает, что если выведены формулы A и $A \to B$, то можно вывести B.

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: $\vdash \phi$.

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

1. $A \to B$	(аксиома 1)
2. $A \to (B \to A)$	(аксиома 1)
3. $(A \to (B \to A)) \to ((A \to B) \to (A \to A))$	(аксиома 2)
4. $(A \to B) \to (A \to A)$	(2,3, MP)
5. $A \to A$	(1,4, MP)

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.
Если в какой-то момент вывели $\perp$, то формула невыполнима.
Если нельзя применить правило резолюции так, чтобы получить новый дизъюнкт, а $\perp$ не выведен, то формула выполнима.

8) Языки первого порядка

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 $\sigma = \langle P_1, \ldots, P_k, f_1, \ldots, f_m \rangle$ – набор предикатных и функциональных символов, обозначающих те или иные связи между объектами.
  1. Предикат валентности N на множестве A – это функция $P : A^N \to \{0, 1\}$
     Предикатный символ — символ, обозначающий предикат.
     Например: $P^{(3)}, <^{(2)}, \subset^{(2)}, Prime^{(1)}$
  2. Функция валентности N на множестве A – это функция $f : A^N \to A$.
     Функциональный символ — символ алфавита, обозначающий функцию.
     Например: $f^{(3)}, +^{(2)}, \cap^{(2)}, sin^{(1)}$
     * При этом символы валентности ноль – это константы: $11, \pi, e, \varnothing$
- Символы логических операций: $\wedge, \vee, \neg, \to$
- Кванторы: $\forall, \exists$
- Служебные символы: скобки и запятые.

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

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

Определение: Атомарной формулой называется выражение вида $P^{(k)}(t_1, ..., t_k)$, где $k > 0$, $t_1, \ldots, t_k$ — 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 $(\phi \wedge \psi), (\phi \vee \psi), (\phi \to \psi), \phi$ также являются формулами;
3. Если ϕ является формулой, а x — индивидная переменная, то $x\phi$ и $\forall x\phi$ также являются формулами.

9) Интерпретация языка первого порядка, 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 $[P] : M^k \to \{0, 1\}$;
- для каждого k-местного функционального символа $f \in \sigma$ задана некоторая функция $[f] : M^k \to M$;

Определение: Оценкой переменных называется функция $\pi : Var \to M$, где Var — множество индивидных переменных.

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

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 $t = f(t_1, \ldots, t_k)$, то $[t](\pi) = [f]([t_1](\pi), \ldots, [t_k](\pi))$

Значение формулы также определяется рекурсивно.

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

* Если $\phi = \neg\psi$, то $[\phi](\pi) = not([\psi](\pi))$

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

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

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

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

Пример 1: Для любой формулы ϕ формулы $\forall x \forall y \phi \rightarrow \forall y \forall x \phi$ и $\exists x \exists y \phi \rightarrow \exists y \exists x \phi$

Пример 2: Для любой формулы ϕ формулы $\exists x \forall y \phi \rightarrow \forall y \exists x \phi$. Обратная импликация общезначима не всегда. Например, если некоторое блюдо попробовали все гости, то каждый гость попробовал хотя бы одно блюдо. Но если к каждому замку подходит некоторый ключ, это ещё не значит, что один из ключей подходит сразу ко всем замкам

10) Свободные и связные 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, а остальные переменные свободны. Более корректно говорить не о связанных и свободных переменных, а о связанных и свободных вхождениях переменных.

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

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

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

11) Выразимость предиката или функции в данной интерпретации.

Зафиксируем некоторую сигнатуру σ и ее интерпретацию с носителем M.

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

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

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

12) Аксиомы исчисления предикатов, правила Бернайса, правило обобщения.

Аксиомы исчисления предикатов:

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

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

Пример: Следствием из A_{12}, A_{13} является силлогизма: $\forall x\phi(x) \to \exists x\phi$

Правила вывода:

1. Modus ponens:
$$\frac{A \quad A \to B}{B}$$
2. 1-ое правило Бернайса:
$$\frac{\phi \to \psi}{\exists x\ \phi \to \psi}$$
3. 2-ое правило Бернайса:
$$\frac{\phi \to \psi}{\phi \to \forall x\ \psi}$$
4. Правило обобщения:
$$\frac{\phi}{\forall x\ \phi}$$

Пример Имеется формула:

$$\exists x\ \forall y\, \phi \ \to \ \forall y\ \exists x\, \phi.$$

Продемонстрируем ее вывод:

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

13) Аксиомы равенства.

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

1. $\forall x\ \ (x = x)$ – аксиома рефлексивности,
2. $\forall x \forall y\ \ \big((x = y) \to (y = x)\big)$ – аксиома симметричности,
3. $\forall x \forall y \forall z\ \ \big(\big((x = y) \wedge (y = z)\big) \to (x = z)\big)$ – 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:

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

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.

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.

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: $(\phi(0) \wedge \forall x(\phi(x) \rightarrow \phi(Sx))) \rightarrow \forall x \phi(x)$

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. $\forall x \forall y \ x \cdot Sy = x \cdot y + x$

16) Совместность, непротиворечивость, полнота теории.

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 $\neg\phi$, и непротиворечивой в противном случае.

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

Пример: Короткий 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. $\forall x \forall y\ (x=y \to Sx=Sy)$ – аксиома равенства
7. $SS0+0=SS0 \to S(SS0+0)=SSS0$ – 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.