Введение в математическую логику

Краткий конспект лекций

(весна 2005, мехмат МГУ, 1-й курс, 2-й поток)

Предварительный вариант (25.05.2005)

М. Р. Пентус

1 Введение

1.1 Предварительные сведения

1.1. В этом курсе нуль является натуральным числом. Множество всех натуральных чисел обозначается $\mathbb{N}$. Множество всех целых чисел обозначается $\mathbb{Z}$. Множество всех рациональных чисел обозначается $\mathbb{Q}$. Множество всех действительных чисел обозначается $\mathbb{R}$.

1.2. Натуральные числа будем обозначать буквами i, j, k, l, m, n (возможно, с индексами).

1.3. Множество A называется *счётным*, если существует биекция между A и $\mathbb{N}$.

1.4. *Принцип математической индукции* состоит в следующем: утверждение $A(x)$, зависящее от натурального параметра x, считается доказанным, если доказано $A(0)$ и для любого натурального числа n из предположения, что верно $A(n)$, выведено, что верно также $A(n+1)$.

Часто удобно пользоваться следующей эквивалентной формой принципа математической индукции, называемой иногда *принципом возвратной индукции*: утверждение $A(x)$, зависящее от натурального параметра x, считается доказанным, если для всякого натурального числа n из предположения, что $A(x)$ верно при любом натуральном $x < n$, следует, что $A(x)$ верно также при $x = n$.

1.5. Формула, начинающаяся с квантора существования по пустому множеству, ложна. Формула, начинающаяся с квантора всеобщности по пустому множеству, истинна.

1.2 Алфавит, буква, слово

[П1, 2.2], **[КД, с. 168]**, **[ЛМ, II.1]**

Определение 1.6. *Алфавитом* называется конечное непустое множество. Его элементы называются *символами* (*буквами*).

Определение 1.7. *Словом* (*цепочкой*, *строкой*)в алфавите Σ называется конечная последовательность элементов Σ.

Пример 1.8. Рассмотрим алфавит $\Sigma = \{a, b, c\}$. Тогда $baaa$ является словом в алфавите Σ.

Определение 1.9. Слово, не содержащее ни одного символа (то есть последовательность длины 0), называется *пустым словом* и обозначается ε.

Определение 1.10. *Длина* слова w, обозначаемая $|w|$, есть число символов в w, причём каждый символ считается столько раз, сколько раз он встречается в w.

Определение 1.11. Если x и y — слова в алфавите Σ, то слово xy (результат приписывания слова y в конец слова x) называется *конкатенацией* (*катенацией*, *сцеплением*) слов x и y. Иногда конкатенацию слов x и y обозначают $x \cdot y$.

Определение 1.12. Если x — слово и $n \in \mathbb{N}$, то через x^n обозначается слово

$$\underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ раз}}.$$

Положим $x^0 \rightleftharpoons \varepsilon$ (знак $\rightleftharpoons$ читается «равно по определению»).

Пример 1.13. По принятым соглашениям $ba^3 = baaa$ и $(ba)^3 = bababa$.

Определение 1.14. Множество всех слов в алфавите Σ обозначается Σ^*.

Определение 1.15. Подмножества множества Σ^* называются *словарными множествами*. (Мал, 11.1.)

Замечание 1.16. Множество Σ^* счётно. В самом деле, в алфавите Σ множество всех слов данной длины конечно, следовательно, Σ^* является объединением счётного числа конечных множеств.

2 Логика высказываний

2.1 Высказывания и высказывательные формы

[УВП, 2.1], **[П1, 2.1]**, **[КД, с. 13–17]**, **[ВШ2, 1.1]**

Определение 2.1. *Высказыванием* называется повествовательное предложение, для которого имеет смысл говорить о его истинности или ложности.

(П1, с. 2.)

Пример 2.2. Предложение «Лиссабон — столица Испании» является высказыванием.

Определение 2.3. *Высказывательной формой* называется выражение, превращающееся в высказывание при замене переменных именами предметов.

(КД, с. 15.)

Пример 2.4. Выражение «z — столица Испании» является высказывательной формой.

2.2 Логические операции

[УВП, 2.2], **[П1, 2.1]**, **[ВШ2, 1.1]**, [Гин, 1], [Сто, 2.1]

Определение 2.5. *Логическая операция* — это такой способ построения сложного высказывания из данных высказываний, при котором истинностное значение сложного высказывания полностью определяется истинностными значениями исходных высказываний.

(П1, с. 2.)

Пример 2.6. Отрицание является логической операцией. Предложение «Неверно, что Лиссабон — столица Испании» построено из высказывания «Лиссабон — столица Испании» с помощью отрицания.

2.3 Формулы логики высказываний

[ВШ2, 1.1], **[УВП, 2.3]**, **[П1, 2.3]**, **[ЛМ, II.1]**, **[Мен, 1.1]**, **[Кли, 1]**, [КД, с. 42–44], [Bil, 1]

Определение 2.7 (истинностное значение). Существуют два *истинностных значения* — «истина» и «ложь». Мы будем обозначать их И и Л соответственно. (Иногда удобнее использовать обозначения 1 и 0.)

Определение 2.8 (пропозициональная переменная). *Пропозициональной переменной* называется переменная, допустимыми значениями которой являются высказывания.

(УВП, с. 23.)

2.9. Пропозициональные переменные будем обозначать буквами P, Q и т. д. (возможно, с индексами). В задачах и примерах неявно предполагается, что разным обозначениям соответствуют разные переменные.

Определение 2.10 (пропозициональная связка). Знаки $\neg$, $\wedge$, $\vee$, $\rightarrow$ (и аналогичные знаки, которые будут введены позже) называются *пропозициональными связками*.

Определение 2.11 (пропозициональная формула (формула логики высказываний)).

1. Если P — пропозициональная переменная, то P — пропозициональная формула.
2. Если A — пропозициональная формула, то $\neg A$ — пропозициональная формула.
3. Если A и B — пропозициональные формулы, то $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ — пропозициональные формулы.

Точнее, *пропозициональные формулы* (или просто *формулы*) образуют *минимальное* множество, обладающее указанными свойствами. В дальнейшем в аналогичных определениях всегда подразумевается такая оговорка о минимальности.

(ВШ2, с. 12.)

2.12. Пропозициональные формулы будем обозначать буквами A, B и т. д. (возможно, с индексами). Разным обозначениям может соответствовать одна и та же формула.

Определение 2.13. *Главной связкой* формулы называется та связка, которая при построении формулы применяется последней.

(Мен, с. 23.)

Определение 2.14 (эквивалентность (эквиваленция)). Если A и B — пропозициональные формулы, то запись $(A \leftrightarrow B)$ является сокращённым обозначением для формулы $((A \to B) \wedge (B \to A))$.

(ВШ2, с. 14.)

2.4 Соглашения о скобках

[П1, с. 5], **[УВП, с. 30]**, **[Мен, с. 27]**, [КД, с. 59], [Кли, с. 15–16], [Шён, с. 35–36]

2.15. При записи формул принято опускать некоторые скобки (для удобства). Полученные при этом выражения являются сокращёнными обозначениями для формул. Во-первых, можно опустить внешнюю пару скобок. Например, запись $P \to (Q \to P)$ обозначает формулу $(P \to (Q \to P))$. Во-вторых, если в сокращённой записи рядом находятся две операции $\wedge$, то при отсутствии скобок внутренней считается та, которая находится левее. Другими словами, связка $\wedge$ считается *левоассоциативной*. Например, $P \wedge Q \wedge R$ и $(P \wedge Q) \wedge R$ обозначают одну и ту же формулу (длина этой формулы — 9 символов). Однако в записи $P \wedge (Q \wedge R)$ ни одной скобки опустить нельзя. Связка $\vee$ тоже является левоассоциативной, но связка $\to$ не является ни левоассоциативной, ни правоассоциативной (в этом курсе). В-третьих, если в сокращённой записи рядом находятся разные связки, то при отсутствии скобок внутренней считается та, которая имеет более высокий приоритет согласно следующему списку, составленному в порядке убывания приоритетов: $\neg$, $\wedge$, $\vee$, $\to$, $\leftrightarrow$. Иными словами, связки с более высоким приоритетом связывают сильнее.

Все эти сокращения являются приёмами изложения, а не элементами языка логики высказываний.

Разрешается также добавить внешнюю пару скобок. Например, запись $(\neg P)$ обозначает формулу $\neg P$. Добавление скобок пригодится, например, в определении 2.44.

2.5 Подформулы в логике высказываний

[ЛМ, II.1], **[П1, 2.3]**

Определение 2.16. *Подформулами* формулы A называются те подслова формулы A, которые сами являются формулами.

Формальное определение множества подформул формулы A (обозначение $\mathrm{SubFm}(A)$) индуктивное.

1. $\mathrm{SubFm}(P) \rightleftharpoons \{P\}$.
2. $\mathrm{SubFm}(\neg A) \rightleftharpoons \{\neg A\} \cup \mathrm{SubFm}(A)$.
3. $\mathrm{SubFm}(A \wedge B) \rightleftharpoons \{(A \wedge B)\} \cup \mathrm{SubFm}(A) \cup \mathrm{SubFm}(B)$. Аналогично для $\vee$ и $\to$.

Определение 2.17. Подформула формулы A, отличная от самой формулы A, называется *собственной подформулой* формулы A.
(П1, с. 5.)

2.6 Однозначность разбора в логике высказываний (без доказательства)

[ВШ2, 1.1], [П1, 2.3], [Bil, 1]

Теорема 2.18 (без доказательства). *Каждая пропозициональная формула, не являющаяся переменной, может быть представлена единственным образом как* $\neg A$, $(A \wedge B)$, $(A \vee B)$ *или* $(A \to B)$.
(ВШ2, теорема 2, с. 16.)
(П1, теорема 2.2, с. 5.)

2.7 Таблицы истинности

[П1, 2.1, 2.4], **[Мен, 1.1]**, **[УВП, 2.2–2.3]**, **[ВШ2, 1.1]**, **[ЛМ, II.1]**, **[Кли, 2]**, [КД, с. 17, 73–75], [Сто, 2.2], [Гин, 1], [Шён, 2.2], [Bil, 2]

Определение 2.19. *Оценкой пропозициональных переменных* (или просто *оценкой*) называется произвольная функция из множества всех пропозициональных переменных в множество истинностных значений.

Определение 2.20. *Истинностное значение* (или просто *значение*) формулы при данной оценке пропозициональных переменных определяется индукцией по построению формулы в соответствии со следующими таблицами.

A	$\neg A$
Л	И
И	Л

A	B	$A \wedge B$	$A \vee B$	$A \to B$
Л	Л	Л	Л	И
Л	И	Л	И	И
И	Л	Л	И	Л
И	И	И	И	И

Формальное определение индуктивное.

1. Значение пропозициональной переменной P при оценке g равно $g(P)$.

2. Значение $\neg A$ равно И тогда и только тогда, когда значение A равно Л.
3. Значение $A \wedge B$ равно И тогда и только тогда, когда значение A равно И и значение B равно И.
4. Значение $A \vee B$ равно И тогда и только тогда, когда значение A равно И или значение B равно И.
5. Значение $A \to B$ равно И тогда и только тогда, когда значение A равно Л или значение B равно И.

Если значение формулы A при данной оценке равно И, то говорят, что формула A *истинна* при данной оценке. Иначе формула A *ложна* при данной оценке.

Замечание 2.21. Если оценки g_1 и g_2 совпадают на всех переменных, входящих в формулу A, то значение A при оценке g_1 совпадает со значением A при оценке g_2.
(П1, теорема 2.3, с. 6.)

Определение 2.22. Пусть дан конечный список $P_1, \ldots, P_n$, состоящий из n различных пропозициональных переменных. Пусть формула A содержит только переменные из данного списка. Тогда *таблицей истинности* (или *истинностной таблицей*) формулы A над списком $P_1, \ldots, P_n$ называется таблица, указывающая значения формулы A при всех возможных оценках переменных $P_1, \ldots, P_n$. (Существует 2^n таких оценок, каждая из них записывается в отдельной строке.)
(П1, с. 6–7.)

Упражнение 2.23. Построить таблицу истинности для формулы $P \leftrightarrow Q$.

Упражнение 2.24. Построить таблицу истинности для формулы $\neg P \vee Q$.

2.8 Тавтологии

[ЛМ, II.1], **[ВШ2, 1.1]**, **[УВП, 2.3]**, **[Мен, 1.2]**, **[П1, 2.5]**, **[Кли, 2, 3, 8]**, [КД, с. 44–45], [Bil, 2], [Сто, 2.3], [Гин, 1]

Определение 2.25. Пропозициональная формула, истинная при каждой оценке пропозициональных переменных, называется *тавтологией* (*тождественно истинной*).

Упражнение 2.26. Является ли тавтологией $P \vee \neg P$?

Определение 2.27. Пропозициональная формула, истинная хотя бы при одной оценке пропозициональных переменных, называется *выполнимой*.

Определение 2.28. Пропозициональная формула, ложная при каждой оценке пропозициональных переменных, называется *противоречием* (*тождественно ложной*).

Теорема 2.29. *Следующие условия равносильны.*

1. *Формула A — противоречие.*
2. *Формула A не является выполнимой.*
3. *Формула $\neg A$ — тавтология.*

Доказательство. Теорема непосредственно следует из определений. □

2.9 Равносильные формулы в логике высказываний

[ВШ2, 1.1], **[Мен, 1.2]**, **[П1, 2.6]**, **[Кли, 3–5]**, **[ЛМ, II.1]**, [КД, с. 45], [Сто, 2.3], [Гин, 1]

Определение 2.30. Формулы A и B называются *равносильными* (*эквивалентными*) (обозначение $A \sim B$), если при каждой оценке пропозициональных переменных значение A совпадает со значением B.

Пример 2.31. $P \to Q \sim \neg Q \to \neg P$.

Упражнение 2.32. Равносильны ли формулы $P \vee (P \wedge Q)$ и P?

Ответ 2.32. Да.

Теорема 2.33.

1. *Имеют место коммутативность и ассоциативность* $\wedge$ *и* $\vee$.
2. *Имеет место дистрибутивность* $\wedge$ *относительно* $\vee$: $A \wedge (B \vee C) \sim (A \wedge B) \vee (A \wedge C)$.
3. *Имеет место дистрибутивность* $\vee$ *относительно* $\wedge$.
4. *Верен закон снятия двойного отрицания*: $\neg\neg A \sim A$.
5. *Справедливы законы де Мóргана*: $\neg(A \wedge B) \sim \neg A \vee \neg B$ *и наоборот.*
6. *Справедливы законы поглощения*: $A \vee (A \wedge B) \sim A$ *и наоборот.*
7. $A \to B \sim \neg A \vee B$.

Доказательство. Теорема следует из определений 2.20 и 2.30. □

Упражнение 2.34. Равносильны ли формулы $P \to (Q \to R)$ и $(P \to Q) \to R$?

Ответ 2.34. Нет. Рассмотрим такую оценку g, что $g(P) = g(Q) = g(R) =$ Л.

Упражнение 2.35. Равносильны ли формулы $P \to (Q \to R)$ и $(P \wedge Q) \to R$?

Ответ 2.35. Да.

Упражнение 2.36. Равносильны ли формулы $P \to (Q \to R)$ и $Q \to (P \to R)$?

Ответ 2.36. Да.

2.37. В задаче на упрощение формулы необходимо найти равносильную, но более короткую формулу. Здесь формулы рассматриваются как конечные последовательности символов из алфави́та, содержащего все пропозициональные переменные и ещё шесть символов: левая скобка, правая скобка и четыре пропозициональные связки.

Упражнение 2.38. Упростить $(P \leftrightarrow Q) \to P$.

Ответ 2.38. $P \vee Q$.

Упражнение 2.39. Упростить $\neg P \to \neg Q$.

Ответ 2.39. $Q \to P$.

Упражнение 2.40. Упростить $(P \vee Q) \wedge (P \vee R) \wedge (Q \vee R \vee \neg P)$.

Ответ 2.40. $(P \vee (Q \wedge R)) \wedge (Q \vee R)$.

Теорема 2.41. *Формулы A и B равносильны тогда и только тогда, когда формула $A \leftrightarrow B$ является тавтологией.*

Теорема 2.42. *Отношение $\sim$ рефлексивно, симметрично и транзитивно.*

Замечание 2.43.

1. Если $A \sim B$ и A — тавтология, то B — тавтология.
2. Если $A \sim B$ и A выполнима, то B выполнима.
3. Если $A \sim B$ и A — противоречие, то B — противоречие.

2.10 Подстановка вместо пропозициональной переменной

[ЛМ, II.1], **[П1, 2.3, 2.5, 2.6]**, **[Кли, 3, 4]**, [Сто, 2.3, 2.4]

Определение 2.44. Если C и D — формулы, а P — пропозициональная переменная, то через $C(P\backslash D)$ обозначим результат подстановки формулы D вместо P в формулу C.

Формальное определение даётся с помощью индукции по построению формулы C.

$$\begin{aligned}
&P(P\backslash D) \rightleftharpoons D,\\
&Q(P\backslash D) \rightleftharpoons Q, \text{ если } Q \text{ — переменная, отличная от } P,\\
&(\neg A)(P\backslash D) \rightleftharpoons \neg(A(P\backslash D)),\\
&(A \wedge B)(P\backslash D) \rightleftharpoons (A(P\backslash D)) \wedge (B(P\backslash D)),\\
&(A \vee B)(P\backslash D) \rightleftharpoons (A(P\backslash D)) \vee (B(P\backslash D)),\\
&(A \to B)(P\backslash D) \rightleftharpoons (A(P\backslash D)) \to (B(P\backslash D)).
\end{aligned}$$

Пример 2.45. Пусть $C = (P_1 \to P_2) \to P_2$ и $D = P_3 \to P_2$. Тогда

$$C(P_2\backslash D) = (P_1 \to (P_3 \to P_2)) \to (P_3 \to P_2).$$

Теорема 2.46 (о подстановке, без доказательства). *Если A — тавтология, B — произвольная формула, а P — пропозициональная переменная, то $A(P\backslash B)$ — тавтология.*

(П1, теорема 2.4, с. 8.)

Доказательство. Рассмотрим произвольную оценку g. Обозначим через g' оценку, полученную из g присвоением переменной P значения формулы B при оценке g. Индукцией по построению формулы C можно доказать, что значение формулы $C(P\backslash B)$ при оценке g совпадает со значением формулы C при оценке g'. Положим $C = A$. Так как формула A истинна при оценке g', то формула $A(P\backslash B)$ истинна при оценке g. □

Пример 2.47. Для любой формулы B формула $B \vee \neg B$ является тавтологией. Например, формула $(P_3 \leftrightarrow P_1) \vee \neg(P_3 \leftrightarrow P_1)$ является тавтологией.

Теорема 2.48. *Пусть A, B, C — формулы, а P — пропозициональная переменная. Если $A \sim B$, то $A(P\backslash C) \sim B(P\backslash C)$.*

Доказательство. Пусть $A \sim B$. По теореме 2.41 $A \leftrightarrow B$ — тавтология. По теореме 2.46 $(A \leftrightarrow B)(P\backslash C)$ — тавтология. Из определений следует, что $(A \leftrightarrow B)(P\backslash C)$ совпадает с $A(P\backslash C) \leftrightarrow B(P\backslash C)$. По теореме 2.41 $A(P\backslash C) \sim B(P\backslash C)$. □

Пример 2.49. Пусть $A = (P_1 \to P_2) \to P_2$, $B = P_1 \vee P_2$, $C = P_3 \to P_2$. Так как $(P_1 \to P_2) \to P_2 \sim P_1 \vee P_2$, то $(P_1 \to (P_3 \to P_2)) \to (P_3 \to P_2) \sim P_1 \vee (P_3 \to P_2)$.

Лемма 2.50. *Если $A \sim B$, то $\neg A \sim \neg B$. Если $A_1 \sim B_1$ и $A_2 \sim B_2$, то $A_1 \wedge A_2 \sim B_1 \wedge B_2$, $A_1 \vee A_2 \sim B_1 \vee B_2$, $A_1 \to A_2 \sim B_1 \to B_2$.*

Теорема 2.51 (об эквивалентной замене). *Пусть A, B, C — формулы, а P — пропозициональная переменная. Если $A \sim B$, то $C(P\backslash A) \sim C(P\backslash B)$.*

(П1, теорема 2.5, с. 10.)

Доказательство. Теорема доказывается индукцией по построению формулы C. □

Пример 2.52. Пусть $A = Q \vee Q$, $B = Q$, $C = P \wedge R$. Так как $Q \vee Q \sim Q$, то $(Q \vee Q) \wedge R \sim Q \wedge R$.

Упражнение 2.53. Существуют ли такие выполнимые формулы A и B, что формула $A(P_1 \backslash B)$ не является выполнимой?

Ответ 2.53. Да. Например, $A = \neg P_1$, $B = P_2 \vee \neg P_2$.

2.11 Дизъюнктивные и конъюнктивные нормальные формы

[П1, 2.8], **[ЛМ, II.1]**, **[ВШ2, 1.2]**, **[Мен, 1.3]**, [Кли, 8], [КД, с. 45, 89–90], [Гин, 2]

Определение 2.54. *Литералами* называются формулы вида P и формулы вида $\neg P$.

Пример 2.55. Формула P_3 является литералом, а формулы $P_3 \vee P_1$ и $\neg\neg P_3$ не являются литералами.

Определение 2.56. *Элементарной конъюнкцией* (*конъюнктом*) называется произвольная конъюнкция литералов. Формальное определение индуктивное.

1. Если L — литерал, то L — элементарная конъюнкция.
2. Если K — элементарная конъюнкция и L — литерал, то $(K \wedge L)$ — элементарная конъюнкция.

Пример 2.57. Формула $(P \wedge \neg Q) \wedge \neg P$ является элементарной конъюнкцией, а формула $P \wedge (\neg Q \wedge \neg P)$ не является элементарной конъюнкцией.

Определение 2.58. *Дизъюнктивной нормальной формой* называется произвольная дизъюнкция элементарных конъюнкций. Формальное определение индуктивное.

1. Если K — элементарная конъюнкция, то K — дизъюнктивная нормальная форма.
2. Если F — дизъюнктивная нормальная форма и K — элементарная конъюнкция, то $(F \vee K)$ — дизъюнктивная нормальная форма.

Пример 2.59. Формулы $(P \wedge \neg R) \vee (Q \wedge R)$ и $(P \wedge Q \wedge R) \vee \neg P \vee \neg R$ являются дизъюнктивными нормальными формами.

Упражнение 2.60. Привести к дизъюнктивной нормальной форме формулу $(P \vee Q) \to R$.

Ответ 2.60. $(\neg P \wedge \neg Q) \vee R$.

Определение 2.61. *Элементарной дизъюнкцией* (*дизъюнктом*) называется произвольная дизъюнкция литералов. Формальное определение индуктивное.

1. Если L — литерал, то L — элементарная дизъюнкция.
2. Если D — элементарная дизъюнкция и L — литерал, то $(D \vee L)$ — элементарная дизъюнкция.

Определение 2.62. *Конъюнктивной нормальной формой* называется произвольная конъюнкция элементарных дизъюнкций. Формальное определение индуктивное.

1. Если D — элементарная дизъюнкция, то D — конъюнктивная нормальная форма.
2. Если G — конъюнктивная нормальная форма и D — элементарная дизъюнкция, то $(G \wedge D)$ — конъюнктивная нормальная форма.

Упражнение 2.63. Привести к конъюнктивной нормальной форме формулу $(P \vee Q) \to R$.

Ответ 2.63. $(\neg P \vee R) \wedge (\neg Q \vee R)$.

Теорема 2.64. *Каждая пропозициональная формула равносильна некоторой дизъюнктивной нормальной форме и некоторой конъюнктивной нормальной форме.*

Доказательство. Выразим $\to$ через $\neg$ и $\vee$. Используем законы де Моргана и закон снятия двойного отрицания. Используем ассоциативность и дистрибутивность.

В строгом доказательстве индукцией по длине формулы рассматриваются девять случаев: P, $A \to B$, $A \vee B$, $A \wedge B$, $\neg P$, $\neg(A \to B)$, $\neg(A \vee B)$, $\neg(A \wedge B)$, $\neg\neg P$. □

Определение 2.65. Формула A называется *совершенной дизъюнктивной нормальной формой*, если она является дизъюнктивной нормальной формой и каждая встречающаяся в A переменная входит в каждую элементарную конъюнкцию ровно один раз (с отрицанием или без).

Теорема 2.66. *Если формула A не противоречие, то A равносильна некоторой совершенной дизъюнктивной нормальной форме.*

Доказательство. Пусть $P_1, \ldots, P_n$ — список переменных, встречающихся в формуле A. Построим таблицу истинности формулы A над списком $P_1, \ldots, P_n$. Для каждой строки, где формула A истинна, составим элементарную конъюнкцию, истинную только при оценке, соответствующей этой строке. Дизъюнкция всех этих элементарных конъюнкций является искомой совершенной дизъюнктивной нормальной формой.

(П1, с. 13.) □

Упражнение 2.67. Привести к совершенной дизъюнктивной нормальной форме формулу $\neg(P \leftrightarrow Q)$.

Ответ 2.67. $(\neg P \wedge Q) \vee (P \wedge \neg Q)$.

Определение 2.68. Формула A называется *совершенной конъюнктивной нормальной формой*, если она является конъюнктивной нормальной формой и каждая встречающаяся в A переменная входит в каждую элементарную дизъюнкцию ровно один раз (с отрицанием или без).

Теорема 2.69. *Если формула A не тавтология, то A равносильна некоторой совершенной конъюнктивной нормальной форме.*

Доказательство. Пусть $P_1, \ldots, P_n$ — список переменных, встречающихся в формуле A. Построим таблицу истинности формулы A над списком $P_1, \ldots, P_n$. Для каждой строки, где формула A ложна, составим элементарную дизъюнкцию, ложную только при оценке, соответствующей этой строке. Конъюнкция всех этих элементарных дизъюнкций является искомой совершенной конъюнктивной нормальной формой.

(П1, с. 13.) □

Упражнение 2.70. Привести к совершенной конъюнктивной нормальной форме формулу $\neg(P \leftrightarrow Q)$.

Ответ 2.70. $(P \vee Q) \wedge (\neg P \vee \neg Q)$.

2.12 Логическое следование в логике высказываний

[П1, 2.11], **[Кли, 7]**, [Сто, 2.4–2.5], [Bil, 2]

Определение 2.71. Пусть Γ — некоторое множество формул логики высказываний и A — формула логики высказываний. Говорят, что формула A *логически следует* (или просто *следует*) из множества Γ (обозначение $\Gamma \vDash A$), если формула A истинна при каждой оценке пропозициональных переменных, при которой истинны все формулы из Γ.

Пример 2.72. $\{P \vee Q, R, \neg Q\} \vDash P \wedge R$.

Замечание 2.73. Формула A следует из множества $\{B_1, \dots, B_n\}$ тогда и только тогда, когда формула $B_1 \wedge \dots \wedge B_n \to A$ является тавтологией.

(П1, теорема 2.11, с. 16.)

2.13 Полные системы булевых функций

[П1, 3.1], **[ВШ2, 1.2]**, **[Мен, 1.3]**, **[ЛМ, II.2]**, [КД, с. 43], [Гин, 6]

Определение 2.74. Если $n \in \mathbb{N}$, то n-местной *булевой функцией* называется произвольная функция из множества $\{\text{И}, \text{Л}\}^n$ в множество $\{\text{И}, \text{Л}\}$.

(ВШ2, с. 12.)

2.75. Можно рассматривать формулы, использующие и другие пропозициональные связки (кроме $\neg$, $\wedge$, $\vee$, $\to$), вводимые с помощью таблиц истинности.

Определение 2.76. Введём двуместные операции $\oplus$, $|$, $\downarrow$, истинностные значения которых определяются в соответствии со следующей таблицей.

A	B	$A \oplus B$	$A \mid B$	$A \downarrow B$
Л	Л	Л	И	И
Л	И	И	И	Л
И	Л	И	И	Л
И	И	Л	Л	Л

Операция $|$ называется *штрихом Шеффера*, операция $\downarrow$ называется *стрелкой Пирса*.

Теорема 2.77.

1. $A \oplus B \sim \neg(A \leftrightarrow B)$.
2. $A \mid B \sim \neg(A \wedge B)$.
3. $A \downarrow B \sim \neg(A \vee B)$.

Упражнение 2.78. Сколько существует различных n-местных булевых функций?

Ответ 2.78. 2^{2^n}.

Упражнение 2.79. Сколько существует различных 0-местных булевых функций?

Ответ 2.79. 2.

Определение 2.80. Введём 0-местные операции $\perp$ и $\top$, истинностные значения которых определяются в соответствии со следующими таблицами.

$\perp$
Л

$\top$
И

Теорема 2.81.

1. $A \wedge \neg A \sim \perp$.
2. $A \vee \neg A \sim \top$.
3. $\neg\top \sim \perp$.

4. $\neg\bot \sim \top$.
5. $A \wedge \top \sim A$.
6. $A \wedge \bot \sim \bot$.
7. $A \vee \top \sim \top$.
8. $A \vee \bot \sim A$.

Определение 2.82. Если зафиксирован конечный список, состоящий из n различных пропозициональных переменных, то каждая формула, содержащая только переменные из данного списка, *задаёт* некоторую n-местную булеву функцию.

Пример 2.83. Рассмотрим список переменных P_1, P_2. Тогда формула $\neg P_2 \wedge P_1$ задаёт следующую булеву функцию:

$$\langle \text{Л}, \text{Л} \rangle \mapsto \text{Л}, \qquad \langle \text{Л}, \text{И} \rangle \mapsto \text{Л}, \qquad \langle \text{И}, \text{Л} \rangle \mapsto \text{И}, \qquad \langle \text{И}, \text{И} \rangle \mapsto \text{Л}.$$

Определение 2.84. Пусть Φ — некоторое множество булевых функций. Система Φ называется *полной*, если для каждого положительного n каждая n-местная булева функция задаётся некоторой формулой, составленной из скобок, переменных и обозначений операций из Φ.

Теорема 2.85. *Система* $\{\vee, \wedge, \neg\}$ *полна.*

(ВШ2, теорема 3, с. 18.)

Доказательство. Тождественно ложная функция задаётся формулой $P_1 \wedge \neg P_1$. Для остальных функций можно использовать доказательство теоремы 2.66.

(П1, с. 13.) □

Пример 2.86. Система $\{\vee, \neg\}$ полна, так как $A \wedge B \sim \neg(\neg A \vee \neg B)$.

Пример 2.87. Система $\{\rightarrow, \bot\}$ полна, так как $\neg A \sim A \rightarrow \bot$ и $A \vee B \sim (A \rightarrow \bot) \vee B$.

Пример 2.88. Система $\{|\}$ полна, так как $\neg A \sim A \mid A$ и $A \vee B \sim (A \mid A) \mid (B \mid B)$.

Пример 2.89. Система $\{\downarrow\}$ полна, так как $\neg A \sim A \downarrow A$ и $A \vee B \sim (A \downarrow B) \downarrow (A \downarrow B)$.

Упражнение 2.90. Является ли полной система булевых функций $\{\vee, \leftrightarrow, \bot\}$?

Ответ 2.90. Да. $\neg A \sim A \leftrightarrow \bot$, $A \wedge B \sim \neg(\neg A \vee \neg B)$.

2.14 Выражение одних логических операций через другие

[П1, 3.1], [ЛМ, II.2]

Определение 2.91. Пусть Φ — некоторое множество булевых функций. Говорят, что n-местная булева функция ψ *выражается* через функции из множества Φ, если формула $\psi(P_1, \ldots, P_n)$ равносильна некоторой формуле, составленной из скобок, переменных и обозначений функций из Φ. Здесь $P_1, \ldots, P_n$ — различные пропозициональные переменные.

3 Логика предикатов

3.1 Кванторы

[УВП, 2.4], **[ВШ2, с. 86]**, **[П1, 5.1]**, **[Мен, 2.1]**, [Шён, 2.3], [Сто, 2.6]

3.1. *Квантор всеобщности* (или *квантор общности*) $\forall$ и *квантор существования* $\exists$ позволяют из высказывательной формы, зависящей от некоторого параметра, получить другую высказывательную форму, не зависящую от этого параметра.

Кванторная приставка $\forall v$ читается «для каждого v имеет место...». Кванторная приставка $\exists v$ читается «существует такой v, что...».

Пример 3.2. Высказывательная форма «$x \cdot y = 1$» зависит от параметров x и y. Высказывательная форма «существует такой y, что $x \cdot y = 1$» зависит от параметра x. Высказывание «для каждого x существует такой y, что $x \cdot y = 1$» не зависит от параметров.

3.2 Понятие предиката

[УВП, 2.5], **[ВШ2, 3.1]**, **[П1, 5.2]**, [Шён, 2.1], [Сто, 2.6]

Определение 3.3. Если M — множество и $k \in \mathbb{N}$, то k-местным *предикатом* на множестве M называется произвольное отображение из множества M^k в множество $\{\text{И}, \text{Л}\}$.

(ВШ2, с. 87.)

Пример 3.4. Пример трёхместного предиката $\boldsymbol{Q}$ на множестве $\mathbb{R}$:

$$\boldsymbol{Q}(a_1, a_2, a_3) = \begin{cases} \text{И}, & \text{если } a_1^2 + a_2^2 = a_3^2, \\ \text{Л} & \text{иначе.} \end{cases}$$

Определение 3.5. Если M — множество и $k \in \mathbb{N}$, то k-местной *функцией* на множестве M называется произвольное отображение из множества M^k в множество M.

(ВШ2, с. 87.)

Пример 3.6. Пример трёхместной функции $\boldsymbol{f}$ на множестве $\mathbb{N}$:

$$\boldsymbol{f}(a_1, a_2, a_3) = 2^{a_1} 3^{a_2} 5^{a_3}.$$

3.7. Будем отождествлять нульместные функции на M с элементами M, а нульместные предикаты на M с элементами множества $\{\text{И}, \text{Л}\}$.

3.3 Языки первого порядка

[ВШ2, 3.1], **[П1, 5.3]**, **[ЛМ, II.4]**, [УВП, 2.6], [Мен, 2.1], [Кли, 16, 28], [КД, с. 49–50, 75–79, 120–121], [Шён, 2.4], [Bil, 5]

Определение 3.8. Каждый *язык первого порядка* (или *элементарный язык*) задаётся своей сигнатурой — набором из двух множеств $\Omega = \langle \mathrm{Fn}, \mathrm{Pr} \rangle$, где Fn — множество *функциональных символов* и Pr — множество *предикатных символов*. При этом с каждым функциональным и предикатным символом связано некоторое натуральное число — количество аргументов (или *валентность*) этого символа. Валентность может быть нулевой.

(ВШ2, с. 88.)

(П1, с. 33.)

3.9. Функциональные и предикатные символы валентности 0 называются *нульместными* или *нульарными*. Функциональные и предикатные символы валентности 1 называются *одноместными* или *унарными*. Функциональные и предикатные символы валентности 2 называются *двуместными* или *бинарными*. Функциональные и предикатные символы валентности 3 называются *трёхместными* или *тернарными*.

Пример 3.10. Сигнатура теории упорядоченных множеств содержит два двуместных предикатных символа: $=$ и $<$. Аксиомы частичного порядка записываются так:

$$\begin{aligned}
&\forall x\, \neg(x < x),\\
&\forall x\, \forall y\, \forall z\, (x < y \wedge y < z \to x < z).
\end{aligned}$$

Пример 3.11. Сигнатура теории групп содержит двуместный предикатный символ $=$ и три функциональных символа: двуместный $\cdot$, одноместный inv и нульместный e. Аксиомы теории групп записываются так:

$$\begin{aligned}
&\forall x\, \forall y\, \forall z\, ((x \cdot y) \cdot z = x \cdot (y \cdot z)),\\
&\forall x\, (x \cdot e = x \wedge e \cdot x = x),\\
&\forall x\, (x \cdot \mathrm{inv}(x) = e \wedge \mathrm{inv}(x) \cdot x = e).
\end{aligned}$$

(ВШ2, с. 90–91.)

Определение 3.12. Функциональные символы валентности 0 называются *константами* (или *индивидными константами*).

(ВШ2, с. 88.)

Определение 3.13. *Переменная* — это языково́е выражение, служащее для обозначения произвольного объекта из некоторого фиксированного множества, называемого *областью возможных значений* этой переменной. Во всяком языке первого порядка имеется счётный набор *индивидных переменных* (*предметных переменных*, или просто *переменных*).

(УВП, с. 19, 28.)

3.14. Мы будем рассматривать *односортные* языки первого порядка. Это значит, что в каждой конкретной интерпретации все индивидные переменные имеют одну и ту же область возможных значений. (Формальное определение интерпретации будет дано в разделе 3.8.)

3.15. Индивидные переменные будем обозначать буквами u, v, w, x, y, z (возможно, с индексами). Нульместные функциональные символы будем обозначать буквами c, d и т. д. (возможно, с индексами). Ненульместные функциональные символы будем обозначать буквами f, g и т. д. (возможно, с индексами). Предикатные символы будем обозначать буквами P, Q и т. д. (возможно, с индексами). В задачах и примерах неявно предполагается, что разным обозначениям соответствуют разные переменные и разные символы из сигнатуры. Например, в формуле $\forall x\, \exists y\, f(x, y) = c$ буквы x и y обозначают различные переменные.

Определение 3.16. *Алфавитом* языка первого порядка с сигнатурой Ω называется множество, состоящее из символов сигнатуры Ω, индивидных переменных, левой и правой скобок, запятой и символов $\forall$, $\exists$, $\neg$, $\wedge$, $\vee$, $\to$.

(ЛМ, II.4.)

3.17. Некоторые конечные последовательности символов из такого алфавита называются *термами* (или *правильно построенными термами*) и *формулами* (или *правильно построенными формулами*) данной сигнатуры.

Определение 3.18 (терм сигнатуры Ω).

1. Если v — индивидная переменная, то v — терм сигнатуры Ω.
2. Если c — нульместный функциональный символ сигнатуры Ω, то c — терм сигнатуры Ω.
3. Если f — n-местный функциональный символ сигнатуры Ω, где $n > 0$, и $t_1, \ldots, t_n$ — термы сигнатуры Ω, то $f(t_1, \ldots, t_n)$ — терм сигнатуры Ω.

(ВШ2, с. 88.)

Пример 3.19. Примеры термов сигнатуры теории групп: $\mathrm{inv}(\mathrm{inv}(x))$, $\mathrm{inv}(e)$, $\cdot(x, \cdot(y, z))$.

3.20. Если f — двуместный функциональный символ, то обычно вместо $f(t_1, t_2)$ пишут $(t_1\, f\, t_2)$ или даже $t_1\, f\, t_2$. Например, в сигнатуре теории групп запись $x \cdot (y \cdot z)$ обозначает терм $\cdot(x, \cdot(y, z))$.

Определение 3.21 (атомарная формула сигнатуры Ω).

1. Если P — нульместный предикатный символ сигнатуры Ω, то P — атомарная формула сигнатуры Ω.
2. Если P — n-местный предикатный символ сигнатуры Ω, где $n > 0$, и $t_1, \ldots, t_n$ — термы сигнатуры Ω, то $P(t_1, \ldots, t_n)$ — атомарная формула сигнатуры Ω.

(ВШ2, с. 89.)

Пример 3.22. Примеры атомарных формул сигнатуры теории групп: $=(x, y)$, $=(\mathrm{inv}(\mathrm{inv}(x)), x)$.

3.23. Если P — двуместный предикатный символ, то обычно вместо $P(t_1, t_2)$ пишут $(t_1\ P\ t_2)$ или даже $t_1\ P\ t_2$. Например, в сигнатуре теории групп запись $\mathrm{inv}(\mathrm{inv}(x)) = x$ обозначает атомарную формулу $=(\mathrm{inv}(\mathrm{inv}(x)), x)$.

Определение 3.24 (формула сигнатуры Ω).

1. Если A — атомарная формула сигнатуры Ω, то A — формула сигнатуры Ω.
2. Если A — формула сигнатуры Ω, то $\neg A$ — формула сигнатуры Ω.
3. Если A и B — формулы сигнатуры Ω, то $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ — формулы сигнатуры Ω.
4. Если A — формула сигнатуры Ω, а v — индивидная переменная, то $\forall v\, A$ и $\exists v\, A$ — формулы сигнатуры Ω.

(ВШ2, с. 89.)

Пример 3.25. Аксиомы из примеров 3.10 и 3.11 являются формулами соответствующих сигнатур.

Формулы сигнатуры Ω называются также *формулами языка первого порядка* или *формулами логики предикатов*.

3.26. Термы будем обозначать буквами s и t (возможно, с индексами). Формулы языка первого порядка будем обозначать буквами A, B и т. д. (возможно, с индексами). Разным обозначениям может соответствовать один и тот же терм или одна и та же формула. Например, в третьем пункте определения терма обозначениям t_1 и t_2 может соответствовать один и тот же терм.

3.4 Подформулы в логике предикатов

[ЛМ, II.4]

Определение 3.27. *Подформулами* формулы A называются те подслова слова A, которые сами являются формулами.

Формальное определение множества подформул формулы A (обозначение $\mathrm{SubFm}(A)$) индуктивное.

1. $\mathrm{SubFm}(P) \rightleftharpoons \{P\}$.
2. $\mathrm{SubFm}(\neg A) \rightleftharpoons \{\neg A\} \cup \mathrm{SubFm}(A)$.
3. $\mathrm{SubFm}(A \wedge B) \rightleftharpoons \{(A \wedge B)\} \cup \mathrm{SubFm}(A) \cup \mathrm{SubFm}(B)$. Аналогично для $\vee$ и $\to$.
4. $\mathrm{SubFm}(\forall v\, A) \rightleftharpoons \{\forall v\, A\} \cup \mathrm{SubFm}(A)$. Аналогично для $\exists$.

Определение 3.28. Подформула формулы A, отличная от самой формулы A, называется *собственной подформулой* формулы A.

Упражнение 3.29. Является ли $\forall x$ подформулой формулы $\forall x\, P(x)$?

Ответ 3.29. Нет. У этой формулы только две подформулы: она сама и $P(x)$.

3.5 Однозначность разбора в логике предикатов (без доказательства)

Теорема 3.30 (без доказательства). *Каждая формула, не являющаяся атомарной, может быть представлена единственным образом как $\neg A$, $(A \wedge B)$, $(A \vee B)$, $(A \to B)$, $\forall v\, A$ или $\exists v\, A$.*

3.6 Язык теории множеств

[ВШ2, 3.1], [УВП, 2.7], [П1, 5.3], [ЛМ, II.7], [Bil, 5]

Определение 3.31. Сигнатура теории множеств содержит два двуместных предикатных символа: $=$ и $\in$. Функциональных символов нет.

Пример 3.32. Пример формулы языка теории множеств: $\forall z\,(z \in x \to z \in y)$.

Определение 3.33. Введём сокращённое обозначение

$$t_1 \subseteq t_2 \rightleftharpoons \forall v\,(v \in t_1 \to v \in t_2),$$

где в качестве v используется любая переменная, не встречающаяся в термах t_1 и t_2.

Пример 3.34 (аксиома объёмности, или экстенсиональности). Пример формулы языка теории множеств: $\forall x\,\forall y\,(x \subseteq y \wedge y \subseteq x \to x = y)$. Эта формула называется *аксиомой объёмности* или *аксиомой экстенсиональности*.

3.7 Свободные и связанные вхождения переменных

[УВП, 2.1, 2.6], **[ВШ2, 3.2, 4.2]**, **[П1, 5.1]**, **[Мен, 2.1]**, **[ЛМ, II.4]**, [Кли, 16, 28], [КД, с. 50, 60–62, 120], [Шён, 2.3, 2.4], [Bil, 5]

Определение 3.35. Все вхождения переменной в формулу делятся на *свободные* и *связанные*. Вхождение переменной v в формулу A называется свободным, если оно не содержится ни в одной подформуле формулы A, начинающейся с $\forall v$ или $\exists v$.

Формальное определение свободных вхождений переменной в формулу индуктивное.

1. В атомарной формуле все вхождения переменных свободны.
2. Свободные вхождения переменной в формулу A являются её свободными вхождениями в формулу $\neg A$.
3. Свободные вхождения переменной в одну из формул A и B являются её свободными вхождениями в формулы $(A \wedge B)$, $(A \vee B)$, $(A \to B)$.
4. Свободные вхождения переменной, отличной от v, в формулу A являются её свободными вхождениями в формулы $\forall v\, A$ и $\exists v\, A$.

(ВШ2, с. 159–160.)

Определение 3.36. Переменная, имеющая хотя бы одно свободное вхождение в формулу A, называется *свободной переменной* (*параметром*) формулы A. Множество всех свободных переменных формулы A обозначается $\mathrm{FV}(A)$.

Пример 3.37. $\mathrm{FV}(x \cdot y = x) = \{x, y\}$.

Пример 3.38. $\mathrm{FV}(\forall x\,(x \cdot y = x)) = \{y\}$.

3.39. Если t — имя (то есть обозначение) некоторого конкретного объекта из области возможных значений переменной v, то подстановка t вместо всех свободных вхождений переменной v в формулу A является осмысленным (за некоторыми исключениями, см. раздел 3.18). Аналогичная подстановка вместо всех связанных вхождений является бессмысленной.

Чтобы узнать значение формулы A, нужно, как правило, знать значения всех свободных переменных формулы A.

Замечание 3.40.

1. Если $n > 0$ и P — n-местный предикатный символ, то $\mathrm{FV}(P(t_1, \ldots, t_n))$ состоит из всех переменных, встречающихся в термах $t_1, \ldots, t_n$.
2. Если P — нульместный предикатный символ, то $\mathrm{FV}(P) = \varnothing$.
3. $\mathrm{FV}(\neg A) = \mathrm{FV}(A)$.
4. $\mathrm{FV}(A \wedge B) = \mathrm{FV}(A \vee B) = \mathrm{FV}(A \to B) = \mathrm{FV}(A) \cup \mathrm{FV}(B)$.
5. $\mathrm{FV}(\forall v\, A) = \mathrm{FV}(\exists v\, A) = \mathrm{FV}(A) \setminus \{v\}$.

Определение 3.41. Терм называется *замкнутым*, если он не содержит ни одной переменной.

Определение 3.42. Формула называется *замкнутой*, если она не имеет ни одной свободной переменной. Замкнутые формулы называются также *предложениями*.

Определение 3.43. Результат *подстановки терма t вместо переменной v* в терм s обозначается $s[t/v]$.

Формальное определение индуктивное.

1. $v[t/v] \rightleftharpoons t$.
2. Если v и u — различные переменные, то $u[t/v] \rightleftharpoons u$.

3. Если $n > 0$ и f — n-местный предикатный символ, то $f(t_1, \dots, t_n)[t/v] \rightleftharpoons f(t_1[t/v], \dots, t_n[t/v])$.
4. Если c — нульместный предикатный символ, то $c[t/v] \rightleftharpoons c$.

Замечание 3.44. Если v — индивидная переменная, а s и t — термы сигнатуры Ω, то $s[t/v]$ также терм сигнатуры Ω.

Пример 3.45. Запись $(x \cdot \mathrm{inv}(x))[(y \cdot z)/x]$ является обозначением терма $(y \cdot z) \cdot \mathrm{inv}(y \cdot z)$.

Лемма 3.46. *Терм $s[v/v]$ совпадает с термом s.*

Доказательство. Лемма доказывается индукцией по построению терма s. □

Определение 3.47. *Подстановкой терма t вместо переменной v* в формулу C называется замена в формуле C всех свободных вхождений переменной v на терм t. Результат такой подстановки обозначается $(C[t/v])$ или просто $C[t/v]$. Формальное определение индуктивное.

1. Если $n > 0$ и P — n-местный предикатный символ, то
$$P(t_1, \dots, t_n)[t/v] \rightleftharpoons P(t_1[t/v], \dots, t_n[t/v]).$$
2. Если P — нульместный предикатный символ, то $P[t/v] \rightleftharpoons P$.
3. $(\neg A)[t/v] \rightleftharpoons \neg(A[t/v])$.
4. $(A \wedge B)[t/v] \rightleftharpoons (A[t/v]) \wedge (B[t/v])$. Аналогично для $\vee$ и $\to$.
5. $(\forall v\, A)[t/v] \rightleftharpoons \forall v\, A$. Аналогично для $\exists$.
6. Если u — отличная от v переменная, то $(\forall u\, A)[t/v] \rightleftharpoons \forall u\, (A[t/v])$. Аналогично для $\exists$.

Замечание 3.48. Если v — индивидная переменная, t — терм сигнатуры Ω и C — формула сигнатуры Ω, то $C[t/v]$ также формула сигнатуры Ω.

Пример 3.49. Запись $(x \cdot e = \mathrm{inv}(x))[(y \cdot z)/x]$ является обозначением формулы $(y \cdot z) \cdot e = \mathrm{inv}(y \cdot z)$.

Пример 3.50. Запись $(\exists y\, x = y \cdot y \wedge \exists x\, y = x \cdot x)[z/x]$ является обозначением формулы $\exists y\, z = y \cdot y \wedge \exists x\, y = x \cdot x$.

Лемма 3.51. *Формула $C[v/v]$ совпадает с формулой C.*

Доказательство. Лемма доказывается индукцией по построению формулы C. □

3.52. Будем считать, что приоритет у подстановки выше, чем у пропозициональных связок и кванторов. Например, запись $A \wedge B[t/v]$ обозначает не $(A \wedge B)[t/v]$, а $A \wedge (B[t/v])$.

3.53. Во многих учебниках для формулы $C[t/v]$ употребляется обозначение $C(t)$. При этом переменная v фиксирована (для данной формулы C) и данная формула C без круглых скобок вообще не встречается. Следуя этой договорённости, можно, например, формулу $A[0/x] \wedge \forall x\, (A \to A[x + 1/x]) \to \forall x\, A$ записать в виде $A(0) \wedge \forall x\, (A(x) \to A(x + 1)) \to \forall x\, A(x)$.

3.54. Аналогично определению 3.47 можно определить результат одновременной замены n различных переменных на n термов (обозначение $C[t_1/v_1, \dots, t_n/v_n]$) и ввести обозначение $C(t_1, \dots, t_n)$ для формулы $C[t_1/v_1, \dots, t_n/v_n]$.

3.8 Интерпретации

[УВП, 2.8], **[П1, 5.4]**, **[ЛМ, II.4]**, **[ВШ2, 3.2]**, **[Мен, 2.2]**, [Кли, 17], [Шён, 2.5], [КД, с. 28–32, 50, 69–73, 122], [Сто, 2.8], [Bil, 6]

Определение 3.55 (интерпретация). *Интерпретация* $\mathfrak{M}$ языка первого порядка с сигнатурой Ω состоит из

1) непустого множества M, называемого *носителем* (или *основным множеством*) данной интерпретации,
2) отображения, ставящего в соответствие каждому n-местному функциональному символу f сигнатуры Ω некоторую n-местную функцию $f^{\mathfrak{M}}$ на множестве M,
3) отображения, ставящего в соответствие каждому n-местному предикатному символу P сигнатуры Ω некоторый n-местный предикат $P^{\mathfrak{M}}$ на множестве M.

Иногда вместо $f^{\mathfrak{M}}$ и $P^{\mathfrak{M}}$ пишут $\overline{f}$ и $\overline{P}$. Интерпретацию называют также *алгебраической системой* и обозначают $\langle M, \Omega\rangle$.

(П1, с. 36.)

Замечание 3.56. Если c — константа, то $c^{\mathfrak{M}} \in M$. Если P — нульместный предикатный символ, то $P^{\mathfrak{M}} \in \{\text{И}, \text{Л}\}$.

3.57. Интерпретации будем обозначать буквами $\mathfrak{L}$ и $\mathfrak{M}$ (возможно, с индексами). Разным обозначениям может соответствовать одна и та же интерпретация.

Элементы носителя интерпретации будем обозначать буквами a и b (возможно, с индексами). Разным обозначениям может соответствовать один и тот же элемент.

3.9 Истинность замкнутой формулы в данной интерпретации

[УВП, 2.9], **[П1, 5.4]**, **[ЛМ, II.4]**, [ВШ2, 3.2], [Мен, 2.2], [Кли, 17], [Шён, 2.5], [КД, с. 28–32, 50, 69–73, 122], [Bil, 6]

Определение 3.58 (сигнатура $\Omega(M)$). Пусть $\langle M, \Omega\rangle$ — некоторая интерпретация. Тогда через $\Omega(M)$ обозначается сигнатура, полученная из сигнатуры Ω добавлением в множество функциональных символов новых констант $\{\underline{a} \mid a \in M\}$. При этом для каждого элемента множества M добавляется ровно одна константа и все новые константы отличны друг от друга и от сигнатурных символов из Ω. Константа $\underline{a}$ называется *именем* элемента M.

(УВП, с. 36.)

Определение 3.59 (значение замкнутого терма). Пусть дана интерпретация $\mathfrak{M} = \langle M, \Omega\rangle$. Для каждого замкнутого терма t сигнатуры $\Omega(M)$ определим его *значение* в интерпретации $\mathfrak{M}$, обозначаемое $[t]^{\mathfrak{M}}$.

1. Если $a \in M$, то $[\underline{a}]^{\mathfrak{M}} \rightleftharpoons a$.
2. Если f — n-местный функциональный символ сигнатуры Ω, где $n > 0$, и $t_1, \dots, t_n$ — термы сигнатуры Ω, то $[f(t_1, \dots, t_n)]^{\mathfrak{M}} = f^{\mathfrak{M}}([t_1]^{\mathfrak{M}}, \dots, [t_1]^{\mathfrak{M}})$.
3. Если c — нульместный функциональный символ сигнатуры Ω, то $[c]^{\mathfrak{M}} \rightleftharpoons c^{\mathfrak{M}}$.

Иногда вместо $[t]^{\mathfrak{M}}$ пишут $[t]$ или $|t|$.

(П1, с. 36.)

Определение 3.60 (истинностное значение замкнутой формулы). Пусть дана интерпретация $\mathfrak{M} = \langle M, \Omega\rangle$. Для каждой замкнутой формулы A сигнатуры $\Omega(M)$ определим *истинностное значение* формулы A в интерпретации $\mathfrak{M}$, обозначаемое $[A]^{\mathfrak{M}}$.

1. Если P — n-местный предикатный символ, где $n > 0$, и $t_1, \ldots, t_n$ — термы сигнатуры $\Omega(M)$, то $[P(t_1, \ldots, t_n)]^{\mathfrak{M}} = P^{\mathfrak{M}}([t_1]^{\mathfrak{M}}, \ldots, [t_1]^{\mathfrak{M}})$.
2. Если P — нульместный предикатный символ, то $[P]^{\mathfrak{M}} \rightleftharpoons P^{\mathfrak{M}}$.
3. $[\neg A]^{\mathfrak{M}} =$ И тогда и только тогда, когда $[A]^{\mathfrak{M}} =$ Л.
4. $[A \wedge B]^{\mathfrak{M}} =$ И тогда и только тогда, когда $[A]^{\mathfrak{M}} =$ И и $[B]^{\mathfrak{M}} =$ И.
5. $[A \vee B]^{\mathfrak{M}} =$ И тогда и только тогда, когда $[A]^{\mathfrak{M}} =$ И или $[B]^{\mathfrak{M}} =$ И.
6. $[A \to B]^{\mathfrak{M}} =$ И тогда и только тогда, когда $[A]^{\mathfrak{M}} =$ Л или $[B]^{\mathfrak{M}} =$ И.
7. $[\exists v\, A]^{\mathfrak{M}} =$ И тогда и только тогда, когда найдётся такой элемент $a \in M$, что $[A[\,\underline{a}\,/v]]^{\mathfrak{M}} =$ И.
8. $[\forall v\, A]^{\mathfrak{M}} =$ И тогда и только тогда, когда для каждого элемента $a \in M$ имеет место $[A[\,\underline{a}\,/v]]^{\mathfrak{M}} =$ И.

Иногда вместо $[A]^{\mathfrak{M}}$ пишут $[A]$.

(П1, с. 36–37.)

Определение 3.61 (истинность замкнутой формулы в $\mathfrak{M}$). Если $[A]^{\mathfrak{M}} =$ И, то говорят, что формула A *истинна* в интерпретации $\mathfrak{M}$ и пишут $\mathfrak{M} \models A$. Если $[A]^{\mathfrak{M}} =$ Л, то говорят, что формула A *ложна* в интерпретации $\mathfrak{M}$ и пишут $\mathfrak{M} \not\models A$.

(П1, с. 37.)

3.10 Выразимые предикаты

[ВШ2, 3.3], [УВП, 2.14]

Определение 3.62. Пусть фиксированы сигнатура Ω и интерпретация $\mathfrak{M} = \langle M, \Omega \rangle$. Пусть $\boldsymbol{R}$ — n-местный предикат на M. Выберем n различных индивидных переменных $v_1, \ldots, v_n$. Говорят, что формула A сигнатуры Ω *выражает* предикат $\boldsymbol{R}$ относительно списка переменных $v_1, \ldots, v_n$, если $\mathrm{FV}(A) \subseteq \{v_1, \ldots, v_n\}$ и для всех $a_1, \ldots, a_n \in M$ имеет место $\boldsymbol{R}(a_1, \ldots, a_n) = [A[\,\underline{a_1}\,/v_1] \ldots [\,\underline{a_n}\,/v_n]]^{\mathfrak{M}}$.

(ВШ2, с. 96.)

(УВП, с. 50.)

Определение 3.63. Предикат называется *выразимым* в интерпретации $\langle M, \Omega \rangle$, если существует формула сигнатуры Ω, выражающая этот предикат.

(ВШ2, с. 96.)

(УВП, с. 51.)

Пример 3.64. Рассмотрим двуместный предикат $\boldsymbol{R}$ на множестве $\mathbb{Z}$, определённый так: $\boldsymbol{R}(a_1, a_2) =$ И тогда и только тогда, когда $a_2 = a_1 + 2$. В стандартной интерпретации сигнатуры $\langle =, < \rangle$ на $\mathbb{Z}$ этот предикат можно выразить формулой $\exists z\, (x < z \wedge z < y \wedge \forall w\, (x < w \wedge w < y \to w = z))$ (относительно списка переменных x, y).

3.65. При задании предикатов в задачах на выразимость элементы носителя интерпретации часто обозначаются теми буквами, которые обычно используются в качестве индивидных переменных. Тогда отпадает необходимость указывать в ответе список переменных. Например, формула из примера 3.64 выражает предикат «$y = x + 2$» в стандартной интерпретации сигнатуры $\langle =, < \rangle$ на множестве $\mathbb{Z}$.

Упражнение 3.66. Выразить двуместный предикат «$x < y$» в стандартной интерпретации сигнатуры $\langle =, + \rangle$ на $\mathbb{N}$.

Ответ 3.66. $\exists z\, (x + z = y) \wedge \neg(x = y)$.

Упражнение 3.67. Выразить трёхместный предикат «число x является наибольшим общим делителем чисел y и z» формулой сигнатуры $\langle \cdot, = \rangle$ в стандартной интерпретации на $\mathbb{N}$.

Ответ 3.67. $\exists w\,(y = x{\cdot}w) \wedge \exists w\,(z = x{\cdot}w) \wedge \forall x_1\,(\exists w\,(y = x_1{\cdot}w) \wedge \exists w\,(z = x_1{\cdot}w) \to \exists w\,(x = x_1{\cdot}w))$.

3.11 Общезначимость и выполнимость формул языка первого порядка

[УВП, 2.10], **[П1, 5.5]**, **[ЛМ, II.5]**, **[ВШ2, 4.1]**, **[Мен, 2.2]**, [Кли, 17–19], [КД, с. 50–51, 81–84, 123], [Bil, 6], [Сто, 3.8]

Лемма 3.68. *Если u и v — различные переменные, c и d — константы, то $s[c/u][d/v]$ совпадает с $s[d/v][c/u]$ и $A[c/u][d/v]$ совпадает с $A[d/v][c/u]$.*

Доказательство. Лемма доказывается индукцией по построению терма s и формулы A. □

Определение 3.69. Пусть A — формула сигнатуры Ω и $\mathrm{FV}(A) = \{v_1, \dots, v_n\}$, где все переменные v_i различные.

1. Формула A называется *общезначимой* (*тождественно истинной*), если для любой интерпретации $\mathfrak{M} = \langle M, \Omega\rangle$ сигнатуры Ω и для любых $a_1, \dots, a_n \in M$ имеет место $\mathfrak{M} \vDash A[\underline{a_1}/v_1]\dots[\underline{a_n}/v_n]$.
2. Формула A называется *выполнимой*, если для некоторой интерпретации $\mathfrak{M} = \langle M, \Omega\rangle$ сигнатуры Ω и для некоторых $a_1, \dots, a_n \in M$ имеет место $\mathfrak{M} \vDash A[\underline{a_1}/v_1]\dots[\underline{a_n}/v_n]$.

(П1, с. 37.)

Замечание 3.70. Корректность определения 3.69 следует из леммы 3.68.

Замечание 3.71. Замкнутая формула A сигнатуры Ω общезначима тогда и только тогда, когда для любой интерпретации $\mathfrak{M}$ сигнатуры Ω имеет место $\mathfrak{M} \vDash A$.

Замечание 3.72. Замкнутая формула A сигнатуры Ω выполнима тогда и только тогда, когда для некоторой интерпретации $\mathfrak{M}$ сигнатуры Ω имеет место $\mathfrak{M} \vDash A$.

Упражнение 3.73. Общезначима ли формула $\exists x\,\forall y\,R(x, y) \to \forall y\,\exists x\,R(x, y)$?

Ответ 3.73. Да.

Упражнение 3.74. Общезначима ли формула $\forall y\,\exists x\,R(x, y) \to \exists x\,\forall y\,R(x, y)$?

Ответ 3.74. Нет. Для доказательства необщезначимости рассмотрим интерпретацию с носителем $\{2, 3\}$, определённую так: $\overline{R}(a_1, a_2) = \text{И}$ тогда и только тогда, когда $a_1 \neq a_2$.

Замечание 3.75. Формула $\forall v\,A$ общезначима тогда и только тогда, когда формула A общезначима.

Теорема 3.76. *Каждая общезначимая формула выполнима.*

Доказательство. Пусть формула A сигнатуры Ω общезначима и $\mathrm{FV}(A) = \{v_1, \dots, v_n\}$. Рассмотрим простейшую интерпретацию $\mathfrak{M} = \langle M, \Omega\rangle$, где $M = \{a_0\}$ и всем предикатным символам ставится в соответствие тождественно истинный предикат. По определению общезначимости $\mathfrak{M} \vDash A[\underline{a_0}/v_1]\dots[\underline{a_0}/v_n]$. Следовательно, формула A выполнима. □

Упражнение 3.77. Общезначима ли формула $\exists x\,P(x) \vee \exists x\,\neg P(x)$? Выполнима ли она?

Ответ 3.77. Общезначима.

Упражнение 3.78. Общезначима ли формула $\exists x\,P(x) \wedge \exists x\,\neg P(x)$? Выполнима ли она?

Ответ 3.78. Выполнима, но не общезначима.

Упражнение 3.79. Общезначима ли формула $\forall x\, P(x) \wedge \forall x\, \neg P(x)$? Выполнима ли она?

Ответ 3.79. Невыполнима.

Теорема 3.80. *Формула A общезначима тогда и только тогда, когда формула $\neg A$ невыполнима.*

Доказательство. Теорема непосредственно следует из определений. □

Замечание 3.81. Пусть в формуле A все предикатные символы нульместны. Формула A общезначима тогда и только тогда, когда её естественный перевод в логику высказываний является тавтологией. При этом переводе предикатные символы заменяются на пропозициональные переменные, причём разные предикатные символы заменяются на разные пропозициональные переменные.

3.12 Равносильность формул языка первого порядка

[УВП, 2.10], **[П1, 5.6]**, **[ЛМ, II.5]**, **[ВШ2, 4.1]**, **[Мен, 2.2]**, [Кли, 19, 24], [КД, с. 85–87, 123]

Определение 3.82. Формулы A и B сигнатуры Ω называются *равносильными* (*эквивалентными*) (обозначение $A \sim B$), если формула $A \leftrightarrow B$ общезначима.

Лемма 3.83. *Если $v \notin \mathrm{FV}(A)$, то $A[t/v]$ совпадает с A.*

Доказательство. Лемма доказывается индукцией по построению формулы A. □

Лемма 3.84. *Пусть A и B — формулы сигнатуры Ω и $\mathrm{FV}(A) \cup \mathrm{FV}(B) \subseteq \{v_1, \ldots, v_n\}$, где все переменные v_i различные. Тогда следующие условия равносильны.*

1. $A \sim B$.
2. *Для любой интерпретации $\mathfrak{M} = \langle M, \Omega \rangle$ сигнатуры Ω и для любых элементов $a_1, \ldots, a_n \in M$ истинностные значения формул $A[\underline{a_1}/v_1]\ldots[\underline{a_n}/v_n]$ и $B[\underline{a_1}/v_1]\ldots[\underline{a_n}/v_n]$ в $\mathfrak{M}$ совпадают.*

Доказательство. В силу леммы 3.83 достаточно провести доказательство для случая, когда $\mathrm{FV}(A) \cup \mathrm{FV}(B) = \{v_1, \ldots, v_n\}$.

Согласно определению общезначимость $A \leftrightarrow B$ означает, что для любой интерпретации $\mathfrak{M} = \langle M, \Omega \rangle$ сигнатуры Ω и для любых $a_1, \ldots, a_n \in M$ имеет место $[(A \leftrightarrow B)[\underline{a_1}/v_1]\ldots[\underline{a_n}/v_n]]^{\mathfrak{M}} = \text{И}$. □

Теорема 3.85. *Отношение $\sim$ рефлексивно, симметрично и транзитивно.*

(УВП, теорема 4, с. 41.)

3.13 Некоторые равносильности с кванторами

[УВП, 2.10], **[П1, 5.6]**, **[ЛМ, II.5]**

Теорема 3.86 (некоторые законы о кванторах).

1. $\neg\exists v\, A \sim \forall v\, \neg A$.
2. $\neg\forall v\, A \sim \exists v\, \neg A$.
3. *Если $v \notin \mathrm{FV}(B)$, то $\exists v\, A \wedge B \sim \exists v\, (A \wedge B)$.*
4. *Если $v \notin \mathrm{FV}(B)$, то $\forall v\, A \wedge B \sim \forall v\, (A \wedge B)$.*
5. *Если $v \notin \mathrm{FV}(B)$, то $\exists v\, A \vee B \sim \exists v\, (A \vee B)$.*
6. *Если $v \notin \mathrm{FV}(B)$, то $\forall v\, A \vee B \sim \forall v\, (A \vee B)$.*

7. $\exists v\, A \lor \exists v\, B \sim \exists v\, (A \lor B)$.
8. $\forall v\, A \land \forall v\, B \sim \forall v\, (A \land B)$.
9. *Если* $v \notin \mathrm{FV}(A)$, *то* $\exists v\, A \sim A$.
10. *Если* $v \notin \mathrm{FV}(A)$, *то* $\forall v\, A \sim A$.
11. $\exists u\, \exists v\, A \sim \exists v\, \exists u\, A$.
12. $\forall u\, \forall v\, A \sim \forall v\, \forall u\, A$.

(П1, теорема 5.2, с. 38–39.)

(УВП, теорема 2, с. 39.)

(ЛМ, Упражнение II.5.16.)

Доказательство. Убедимся, что справедливо утверждение 1. Сначала докажем, что $\neg\exists v\, A \sim \forall v\, \neg A$, для случая, когда $\mathrm{FV}(A) \subseteq \{v\}$. Для этого необходимо проверить, что для любой интерпретации $\mathfrak{M} = \langle M, \Omega\rangle$ сигнатуры Ω условия

$$[\neg\exists v\, A]^{\mathfrak{M}} = \text{И} \tag{1}$$

и

$$[\forall v\, \neg A]^{\mathfrak{M}} = \text{И} \tag{2}$$

равносильны. Условие (1) означает, что неверно, что для некоторого $a \in M$ имеет место $[A[\,\underline{a}\,/v]]^{\mathfrak{M}} = \text{И}$. Условие (2) означает, что для каждого $a \in M$ имеет место $[A[\,\underline{a}\,/v]]^{\mathfrak{M}} = \text{Л}$. Следовательно, условия (1) и (2) равносильны.

Докажем теперь $\neg\exists v\, A \sim \forall v\, \neg A$ в общем случае. Пусть $\mathrm{FV}(A) \setminus \{v\} = \{v_1, \ldots, v_n\}$, где все переменные v_i различные. Необходимо доказать, что для любой интерпретации $\mathfrak{M} = \langle M, \Omega\rangle$ сигнатуры Ω и для любых $a_1, \ldots, a_n \in M$ имеет место $[(\neg\exists v\, A \leftrightarrow \forall v\, \neg A)[\,\underline{a_1}\,/v_1]\ldots[\,\underline{a_n}\,/v_n]]^{\mathfrak{M}} = \text{И}$, то есть $[\neg\exists v\, A[\,\underline{a_1}\,/v_1]\ldots[\,\underline{a_n}\,/v_n]]^{\mathfrak{M}} = [\forall v\, \neg A[\,\underline{a_1}\,/v_1]\ldots[\,\underline{a_n}\,/v_n]]^{\mathfrak{M}}$. Тем самым, общий случай сведён к уже доказанному частному случаю, так как $\mathrm{FV}(A[\,\underline{a_1}\,/v_1]\ldots[\,\underline{a_n}\,/v_n]) \subseteq \{v\}$.

Убедимся, что справедливо утверждение 3. Докажем, что $\exists v\, A \land B \sim \exists v\, (A \land B)$, для случая, когда $\mathrm{FV}(A) \subseteq \{v\}$ и $\mathrm{FV}(B) = \varnothing$ (общий случай сводится к этому частному случаю). Для этого необходимо проверить, что для любой интерпретации $\mathfrak{M} = \langle M, \Omega\rangle$ сигнатуры Ω условия

$$[\exists v\, A \land B]^{\mathfrak{M}} = \text{И} \tag{3}$$

и

$$[\exists v\, (A \land B)]^{\mathfrak{M}} = \text{И} \tag{4}$$

равносильны. Условие (3) означает, что $[B]^{\mathfrak{M}} = \text{И}$ и для некоторого $a \in M$ имеет место $[A[\,\underline{a}\,/v]]^{\mathfrak{M}} = \text{И}$. Условие (4) означает, что для некоторого $b \in M$ имеют место равенства $[A[\,\underline{b}\,/v]]^{\mathfrak{M}} = \text{И}$ и $[B[\,\underline{b}\,/v]]^{\mathfrak{M}} = \text{И}$. Согласно лемме 3.83 $B[\,\underline{b}\,/v]$ совпадает с B. Следовательно, условия (3) и (4) равносильны.

Убедимся, что справедливо утверждение 7. Докажем $\exists v\, A \lor \exists v\, B \sim \exists v\, (A \lor B)$ для случая, когда $\mathrm{FV}(A) \subseteq \{v\}$ и $\mathrm{FV}(B) \subseteq \{v\}$ (общий случай снова сводится к этому частному случаю). Для этого необходимо проверить, что для любой интерпретации $\mathfrak{M} = \langle M, \Omega\rangle$ сигнатуры Ω условия

$$[\exists v\, A \lor \exists v\, B]^{\mathfrak{M}} = \text{И} \tag{5}$$

и

$$[\exists v\, (A \lor B)]^{\mathfrak{M}} = \text{И} \tag{6}$$

равносильны. Условие (5) означает, что для некоторого $a_1 \in M$ имеет место $[A[\,\underline{a_1}\,/v]]^{\mathfrak{M}} = \text{И}$ или для некоторого $a_2 \in M$ имеет место $[B[\,\underline{a_2}\,/v]]^{\mathfrak{M}} = \text{И}$. Условие (6) означает, что для некоторого $b \in M$

имеет место $[A[\underline{b}/v]]^{\mathfrak{M}} = \text{И}$ или $[B[\underline{b}/v]]^{\mathfrak{M}} = \text{И}$. Чтобы вывести (6) из (5), рассмотрим два случая. Если $[A[\underline{a_1}/v]]^{\mathfrak{M}} = \text{И}$, то в качестве b выберем a_1. Если $[B[\underline{a_2}/v]]^{\mathfrak{M}} = \text{И}$, то в качестве b выберем a_2. Аналогично можно вывести (5) из (6).

Убедимся, что справедливо утверждение 9. Докажем $\exists v\, A \sim A$ для случая, когда $\mathrm{FV}(A) = \varnothing$ (общий случай снова сводится к этому частному случаю). Для этого необходимо проверить, что для любой интерпретации $\mathfrak{M} = \langle M, \Omega\rangle$ сигнатуры Ω условия

$$[\exists v\, A]^{\mathfrak{M}} = \text{И} \tag{7}$$

и

$$[A]^{\mathfrak{M}} = \text{И} \tag{8}$$

равносильны. Условие (7) означает, что для некоторого $a \in M$ имеет место $[A[\underline{a}/v]]^{\mathfrak{M}} = \text{И}$. Согласно лемме 3.83 $A[\underline{a}/v]$ совпадает с A. Следовательно, условия (7) и (8) равносильны.

Убедимся, что справедливо утверждение 11. Докажем $\exists u\, \exists v\, A \sim \exists v\, \exists u\, A$ для случая, когда $\mathrm{FV}(A) \subseteq \{u, v\}$ (общий случай снова сводится к этому частному случаю). Если u и v обозначают одну и ту же индивидную переменную, то формулы $\exists u\, \exists v\, A$ и $\exists v\, \exists u\, A$ просто совпадают. Пусть u и v — различные переменные. Необходимо проверить, что для любой интерпретации $\mathfrak{M} = \langle M, \Omega\rangle$ сигнатуры Ω условия

$$[\exists u\, \exists v\, A]^{\mathfrak{M}} = \text{И} \tag{9}$$

и

$$[\exists v\, \exists u\, A]^{\mathfrak{M}} = \text{И} \tag{10}$$

равносильны. Условие (9) означает, что для некоторого $a_1 \in M$ и некоторого $a_2 \in M$ имеет место $[A[\underline{a_1}/u][\underline{a_2}/v]]^{\mathfrak{M}} = \text{И}$. Условие (10) означает, что для некоторого $b_1 \in M$ и некоторого $b_2 \in M$ имеет место $[A[\underline{b_1}/v][\underline{b_2}/u]]^{\mathfrak{M}} = \text{И}$. Чтобы вывести (10) из (9), в качестве b_1 выберем a_2, в качестве b_2 выберем a_1 и применим лемму 3.68. Аналогично можно вывести (9) из (10). $\square$

Замечание 3.87.

1. Если $A \sim B$ и A общезначима, то B общезначима.
2. Если $A \sim B$ и A выполнима, то B выполнима.

Упражнение 3.88. Равносильны ли формулы $\forall x\, \exists y\, R(x, y)$ и $\exists y\, \forall x\, R(x, y)$?
Ответ 3.88. Нет.
Упражнение 3.89. Равносильны ли формулы $\neg\forall x\, (P(x) \to \neg\forall z\, R(x, z))$ и $\exists x\, (P(x) \to \forall z\, R(x, z))$?
Ответ 3.89. Нет.

3.14 Замыкание формулы

Определение 3.90. Замыканием формулы A со свободными переменными $\{v_1, \ldots, v_n\}$ называется формула $\forall v_1 \ldots \forall v_n\, A$.

Лемма 3.91. *Все замыкания формулы A равносильны друг другу.*

Определение 3.92 (истинность незамкнутой формулы в $\mathfrak{M}$). Пусть $\mathrm{FV}(A) \neq \varnothing$. Формула A *истинна* в интерпретации $\mathfrak{M}$, если замыкание формулы A истинна в интерпретации $\mathfrak{M}$.

Замечание 3.93. В силу леммы 3.91 определение 3.92 корректно.

3.15 Теорема о тавтологиях

[УВП, 2.10]

Определение 3.94. Пусть $P_1, \dots, P_k$ — различные пропозициональные переменные. Пусть C — формула логики высказываний, не содержащая других пропозициональных переменных, кроме $P_1, \dots, P_k$. Пусть $D_1, \dots, D_k$ — формулы сигнатуры Ω. Тогда через $C(P_1 \backslash D_1, \dots, P_k \backslash D_k)$ обозначается результат одновременной подстановки в формулу C формул $D_1, \dots, D_k$ вместо различных переменных $P_1, \dots, P_k$.

Теорема 3.95 (о подстановке, без доказательства). *Пусть $P_1, \dots, P_k$ — различные пропозициональные переменные. Пусть A — формула логики высказываний, не содержащая других пропозициональных переменных, кроме $P_1, \dots, P_k$. Пусть $D_1, \dots, D_k$ — формулы сигнатуры Ω. Если формула A — тавтология, то формула $A(P_1 \backslash D_1, \dots, P_k \backslash D_k)$ общезначима.*

(УВП, теорема 1, с. 38.)

Доказательство. Докажем теорему сначала для случая, когда формулы $D_1, \dots, D_k$ замкнуты. Рассмотрим произвольную интерпретацию $\mathfrak{M} = \langle M, \Omega \rangle$ сигнатуры Ω. Определим оценку пропозициональных переменных так: $g(P_i) = [D_i]^{\mathfrak{M}}$ для каждого индекса $i \leqslant k$. Индукцией по построению пропозициональной формулы B, не содержащая других пропозициональных переменных, кроме $P_1, \dots, P_k$, можно доказать, что истинностное значение формулы B при оценке g совпадает с $[B(P_1 \backslash D_1, \dots, P_k \backslash D_k)]^{\mathfrak{M}}$. Пусть формула A — тавтология. Тогда $[A(P_1 \backslash D_1, \dots, P_k \backslash D_k)]^{\mathfrak{M}} = \text{И}$, что и требовалось доказать.

Теперь докажем теорему в общем случае. Пусть $\mathrm{FV}(D_1) \cup \ldots \cup \mathrm{FV}(D_k) = \{v_1, \dots, v_n\}$, где все переменные v_i различные. Пусть даны интерпретация $\mathfrak{M} = \langle M, \Omega \rangle$ и элементы $a_1, \dots, a_n \in M$. Надо доказать, что $[A(P_1 \backslash D_1, \dots, P_k \backslash D_k)[\underline{a_1}/v_1] \dots [\underline{a_n}/v_n]]^{\mathfrak{M}} = \text{И}$. Осталось применить эту же теорему для сигнатуры $\Omega(M)$ и замкнутых формул $D_i[\underline{a_1}/v_1] \dots [\underline{a_n}/v_n]$, где $1 \leqslant i \leqslant k$. □

Теорема 3.96. *Пусть $P_1, \dots, P_k$ — различные пропозициональные переменные. Пусть A и B — формулы логики высказываний, не содержащие других пропозициональных переменных, кроме $P_1, \dots, P_k$. Пусть $D_1, \dots, D_k$ — формулы сигнатуры Ω. Если $A \sim B$, то $A(P_1 \backslash D_1, \dots, P_k \backslash D_k) \sim B(P_1 \backslash D_1, \dots, P_k \backslash D_k)$.*

Доказательство. Теорема непосредственно следует из теорем 2.41 и 3.95 и определений. □

Пример 3.97. Из примера 2.31 и теоремы 3.96 следует, что $D_1 \to D_2 \sim \neg D_2 \to \neg D_1$.

3.16 Теорема о замене

[УВП, 2.10]

Определение 3.98. Если C и D — формулы сигнатуры Ω, а P — нульместный предикатный символ сигнатуры Ω, то через $C(P \backslash D)$ обозначим результат подстановки формулы D вместо P в формулу C.

Формальное определение даётся с помощью индукции по построению формулы C.

$$
\begin{aligned}
&P(P\backslash D) \rightleftharpoons D,\\
&C(P\backslash D) \rightleftharpoons C, \text{ если } C \text{ — атомарная формула, отличная от } P,\\
&(\forall v\, A)(P\backslash D) \rightleftharpoons \forall v\, (A(P\backslash D)),\\
&(\exists v\, A)(P\backslash D) \rightleftharpoons \exists v\, (A(P\backslash D)),\\
&(\neg A)(P\backslash D) \rightleftharpoons \neg(A(P\backslash D)),\\
&(A \wedge B)(P\backslash D) \rightleftharpoons (A(P\backslash D)) \wedge (B(P\backslash D)),\\
&(A \vee B)(P\backslash D) \rightleftharpoons (A(P\backslash D)) \vee (B(P\backslash D)),\\
&(A \to B)(P\backslash D) \rightleftharpoons (A(P\backslash D)) \to (B(P\backslash D)).
\end{aligned}
$$

Лемма 3.99. *Если $A \sim B$, то $\neg A \sim \neg B$, $\forall v\, A \sim \forall v\, B$, $\exists v\, A \sim \exists v\, B$. Если $A_1 \sim B_1$ и $A_2 \sim B_2$, то $A_1 \wedge A_2 \sim B_1 \wedge B_2$, $A_1 \vee A_2 \sim B_1 \vee B_2$, $A_1 \to A_2 \sim B_1 \to B_2$.*

(УВП, теорема 3, с. 40.)

Доказательство. Приведём доказательство утверждения про квантор существования. Пусть A и B — формулы сигнатуры Ω и $A \sim B$. Докажем, что $\exists v\, A \sim \exists v\, B$ для случая, когда $\mathrm{FV}(A) \cup \mathrm{FV}(B) \subseteq \{v\}$ (общий случай сводится к этому частному случаю).

Рассмотрим произвольную интерпретацию $\mathfrak{M} = \langle M, \Omega\rangle$ сигнатуры Ω. Надо доказать, что условия

$$[\exists v\, A]^{\mathfrak{M}} = \text{И} \tag{11}$$

и

$$[\exists v\, B]^{\mathfrak{M}} = \text{И} \tag{12}$$

равносильны. Пусть выполняется (11). Это означает, что для некоторого $a \in M$ имеет место $[A[\,\underline{a}\,/v]]^{\mathfrak{M}} = \text{И}$. Необходимо проверить, что для некоторого $b \in M$ имеет место $[B[\,\underline{b}\,/v]]^{\mathfrak{M}} = \text{И}$. Для этого в качестве b выберем a и воспользуемся тем, что $[A[\,\underline{a}\,/v]]^{\mathfrak{M}} = [B[\,\underline{a}\,/v]]^{\mathfrak{M}}$, так как $A \sim B$. □

Теорема 3.100 (об эквивалентной замене). *Если $A \sim B$, то $C(P\backslash A) \sim C(P\backslash B)$.*

(П1, теорема 5.3, с. 39.)

(УВП, теорема 5, с. 41.)

Доказательство. Теорема доказывается индукцией по построению формулы C. В шаге индукции используется лемма 3.99. □

Пример 3.101. Из примера 3.97 и теоремы 3.100 следует, что

$$\exists y\, \forall x\, (R(x,x) \to R(y,x)) \sim \exists y\, \forall x\, (\neg R(y,x) \to \neg R(x,x)).$$

3.17 Переименование связанных переменных

[ВШ2, 4.6], [КД, с. 85–86]

3.102. Если в формуле A заменить все связанные вхождения переменной v на u, где u — новая переменная, не встречающаяся в формуле A, то смысл формулы от этого не изменится. Такое преобразование формулы называют *переименованием связанной переменной*.

Пример 3.103. Для действительных чисел можно доказать равносильность условий $x < y$ и $\exists z\,(z > 0 \wedge x \cdot z < y \cdot z)$. Вторую формулу можно заменить на $\exists w\,(w > 0 \wedge x \cdot w < y \cdot w)$, но нельзя заменить на $\exists z\,(z > 0 \wedge x \cdot z < w \cdot z)$.

Лемма 3.104. *Если переменная u не встречается в формуле A, то $A[u/v][t/u]$ совпадает с $A[t/v]$.*

Доказательство. Лемма доказывается индукцией по построению формулы A. □

Теорема 3.105. *Если переменная u не встречается в формуле A, то имеют место равносильности $\forall v\, A \sim \forall u\, A[u/v]$ и $\exists v\, A \sim \exists u\, A[u/v]$.*

Доказательство. Теорема непосредственно следует из определений и леммы 3.104. □

Упражнение 3.106. Общезначима ли формула $\exists y\,(R(x,y) \vee \forall z\, \neg R(y,z))$?

Ответ 3.106. Да.

3.18 Корректные подстановки

[ВШ2, 4.2], **[УВП, 2.6]**, **[Мен, 2.1]**, **[ЛМ, II.4]**, [П1, 5.5], [Кли, 18], [КД, с. 65–69, 121–122], [Сто, 2.8], [Шён, 2.4], [Bil, 7]

Определение 3.107. Терм t называется *свободным для переменной v в формуле C*, если никакое свободное вхождение v в C не находится в области действия кванторов по переменным, входящим в терм t.

Можно дать более формальное определение индукцией по построению формулы.

1. Если C — атомарная формула, то t свободен для v в C.
2. Терм t свободен для v в $\neg A$ тогда и только тогда, когда t свободен для v в A.
3. Терм t свободен для v в $A \to B$ тогда и только тогда, когда t свободен для v в A и t свободен для v в B. Аналогично для $\wedge$ и $\vee$.
4. Терм t свободен для v в $\forall u\, A$ тогда и только тогда, когда выполняется хотя бы одно из следующих двух условий:
   (a) $v \notin \mathrm{FV}(\forall u\, A)$,
   (b) терм t свободен для v в A и терм t не содержит переменную u.

   Аналогично для $\exists$.

Определение 3.108. Подстановка терма t вместо переменной v в формулу C называется *свободной* (или *корректной*), если t свободен для v в формуле C.

3.109. Только свободные подстановки являются «осмысленными».

Пример 3.110. Терм y не является свободным для переменной x в формуле $\forall y\,(x \leqslant y)$. Поэтому подстановка y вместо x в эту формулу является некорректной. Кстати, здесь, конечно, x и y — различные переменные.

Теорема 3.111 (без доказательства). *Если формула A общезначима и терм t свободен для переменной v в формуле A, то формула $A[t/v]$ общезначима.*

Пример 3.112. Обозначим через A общезначимую формулу

$$\exists x\,\forall y\, y+z>x \to \forall y\,\exists x\, y+z>x.$$

Обозначим через t терм $w\cdot w$. Формула $A[t/z]$ имеет вид

$$\exists x\,\forall y\, y+(w\cdot w)>x \to \forall y\,\exists x\, y+(w\cdot w)>x.$$

Согласно теореме 3.111 эта формула является общезначимой.

Пример 3.113. Обозначим через A общезначимую формулу

$$\exists y\,(R(x,y)\vee\forall z\,\neg R(y,z)).$$

Терм y не является свободным для x в формуле A. Формула $A[y/x]$ имеет вид $\exists y\,(R(y,y)\vee\forall z\,\neg R(y,z))$. Эта формула не является общезначимой. Например, она ложна в интерпретации с носителем $\{2,3\}$, определённой так: $\overline{R}(a_1,a_2)=\text{И}$ тогда и только тогда, когда $a_1\neq a_2$.

3.19 Формулы $\forall v\, A\to A[t/v]$ и $A[t/v]\to\exists v\, A$

[УВП, 3.4], **[ВШ2, 4.3]**, **[Мен, 2.2]**, **[П1, 5.5]**, [Кли, 18]

Пример 3.114. Формулы $R(c,c)\to\exists x\,R(x,x)$ и $\forall x\,R(x,x)\to R(c,c)$ общезначимы.

Лемма 3.115. *Если* $\mathrm{FV}(A)=\varnothing$, *то формула* $A\to\exists v\,A$ *общезначима.*

Доказательство. Согласно теореме 3.86 формула $A\leftrightarrow\exists v\,A$ общезначима, так как $v\notin\mathrm{FV}(A)$. □

Лемма 3.116. *Если* $\mathrm{FV}(A)=\{v\}$, *то формула* $A\to\exists v\,A$ *общезначима.*

Доказательство. Пусть дана такая формула A сигнатуры Ω, что $\mathrm{FV}(A)=\{v\}$. Очевидно, $\mathrm{FV}(A\to\exists v\,A)=\{v\}$. Пусть даны интерпретация $\mathfrak{M}=\langle M,\Omega\rangle$ и элемент $b\in M$. Надо доказать, что

$$[(A\to\exists v\,A)[\,\underline{b}\,/v]]^{\mathfrak{M}}=\text{И},$$

то есть

$$[(A[\,\underline{b}\,/v]\to\exists v\,A)]^{\mathfrak{M}}=\text{И}.$$

Если $[A[\,\underline{b}\,/v]]^{\mathfrak{M}}=\text{Л}$, то импликация истинна. Если же $[A[\,\underline{b}\,/v]]^{\mathfrak{M}}=\text{И}$, то $[\exists v\,A]^{\mathfrak{M}}=\text{И}$ (согласно определению истинности) и снова импликация истинна. □

Пример 3.117. Формула $R(x,x)\to\exists x\,R(x,x)$ общезначима.

Лемма 3.118. *Формула* $B\to\exists v\,B$ *общезначима.*

Доказательство. Пусть дана формула B сигнатуры Ω и $\mathrm{FV}(B)\setminus\{v\}=\{v_1,\dots,v_n\}$. Пусть даны интерпретация $\mathfrak{M}=\langle M,\Omega\rangle$ и элементы $a_1,\dots,a_n\in M$. Надо доказать, что

$$[(B\to\exists v\,B)[\,\underline{a_1}\,/v_1]\dots[\,\underline{a_n}\,/v_n]]^{\mathfrak{M}}=\text{И},$$

то есть

$$[B[\,\underline{a_1}\,/v_1]\dots[\,\underline{a_n}\,/v_n]\to\exists v\,B[\,\underline{a_1}\,/v_1]\dots[\,\underline{a_n}\,/v_n]]^{\mathfrak{M}}=\text{И}.$$

Обозначим $A=B[\,\underline{a_1}\,/v_1]\dots[\,\underline{a_n}\,/v_n]$. Очевидно, $\mathrm{FV}(A)\subseteq\{v\}$. Осталось применить лемму 3.116 или 3.115 к формуле $A\to\exists v\,A$. □

Лемма 3.119. *Формула* $\forall v\,A\to A$ *общезначима.*

Доказательство. Положив $B = \neg A$ и применив лемму 3.118, получим, что формула $\neg A \to \exists v\, \neg A$ общезначима. Согласно примеру 3.97 и замечанию 3.87 формула $\neg\exists v\, \neg A \to \neg\neg A$ общезначима. Осталось применить теоремы 3.86 и 3.100. □

Теорема 3.120. *Если терм t свободен для переменной v в формуле A, то формулы $\forall v\, A \to A[t/v]$ и $A[t/v] \to \exists v\, A$ общезначимы.*

Доказательство. По лемме 3.119 формула $\forall v\, A \to A$ — тавтология. По теореме 3.111 формула $(\forall v\, A \to A)[t/v]$ — тавтология, так как терм t свободен для переменной v в формуле $\forall v\, A \to A$. Из определения 3.47 следует, что $(\forall v\, A \to A)[t/v]$ совпадает с $\forall v\, A \to A[t/v]$.

Второе утверждение теоремы доказывается аналогично. □

3.20 Предварённые формулы

[УВП, 2.11], **[Мен, 2.10]**, **[П1, 5.7]**, **[ЛМ, II.5]**, [ВШ2, 4.7], [Кли, 25], [Шён, 3.5], [КД, с. 87–88]

Определение 3.121. *Предварённой формулой* называется любая формула вида $Q_1 v_1 \ldots Q_n v_n\, A$, где $Q_1, \ldots, Q_n$ — кванторы, а A — бескванторная формула. Формальное определение индуктивное.

1. Каждая бескванторная формула является предварённой формулой.
2. Если A — предварённая формула и v — индивидная переменная, то $\forall v\, A$ и $\exists v\, A$ являются предварёнными формулами.

Пример 3.122. Формула $\forall x\, \exists y\, (R(x, y) \vee R(z, z))$ является предварённой формулой.

Пример 3.123. Формула $\forall x\, \exists y\, R(x, y) \vee R(z, z)$ не является предварённой формулой. С восстановленными скобками она имеет вид $(\forall x\, \exists y\, R(x, y) \vee R(z, z))$, то есть первый символ — скобка, а не квантор.

Теорема 3.124 (о приведении формул к предварённой форме). *Каждая формула равносильна некоторой предварённой формуле.*

(П1, теорема 5.4, с. 39.)

(УВП, теорема 7, с. 42.)

Доказательство. Теорема доказывается индукцией по построению формулы. В шаге индукции используются теоремы 3.86, 3.105 и 3.100. □

Определение 3.125. Нахождение предварённой формулы, эквивалентной данной формуле, называется *приведением к предварённой нормальной форме*.

Упражнение 3.126. Привести к предварённой нормальной форме формулу

$$(\neg\exists x\, \neg\exists z\, \neg\exists y\, Q(x, y, z)) \to P(x).$$

Ответ 3.126. $\exists w\, \forall z\, \exists y\, (Q(w, y, z) \vee P(x))$.

Упражнение 3.127. Привести к предварённой нормальной форме формулу

$$\exists w\, (y = x \cdot w) \wedge \exists w\, (z = x \cdot w) \wedge \forall x_1\, (\exists w\, (y = x_1 \cdot w) \wedge \exists w\, (z = x_1 \cdot w) \to \exists w\, (x = x_1 \cdot w)).$$

Ответ 3.127. $\forall x_1\, \forall w_3\, \forall w_4\, \exists w_5\, \exists w_1\, \exists w_2\, (y = x \cdot w_1 \wedge z = x \cdot w_2 \wedge (y = x_1 \cdot w_3 \wedge z = x_1 \cdot w_4 \to x = x_1 \cdot w_5)$.

Упражнение 3.128. Привести к предварённой нормальной форме формулу

$$\forall y\, (\forall x\, (x \cdot y = x) \to y = e).$$

Ответ 3.128. $\forall y\, \exists x\, (x \cdot y = x \to y = e)$.

3.21 Аксиоматический метод

[УВП, 3.1], **[П1, 5.8]**, [Сто, 3.1–3.4], [Шён, 1.1–1.2]

3.129. *Аксиоматическим методом* называется способ построения научной теории, при котором некоторые утверждения, называемые *аксиомами*, принимаются без доказательства, а все остальные утверждения этой теории, называемые *теоремами*, получаются как логические следствия аксиом.

Аксиоматический метод в математике впервые был использован Евклидом в III веке до н. э.

Открытие в XIX веке неевклидовой геометрии Николаем Ивановичем Лобачевским и Яношем Больяй и построение различных моделей геометрии Лобачевского средствами геометрии Евклида привели к осознанию возможности рассматривать аксиоматическую теорию формально.

В *формальной аксиоматической теории* не предполагают какое-либо определённое значение исходных (то есть неопределяемых) понятий. Например, в системе аксиом геометрии, разработанной Давидом Гильбертом на рубеже XIX и XX веков, имеются восемь исходных понятий: «точка», «прямая», «плоскость», отношение связи точки и прямой, отношение связи точки и плоскости, трёхместное отношение «находиться между» (для точек), отношение равенства отрезков, отношение равенства углов. Мы вольны выбирать значения этих понятий каким угодно образом, лишь бы при этом оказывались истинными аксиомы.

3.22 Логическое следование в логике предикатов

[УВП, 3.1–3.2], **[П1, 5.10]**, **[ВШ2, 5.3]**, [Кли, 20, 23], [Сто, 2.9], [Шён, 2.6], [Bil, 6]

Определение 3.130. Пусть T — некоторое множество замкнутых формул сигнатуры Ω. *Моделью* множества T называется интерпретация сигнатуры Ω, в которой истинны все формулы из T.

(УВП, с. 58.)

Определение 3.131. Пусть T — некоторое множество замкнутых формул сигнатуры Ω. Если замкнутая формула A сигнатуры Ω истинна во всех моделях множества T, то говорят, что формула A *логически следует* (*семантически следует*, *следует*) из множества T (обозначение $T \vDash A$).

(УВП, с. 58.)

3.132. Вместо $\{B_1, \ldots, B_n\} \vDash A$ обычно пишут $B_1, \ldots, B_n \vDash A$. Вместо $\varnothing \vDash A$ обычно пишут просто $\vDash A$.

Пример 3.133.

$$\forall x\, \neg R(x,x),\ \forall x\, \forall y\, \forall z\, (R(x,y) \wedge R(y,z) \to R(x,z)) \vDash \forall x\, \forall y\, (R(x,y) \to \neg R(y,x)).$$

Определение 3.134. Пусть T — некоторое множество замкнутых формул сигнатуры Ω. Незамкнутая формула A сигнатуры Ω *логически следует* из множества T, если её замыкание логически следует из множества T.

Замечание 3.135. Формула A общезначима тогда и только тогда, когда $\vDash A$.

Замечание 3.136. Замкнутые формулы A и B равносильны тогда и только тогда, когда $A \vDash B$ и $B \vDash A$.

3.23 Теории первого порядка

[П1, 5.9–5.10], [ВШ2, 4.4, 4.5, 5.3], [УВП, 3.6], [ЛМ, II.7], [КД, с. 103–104, 125], [Bil, 6, 7], [Сто, 3.8]

Определение 3.137. *Теорией первого порядка* (*элементарной теорией*) в сигнатуре Ω называется произвольное множество замкнутых формул сигнатуры Ω. Элементы этого множества называются *аксиомами* этой теории.

(П1, с. 41.)

Пример 3.138. Теория с сигнатурой $\langle e, \cdot, = \rangle$ и аксиомами

1) $\forall x\,(x = x)$,
2) $\forall x\,\forall y\,(x = y \to y = x)$,
3) $\forall x\,\forall y\,\forall z\,(x = y \land y = z \to x = z)$,
4) $\forall x_1\,\forall x_2\,\forall y_1\,\forall y_2\,(x_1 = y_1 \land x_2 = y_2 \to x_1 \cdot x_2 = y_1 \cdot y_2)$,
5) $\forall x\,\forall y\,\forall z\,((x \cdot y) \cdot z = x \cdot (y \cdot z))$,
6) $\forall x\,(x \cdot e = x \land e \cdot x = x)$,
7) $\forall x\,\exists y\,(x \cdot y = e \land y \cdot x = e)$

называется *теорией групп*.

Пример 3.139. Теория с сигнатурой $\langle \cdot, = \rangle$ и аксиомами

1) $\forall x\,(x = x)$,
2) $\forall x\,\forall y\,(x = y \to y = x)$,
3) $\forall x\,\forall y\,\forall z\,(x = y \land y = z \to x = z)$,
4) $\forall x_1\,\forall x_2\,\forall y_1\,\forall y_2\,(x_1 = y_1 \land x_2 = y_2 \to x_1 \cdot x_2 = y_1 \cdot y_2)$,
5) $\forall x\,\forall y\,\forall z\,((x \cdot y) \cdot z = x \cdot (y \cdot z))$

называется *теорией полугрупп*.

Определение 3.140. *Теоремами* теории первого порядка T в сигнатуре Ω называются замкнутые формулы сигнатуры Ω, которые логически следуют из T.

(П1, с. 42.)

3.141. Как видно из предыдущего определения, в данном курсе термин «теория первого порядка» соответствует термину «неформальная аксиоматическая теория» (или «семантическая теория») из учебника [УВП, с. 73].

Пример 3.142. Формула $\forall x\,\forall y\,(x \cdot y = e \to y \cdot x = e)$ является теоремой теории групп.

Пример 3.143. Формула $\forall x\,\forall y\,(x \cdot y = y \cdot x)$ не является теоремой теории групп.

Замечание 3.144. Если A — аксиома теории T, то A является теоремой теории T.

Определение 3.145. Теория называется *совместной*, если она имеет хотя бы одну модель.

(П1, с. 41.)

Пример 3.146. Теория групп является совместной. Например, одноэлементная интерпретация с тождественно истинным значением предикатного символа $=$ является моделью теории групп.

Пример 3.147. Рассмотрим сигнатуру Ω, содержащую двуместный предикатный символ R. Теория с аксиомами $\forall x\,\exists y\,R(x,y)$ и $\forall x\,\neg\exists y\,R(y,x)$ является несовместной.

Пример 3.148. *Наивной теорией множеств* называется теория с сигнатурой $\langle =, \in \rangle$ и аксиомами

1) $\forall x\,\forall y\,(x = y \leftrightarrow \forall z\,(z \in x \leftrightarrow z \in y))$.

2) $\exists x\,\forall y\,(y \in x \leftrightarrow A)$, где x и y — различные переменные и $\mathrm{FV}(A) = \{y\}$.

Наивная теория множеств является несовместной, так как формула $\exists x\,\forall y\,(y \in x \leftrightarrow \neg\, y \in y)$ является ложной в любой интерпретации.

Замечание 3.149. Замкнутая формула A сигнатуры Ω является логическим следствием (то есть теоремой) теории T сигнатуры Ω тогда и только тогда, когда теория $T \cup \{\neg A\}$ является несовместной.
(П1, теорема 5.5, с. 42.)
(УВП, теорема 1 в, с. 58.)

Замечание 3.150. Если теория T сигнатуры Ω несовместна, то все замкнутые формулы сигнатуры Ω являются теоремами этой теории.

Замечание 3.151. Если существует такая замкнутая формула A, что A и $\neg A$ являются теоремами теории T, то теория T несовместна.

3.24 Элементарная теория интерпретации

[ВШ2, 5.3], **[УВП, 3.6]**, [Bil, 6]

Определение 3.152. Пусть дана интерпретация $\mathfrak{M} = \langle M, \Omega \rangle$. *Элементарной теорией* интерпретации $\mathfrak{M}$ называется множество $\mathrm{Th}(\mathfrak{M})$, состоящее из всех замкнутых формул сигнатуры Ω, истинных в интерпретации $\mathfrak{M}$.
(ВШ2, с. 212.)

Замечание 3.153. Элементарная теория интерпретации $\mathfrak{M}$ является совместной.

Замечание 3.154. У элементарной теории интерпретации $\mathfrak{M}$ множество теорем совпадает с множеством аксиом.

Замечание 3.155. Две интерпретации одной и той же сигнатуры элементарно эквивалентны тогда и только тогда, когда их элементарные теории совпадают ($\mathfrak{L} \cong \mathfrak{M}$ тогда и только тогда, когда $\mathrm{Th}(\mathfrak{L}) = \mathrm{Th}(\mathfrak{M})$)

3.25 Полные теории первого порядка

[ВШ2, 5.3], **[УВП, 3.6]**, **[ЛМ, II.6, II.7]**, [КД, с. 158], [Bil, 15]

Определение 3.156. Теория T сигнатуры Ω называется *полной*, если для каждой замкнутой формулы A сигнатуры Ω ровно одна из формул A и $\neg A$ является теоремой теории T.

Замечание 3.157. Каждая полная теория является совместной.
Замечание 3.158. Элементарная теория интерпретации $\mathfrak{M}$ является полной.

3.26 Теории первого порядка с равенством

[ВШ2, 5.1, 5.3], **[Мен, 2.8]**, **[ЛМ, II.7]**, [УВП, 3.4], [П1, 6.5], [КД, с. 106]

Определение 3.159. Теория первого порядка T сигнатуры Ω называется *теорией первого порядка с равенством*, если сигнатура Ω содержит выделенный двуместный предикат $=$ и следующие формулы являются теоремами теории T:

1) $\forall x\,(x = x)$,
2) $\forall x\,\forall y\,(x = y \to y = x)$,
3) $\forall x\,\forall y\,\forall z\,(x = y \land y = z \to x = z)$,
4) $\forall x_1 \ldots \forall x_n\,\forall y_1 \ldots \forall y_n\,(x_1 = y_1 \land \ldots \land x_n = y_n \to f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n))$, где $n > 0$ и f — n-местный функциональный символ из сигнатуры Ω,
5) $\forall x_1 \ldots \forall x_n\,\forall y_1 \ldots \forall y_n\,(x_1 = y_1 \land \ldots \land x_n = y_n \land P(x_1, \ldots, x_n) \to P(y_1, \ldots, y_n))$, где $n > 0$ и P — n-местный предикатный символ из сигнатуры Ω.

Определение 3.160. Теория с сигнатурой $\langle =, < \rangle$ и аксиомами

1) $\forall x\,(x = x)$,
2) $\forall x\,\forall y\,(x = y \to y = x)$,
3) $\forall x\,\forall y\,\forall z\,(x = y \land y = z \to x = z)$,
4) $\forall x_1\,\forall x_2\,\forall y_1\,\forall y_2\,(x_1 = y_1 \land x_2 = y_2 \land x_1 < x_2 \to y_1 < y_2)$,
5) $\forall x\,\neg(x < x)$,
6) $\forall x\,\forall y\,\forall z\,(x < y \land y < z \to x < z)$

называется *теорией частично упорядоченных множеств*. Она является теорией первого порядка с равенством.

Определение 3.161. Если к теории частично упорядоченных множеств добавить аксиому $\forall x\,\forall y\,(x < y \lor x = y \lor y < x)$, то получим *теорию линейно упорядоченных множеств*.

Определение 3.162. Если к теории линейно упорядоченных множеств добавить аксиому $\forall x\,\forall y\,(x < y \to \exists z\,(x < z \land z < y))$, то получим *теорию плотных линейно упорядоченных множеств*.

Определение 3.163. Интерпретация $\mathfrak{M}$ сигнатуры Ω с выделенным двуместным предикатом $=$ называется *нормальной* интерпретацией, если в интерпретации $\mathfrak{M}$ предикатному символу $=$ ставится в соответствие предикат тождества. Если нормальная интерпретация $\mathfrak{M}$ является моделью некоторой теории, то $\mathfrak{M}$ называется *нормальной моделью* этой теории.

Пример 3.164. Пусть $\Omega = \langle e, \cdot, = \rangle$. Интерпретация $\langle \mathbb{Z}, \Omega \rangle$, ставящая в соответствие константе e число 0, функциональному символу $\cdot$ операцию сложения и предикатному символу $=$ отношение сравнимости по модулю 6, является моделью теории групп, но не является нормальной моделью теории групп.

Теорема 3.165. *Пусть теория T сигнатуры Ω является теорией первого порядка с равенством. Пусть u, v_1 и v_2 — различные индивидные переменные, а t — терм сигнатуры Ω. Тогда $T \vDash \forall v_1\,\forall v_2\,(v_1 = v_2 \to t[v_1/u] = t[v_2/u])$.*

Теорема 3.166. *Пусть теория T сигнатуры Ω является теорией первого порядка с равенством. Пусть u, v_1 и v_2 — различные индивидные переменные, а A — формула сигнатуры Ω. Если переменные v_1 и v_2 свободны для u в формуле A, то $T \vDash \forall v_1\,\forall v_2\,(v_1 = v_2 \to (A[v_1/u] \leftrightarrow A[v_2/u]))$.*

Определение 3.167. Когда рассматривают теорию первого порядка с равенством, то можно использовать запись $\exists! v\,A$ (или $\exists_1 v\,A$) как сокращение для формулы $\exists v\,A \land \forall v\,\forall u\,(A \land A[u/v] \to v = u)$, где u — новая переменная, отличная от v и не встречающаяся в формуле A.

3.27 Язык формальной арифметики

[УВП, 2.7], **[Мен, 3.1]**, **[БДж, 9, 14]**, **[ЛМ, II.7]**, **[Кли, 38]**, **[П1, 5.3]**, [КД, с. 75–77, 125–126], [Сто, 3.8], [П2, 23], [Bil, 15]

Определение 3.168. *Сигнатура формальной арифметики* содержит константу 0, одноместный функциональный символ S, двуместные функциональные символы $+$ и $\cdot$ и предикатный символ $=$. Язык первого порядка, заданный этой сигнатурой, называется *языком формальной арифметики* или просто *языком арифметики*. При употреблении инфиксной нотации приоритет у символа $\cdot$ выше, чем у $+$, и обе операции считаются левоассоциативными.

Определение 3.169. *Стандартной интерпретацией языка арифметики* называется интерпретация на множестве $\mathbb{N}$, где $\overline{S}(a) = a + 1$, а остальные символы обозначают нуль, сложение, умножение и равенство.

Определение 3.170. Формулы и термы сигнатуры формальной арифметики называются (для краткости) *арифметическими* формулами и термами соответственно.

Пример 3.171. Пример арифметической формулы: $\exists z\,(x+S(z) = y)$. В стандартной интерпретации эта формула выражает предикат $x < y$.

3.28 Арифметика первого порядка

[УВП, 3.7], **[Мен, 3.1]**, **[БДж, 14]**, **[ЛМ, II.7]**, **[Кли, 38]**, [КД, с. 104–106, 125–126], [Сто, 3.8]

Определение 3.172. *Арифметикой Пеано* (или *формальной арифметикой*) называется теория первого порядка с сигнатурой $\langle 0, S, +, \cdot, = \rangle$ и аксиомами

1) $\forall x\,(x = x)$,
2) $\forall x\,\forall y\,(x = y \to y = x)$,
3) $\forall x\,\forall y\,\forall z\,(x = y \wedge y = z \to x = z)$,
4) $\forall x\,\forall y\,(x = y \to S(x) = S(y))$,
5) $\forall x\,\forall y\,(S(x) = S(y) \to x = y)$,
6) $\forall x\,\neg(S(x) = 0)$,
7) $\forall x\,(x + 0 = x)$,
8) $\forall x\,\forall y\,(x + S(y) = S(x + y))$,
9) $\forall x\,(x \cdot 0 = 0)$,
10) $\forall x\,\forall y\,(x \cdot S(y) = (x \cdot y) + x)$,
11) $A[0/v] \wedge \forall v\,(A \to A[S(v)/v]) \to \forall v\,A$, где A — произвольная арифметическая формула, а v — произвольная переменная.

Пример 3.173. Формулы $(0 \cdot 0 = 0) \wedge \forall x\,(0 \cdot x = 0 \to 0 \cdot S(x) = 0) \to \forall x\,(0 \cdot x = 0)$ и $(x + 0 = 0 + x) \wedge \forall y\,(x + y = y + x \to x + S(y) = S(y) + x) \to \forall y\,(x + y = y + x)$ являются аксиомами арифметики Пеано.

Пример 3.174. Формула $\forall x\,\forall y\,(x + y = y + x)$ является теоремой арифметики Пеано.

Пример 3.175 (возвратная индукция). Формула

$$\forall x\,(\forall y\,(y < x \to P(y)) \to P(x)) \to \forall x\,P(x)$$

является теоремой арифметики Пеано. В доказательстве задействована аксиома

$$\forall y\,(y < 0 \to P(y)) \wedge \forall x\,(\forall y\,(y < x \to P(y)) \to \forall y\,(y < S(x) \to P(y))) \to \\ \to \forall x\,\forall y\,(y < x \to P(y)).$$

Здесь в качестве v используется переменная x, а в качестве A — формула $\forall y\,(y < x \to P(y))$.

4 Исчисление высказываний

4.1. В этом разделе буквы A, B и т. д. обозначают формулы логики высказываний, а буквы Γ, Δ и т. д. обозначают множества формул логики высказываний.

4.1 Аксиомы и правила гильбертовского исчисления высказываний

[ВШ2, 2.1], **[П1, 4.1–4.2]**, [КД, с. 45–48], [Мен, 1.4, 1.6], [Кли, 9], [Bil, 3]

Определение 4.2. Аксиомами *классического исчисления высказываний* являются формулы следующих видов:
1) $A \to (B \to A)$,
2) $(A \to B) \to ((A \to (B \to C)) \to (A \to C))$,
3) $A \wedge B \to A$,
4) $A \wedge B \to B$,
5) $A \to (B \to A \wedge B)$,
6) $A \to A \vee B$,
7) $B \to A \vee B$,
8) $(A \to C) \to ((B \to C) \to (A \vee B \to C))$,
9) $(A \to B) \to ((A \to \neg B) \to \neg A)$,
10) $\neg\neg A \to A$.

Правило вывода modus ponens: $\dfrac{A \quad A \to B}{B}$ (MP).

(Мен, с. 49.)

Определение 4.3 (вывод). *Выводом в исчислении высказываний* (или просто *выводом*) называется конечная последовательность формул, каждая из которых является аксиомой или получается из некоторых предыдущих формул по правилу вывода.

(ВШ2, с. 48.)

(П1, с. 23.)

Пример 4.4. Следующая последовательность формул является выводом:

$$\begin{array}{ll}
P \to Q \vee P & \\
Q \to Q \vee P & \\
(P \to Q \vee P) \to ((Q \to Q \vee P) \to (P \vee Q \to Q \vee P)) & \\
(Q \to Q \vee P) \to (P \vee Q \to Q \vee P) & \text{(MP)} \\
P \vee Q \to Q \vee P & \text{(MP).}
\end{array}$$

Определение 4.5 (выводимая формула). Формула A называется *выводимой* в исчислении высказываний или *теоремой* исчисления высказываний (обозначение $\vdash A$), если существует вывод, в котором последняя формула есть A.

(ВШ2, с. 48.)

(П1, с. 23.)

Пример 4.6. $\vdash P \vee Q \to Q \vee P$.

Определение 4.7 (вывод из гипотез). Пусть Γ — некоторое множество формул. *Выводом из* Γ называется конечная последовательность формул, каждая из которых либо принадлежит множеству Γ, либо является аксиомой, либо получается из предыдущих формул по правилу вывода. Элементы множества Γ называются *гипотезами*.

(ВШ2, с. 50.)

(П1, с. 23.)

Пример 4.8. Следующая последовательность формул является выводом из множества гипотез $\{P \wedge Q\}$:

$$
\begin{array}{ll}
P \wedge Q & \text{(гипотеза)} \\
P \wedge Q \to P & \\
P & \text{(MP)} \\
P \wedge Q \to Q & \\
Q & \text{(MP)} \\
Q \to (P \to Q \wedge P) & \\
P \to Q \wedge P & \text{(MP)} \\
Q \wedge P & \text{(MP).}
\end{array}
$$

Определение 4.9 (выводимость из гипотез). Формула A называется *выводимой из множества формул* Γ (обозначение $\Gamma \vdash A$), если существует вывод из Γ, в котором последняя формула есть A.

(ВШ2, с. 50.)

(П1, с. 23.)

4.10. Вместо $\{B_1, \ldots, B_n\} \vdash A$ обычно пишут $B_1, \ldots, B_n \vdash A$.

Пример 4.11. $P \wedge Q \vdash Q \wedge P$.

4.2 Вывод формулы $A \to A$

[ВШ2, 2.1], **[П1, 4.2]**, **[Мен, 1.4]**, **[Кли, 9]**, **[КД, с. 48]**, **[Bil, 3]**

Лемма 4.12. *Формула $A \to A$ выводима.*

(ВШ2, лемма 1, с. 49.)

(П1, теорема 4.1, с. 24.)

Доказательство.

$$
\begin{array}{ll}
(A \to (A \to A)) \to ((A \to ((A \to A) \to A)) \to (A \to A)) & \\
A \to (A \to A) & \\
(A \to ((A \to A) \to A)) \to (A \to A) & \text{(MP)} \\
A \to ((A \to A) \to A) & \\
A \to A & \text{(MP).}
\end{array}
$$

□

4.3 Корректность исчисления высказываний

[ВШ2, 2.1], **[П1, 4.2]**, [Мен, 1.4], [Кли, 11], [КД, с. 48], [Bil, 4], [Сто, 3.6]

Теорема 4.13 (о корректности). *Если $\vdash A$, то $\vDash A$.*

(ВШ2, теорема 17, с. 48.)

(П1, теорема 4.5, с. 25.)

Доказательство. Теорема доказывается индукцией по длине вывода формулы A. □

Теорема 4.14 (обобщённая теорема о корректности). *Если $\Gamma \vdash A$, то $\Gamma \vDash A$.*

(П1, теорема 4.7, с. 25.)

Доказательство. Теорема доказывается аналогично теореме 4.13. □

4.4 Теорема о дедукции для исчисления высказываний

[ВШ2, 2.1], **[Мен, 1.4]**, **[П1, 4.2]**, [Кли, 10], [Bil, 3]

Теорема 4.15 (о дедукции). *Если* $\Gamma \cup \{A\} \vdash B$, *то* $\Gamma \vdash (A \to B)$.

(Мен, предложение 1.8, с. 40.)

(ВШ2, лемма 2, с. 50.)

(П1, теорема 4.6, с. 25.)

Доказательство. Теорема доказывается индукцией по длине вывода формулы B из множества гипотез $\Gamma \cup \{A\}$.

Если B является аксиомой или принадлежит Γ, то искомый вывод выглядит так:

$$\begin{array}{ll} B & \\ B \to (A \to B) & \\ (A \to B) & \text{(MP).} \end{array}$$

Если B совпадает с A, то используем лемму 4.12.

Если B получена из некоторых предыдущих формул по правилу вывода modus ponens, то эти формулы имеют вид C и $C \to B$. Согласно предположению индукции $\Gamma \vdash (A \to C)$ и $\Gamma \vdash (A \to (C \to B))$. Искомый вывод формулы B из множества гипотез $\Gamma \cup \{A\}$ состоит из этих двух выводов и следующих формул:

$$\begin{array}{ll} (A \to C) \to ((A \to (C \to B)) \to (A \to B)) & \\ (A \to (C \to B)) \to (A \to B) & \text{(MP)} \\ A \to B & \text{(MP).} \end{array}$$

□

4.16. Вместо $\Gamma \cup \{A\} \vdash B$ обычно пишут $\Gamma, A \vdash B$.

Пример 4.17. Можно проверить, что $P \to Q,\ \neg Q \vdash \neg P$:

$$\begin{array}{ll} P \to Q & \\ \neg Q & \\ (P \to Q) \to ((P \to \neg Q) \to \neg P) & \\ (P \to \neg Q) \to \neg P & \text{(MP)} \\ \neg Q \to (P \to \neg Q) & \\ P \to \neg Q & \text{(MP)} \\ \neg P & \text{(MP).} \end{array}$$

Следовательно, $P \to Q \vdash \neg Q \to \neg P$.

Пример 4.18. Из примера 4.11 и теоремы 4.15 следует, что $\vdash P \wedge Q \to Q \wedge P$.

Теорема 4.19. *Пусть* Γ *— некоторое множество формул. Тогда* $\Gamma \vdash (A \to B)$ *в том и только том случае, когда* $\Gamma \cup \{A\} \vdash B$.

(ВШ2, лемма 2, с. 50.)

(П1, теорема 4.6, с. 25.)

Доказательство. Достаточность доказана в теореме 4.15. Необходимость доказывается одним применением правила modus ponens. □

4.5 Свойства выводимости из гипотез

[ВШ2, 2.1], **[П1, 4.2]**, **[Мен, 1.4]**, [Bil, 3–4]

Теорема 4.20 (монотонность). *Если $\Delta \subseteq \Gamma$ и $\Delta \vdash A$, то $\Gamma \vdash A$.*

(П1, теорема 4.2, с. 24.)

(Мен, с. 37.)

Доказательство. Теорема непосредственно следует из определений. □

Теорема 4.21 (компактность). *Если $\Gamma \vdash A$, то существует такое конечное множество $\Delta \subseteq \Gamma$, что $\Delta \vdash A$.*

(П1, теорема 4.4, с. 25.)

(Мен, с. 37.)

Доказательство. Теорема непосредственно следует из определений. □

Теорема 4.22 (транзитивность). *Если $\Gamma \vdash A$ и для каждой формулы $B \in \Gamma$ имеет место $\Delta \vdash B$, то $\Delta \vdash A$.*

(П1, теорема 4.3, с. 24.)

(Мен, с. 37.)

Доказательство. Заменим в выводе формулы A каждую гипотезу на её вывод из Δ. □

4.6 Полнота исчисления высказываний

[ВШ2, 2.1], [Мен, 1.4], [Кли, 12], [П1, 4.4], [Bil, 4]

Лемма 4.23.

1. $A,\ B \vdash A \wedge B$.
2. $A,\ \neg B \vdash \neg(A \wedge B)$.
3. $\neg A,\ B \vdash \neg(A \wedge B)$.
4. $\neg A,\ \neg B \vdash \neg(A \wedge B)$.
5. $A,\ B \vdash A \vee B$.
6. $A,\ \neg B \vdash A \vee B$.
7. $\neg A,\ B \vdash A \vee B$.
8. $\neg A,\ \neg B \vdash \neg(A \vee B)$.
9. $A,\ B \vdash A \to B$.
10. $A,\ \neg B \vdash \neg(A \to B)$.
11. $\neg A,\ B \vdash A \to B$.
12. $\neg A,\ \neg B \vdash A \to B$.
13. $A \vdash \neg\neg A$.
14. $\neg A \vdash \neg A$.

(ВШ2, лемма 3, с. 55.)

Определение 4.24. Введём обозначение $\neg_\tau A$, где A — формула, а τ — истинностное значение. По определению $\neg_{\text{И}} A$ обозначает A, а $\neg_{\text{Л}} A$ обозначает $\neg A$.

Лемма 4.25. *Пусть A — формула логики высказываний, не содержащая других пропозициональных переменных, кроме $P_1, \dots, P_n$. Пусть τ — истинностное значение формулы A при оценке пропозициональных переменных g. Тогда*

$$\neg_{g(P_1)} P_1, \dots, \neg_{g(P_n)} P_n \vdash \neg_\tau A.$$

(ВШ2, лемма 4, с. 56.)

Доказательство. Лемма доказывается индукцией по построению формулы A. В шаге индукции используются лемма 4.23 и теорема 4.22. □

Лемма 4.26. *Пусть* $\Gamma, B \vdash A$ *и* $\Gamma, \neg B \vdash A$. *Тогда* $\Gamma \vdash A$.

Доказательство. Согласно теореме о дедукции $\Gamma \vdash (B \to A)$ и $\Gamma \vdash (\neg B \to A)$. Проверим, что $B \to A,\ \neg B \to A \vdash A$:

$$\begin{array}{ll}
B \to A & \\
\neg B \to A & \\
(\neg A \to \neg B) \to ((\neg A \to \neg\neg B) \to \neg\neg A) & \\
\neg A \to \neg B & \text{(пример 4.17)} \\
(\neg A \to \neg\neg B) \to \neg\neg A & \text{(MP)} \\
\neg A \to \neg\neg B & \text{(пример 4.17)} \\
\neg\neg A & \text{(MP)} \\
\neg\neg A \to A & \\
A & \text{(MP).}
\end{array}$$

Осталось применить теорему 4.22. □

Теорема 4.27 (о полноте). *Если* $\vDash A$, *то* $\vdash A$.

(ВШ2, теорема 18, с. 49–56.)

Доказательство. Пусть формула A является тавтологией. Докажем, что для каждого $k \leqslant n$ при любой оценке пропозициональных переменных g имеет место

$$\neg_{g(P_1)} P_1, \ldots, \neg_{g(P_k)} P_k \vdash A. \tag{13}$$

Для $k = n$ это следует из леммы 4.25, так как истинностное значение формулы A при оценке пропозициональных переменных g равно И, а $\neg_{\text{И}} A$ совпадает с A. С помощью леммы 4.26 можно вывести из утверждения (13) для $k = m$ то же утверждение для $k = m - 1$, если $m > 0$. Следовательно, утверждение (13) верно для всех значений k от 0 до n. При $k = 0$ получаем $\vdash A$. □

Замечание 4.28. Если множество Γ конечно и $\Gamma \vDash A$, то $\Gamma \vdash A$.

Доказательство. Пусть $B_1, \ldots, B_n \vDash A$. Согласно замечанию 2.73 формула $\vDash B_1 \wedge \ldots \wedge B_n \to A$ является тавтологией. Согласно теореме 4.27 $\vdash B_1 \wedge \ldots \wedge B_n \to A$. Осталось вывести $B_1, \ldots, B_n \vdash B_1 \wedge \ldots \wedge B_n$ и применить правило modus ponens. □

4.7 Противоречивое множество формул логики высказываний

[П1, 4.2], [ВШ2, 2.1, 2.2], [Bil, 4]

Определение 4.29. Множество формул Γ называется *противоречивым*, если существует такая формула A, что $\Gamma \vdash A$ и $\Gamma \vdash \neg A$. В противном случае множество Γ называется *непротиворечивым*.

(ВШ2, с. 57.)

(П1, с. 26.)

Теорема 4.30. *Множество формул* Γ *противоречиво тогда и только тогда, когда для любой формулы* A *имеет место* $\Gamma \vdash A$.

(П1, теорема 4.10, с. 28.)

Доказательство. Достаточно проверить, что $B,\ \neg B \vdash A$. □

Теорема 4.31 (принцип приведения к абсурду). *Если* $\Gamma, A \vdash B$ *и* $\Gamma, A \vdash \neg B$, *то* $\Gamma \vdash \neg A$.

(П1, теорема 4.8, с. 26.)

(ВШ2, с. 53.)

Доказательство. Применим теорему о дедукции и проверим, что $A \to B,\ A \to \neg B \vdash \neg A$. □

5 Исчисление предикатов

5.1. В этом разделе буквы A, B и т. д. обозначают формулы логики предикатов, а буквы Γ, Δ и т. д. обозначают множества формул логики предикатов.

5.1 Аксиомы и правила гильбертовского исчисления предикатов

[П1, 6.1], **[ВШ2, 4.2]**, [КД, с. 91–94, 95, 123–124], [УВП, 3.4, 3.5], [Кли, 21], [Bil, 7]

Определение 5.2. Аксиомами *классического исчисления предикатов в сигнатуре* Ω являются формулы следующих видов:
1) $A \to (B \to A)$,
2) $(A \to B) \to ((A \to (B \to C)) \to (A \to C))$,
3) $A \wedge B \to A$,
4) $A \wedge B \to B$,
5) $A \to (B \to A \wedge B)$,
6) $A \to A \vee B$,
7) $B \to A \vee B$,
8) $(A \to C) \to ((B \to C) \to (A \vee B \to C))$,
9) $(A \to B) \to ((A \to \neg B) \to \neg A)$,
10) $\neg\neg A \to A$,
11) $\forall v\, A \to A[t/v]$, где терм t свободен для v в формуле A,
12) $A[t/v] \to \exists v\, A$, где терм t свободен для v в формуле A.

Правила вывода:
1) $\dfrac{A \quad A \to B}{B}$,
2) $\dfrac{B \to A}{B \to \forall v\, A}$, где $v \notin \mathrm{FV}(B)$,
3) $\dfrac{A \to B}{\exists v\, A \to B}$, где $v \notin \mathrm{FV}(B)$.

Последние два правила называются *правилами Бернайса*.

Определение 5.3 (вывод). *Выводом в исчислении предикатов в сигнатуре* Ω называется конечная последовательность формул сигнатуры Ω, каждая из которых является аксиомой или получается из предыдущих формул по некоторому правилу вывода.

Определение 5.4 (выводимая формула). Пусть A — формула сигнатуры Ω. Формула A называется *выводимой в исчислении предикатов в сигнатуре* Ω (обозначение $\vdash A$), если существует вывод, в котором последняя формула есть A.

Определение 5.5 (вывод из замкнутых гипотез). Пусть Γ — некоторое множество замкнутых формул сигнатуры Ω. *Выводом из* Γ *в сигнатуре* Ω называется конечная последовательность формул сигнатуры Ω, каждая из которых либо принадлежит множеству Γ, либо является аксиомой, либо получается из предыдущих формул по некоторому правилу вывода. Элементы множества Γ называются *гипотезами*.

(ВШ2, с. 172.)

Определение 5.6 (выводимость из замкнутых гипотез). Пусть A — формула сигнатуры Ω и Γ — некоторое множество замкнутых формул сигнатуры Ω. Формула A называется *выводимой из* Γ (обозначение $\Gamma \vdash A$), если существует вывод из Γ в сигнатуре Ω, в котором последняя формула есть A.

(ВШ2, с. 172.)

Замечание 5.7 (монотонность). Если $\Delta \subseteq \Gamma$ и $\Delta \vdash A$, то $\Gamma \vdash A$.

(П1, с. 44.)

Замечание 5.8 (компактность). Если $\Gamma \vdash A$, то существует такое конечное множество $\Delta \subseteq \Gamma$, что $\Delta \vdash A$.

(П1, с. 44.)

Теорема 5.9 (транзитивность). *Если $\Gamma \vdash A$ и для каждой формулы $B \in \Gamma$ имеет место $\Delta \vdash B$, то $\Delta \vdash A$.*

Доказательство. Заменим в выводе формулы A каждую гипотезу на её вывод из Δ. □

5.2 Корректность исчисления предикатов

[П1, 6.1], **[ВШ2, 4.3]**, [КД, с. 94, 125], [УВП, 3.4], [Bil, 8]

Теорема 5.10. *Пусть A — формула сигнатуры Ω. Если $\vdash A$, то формула A общезначима.*

(ВШ2, теорема 43, с. 165.)

(П1, теорема 6.1, с. 44.)

Доказательство. Теорема доказывается индукцией по длине вывода формулы A. □

Теорема 5.11 (обобщённая теорема о корректности). *Пусть A — замкнутая формула сигнатуры Ω и Γ — некоторое множество замкнутых формул сигнатуры Ω. Если $\Gamma \vdash A$, то $\Gamma \vDash A$.*

(ВШ2, теорема 44, с. 174.)

(П1, теорема 6.4, с. 47.)

Доказательство. Индукцией по длине вывода можно доказать (аналогично теореме 5.10), что для каждой (не обязательно замкнутой) формулы A сигнатуры Ω, если $\Gamma \vdash A$ и формула A не содержит других свободных переменных кроме $v_1, \ldots, v_n$, то для любой модели $\mathfrak{M} = \langle M, \Omega \rangle$ множества Γ и для любых $a_1, \ldots, a_n \in M$ имеет место $\mathfrak{M} \vDash A[\underline{a_1}/v_1] \ldots [\underline{a_n}/v_n]$.

В случае замкнутой формулы A получаем $\Gamma \vDash A$. □

5.3 Теорема о дедукции для исчисления предикатов

[ВШ2, 4.4], **[Мен, 2.4]**, [П1, 6.2], [УВП, 3.5], [КД, с. 96–97, 125], [Кли, 22], [Bil, 7]

Теорема 5.12. *Пусть Γ — некоторое множество замкнутых формул сигнатуры Ω и A — замкнутая формула сигнатуры Ω. Тогда $\Gamma \vdash (A \to B)$ в том и только том случае, когда $\Gamma \cup \{A\} \vdash B$.*

(ВШ2, лемма, с. 172.)

Доказательство. Теорема доказывается аналогично теореме 4.15.

При разборе правила Бернайса

$$\frac{B \to C}{B \to \forall v\, C}\ ,$$

где $v \notin \mathrm{FV}(B)$, используются равносильности $(A \to (B \to C)) \sim (A \wedge B \to C)$ и $(A \wedge B \to \forall v\, C) \sim A \to (B \to \forall v\, C))$.

При разборе правила Бернайса

$$\frac{C \to B}{\exists v\, C \to B}\ ,$$

где $v \notin \mathrm{FV}(B)$, используются равносильности $(A \to (C \to B)) \sim (C \to (A \to B))$ и $(\exists v\, C \to (A \to B)) \sim (A \to (\exists v\, C \to B))$. □

5.4 Теорема Гёделя о полноте (без доказательства)

[УВП, 4.1–4.4], **[ВШ2, 4.4–4.5]**, **[Мен, 2.5]**, [П1, 6.3–6.4], [КД, с. 208–213], [Bil, 8]

Теорема 5.13 (теорема о полноте, без доказательства). *Пусть A — формула сигнатуры Ω. Если формула A общезначима, то $\vdash A$.*

(ВШ2, теорема 49, с. 185.)

(УВП, теорема 9, с. 87.)

Теорема 5.14 (обобщённая теорема о полноте, без доказательства). *Пусть A — замкнутая формула сигнатуры Ω и Γ — некоторое множество замкнутых формул сигнатуры Ω. Если $\Gamma \vDash A$, то $\Gamma \vdash A$.*

(ВШ2, теорема 51, с. 186.)

(УВП, теорема 11, с. 87.)

5.5 Теорема компактности для логики предикатов

[УВП, 4.4], **[ВШ2, 4.5]**, **[БДж, 17]**, **[ЛМ, II.6]**, [П1, 6.4], [КД, с. 213], [Bil, 8, 9]

Теорема 5.15 (теорема Мальцева о компактности). *Пусть A — замкнутая формула сигнатуры Ω и Γ — некоторое множество замкнутых формул сигнатуры Ω. Если $\Gamma \vDash A$, то существует такое конечное множество $\Delta \subseteq \Gamma$, что $\Delta \vDash A$.*

(УВП, теорема 14, с. 88.)

(ВШ2, теорема 50, с. 185.)

Доказательство. Пусть $\Gamma \vDash A$. Согласно теореме 5.14 $\Gamma \vdash A$. Согласно замечанию 5.8 существует такое конечное множество $\Delta \subseteq \Gamma$, что $\Delta \vdash A$. Согласно теореме 5.11 $\Delta \vDash A$. □

Теорема 5.16 (локальная теорема Мальцева). *Пусть Γ — некоторое множество замкнутых формул сигнатуры Ω. Если каждое конечное подмножество множества Γ имеет модель, то и само множество Γ имеет модель.*

(УВП, теорема 13, с. 88.)

(ВШ2, теорема 50, с. 185.)

Доказательство. Зафиксируем произвольную замкнутую формулу B сигнатуры Ω. Пусть множество Γ не имеет ни одной модели. Тогда $\Gamma \vDash B \wedge \neg B$. Согласно теореме 5.15 существует такое конечное множество $\Delta \subseteq \Gamma$, что $\Delta \vDash B \wedge \neg B$. Очевидно, множество Δ не имеет ни одной модели, что противоречит условию теоремы. Поэтому Γ имеет модель. □

Теорема 5.17. *Пусть T — некоторая теория первого порядка с равенством. Если теория T имеет модель, то T имеет и нормальную модель.*

(ВШ2, теорема 59, с. 203.)

Доказательство. Пусть $\mathfrak{M} = \langle M, \Omega \rangle$ является моделью теории T. Согласно определению теории первого порядка с равенством отношение $=^{\mathfrak{M}}$ является отношением эквивалентности (то есть оно рефлексивно, симметрично и транзитивно). Множество M разбивается на классы эквивалентности, множество этих классов обозначается $M/{=^{\mathfrak{M}}}$. Формально

$$(M/{=^{\mathfrak{M}}}) = \{\mathcal{A} \subseteq M \mid \mathcal{A} = \{b \in M \mid a =^{\mathfrak{M}} b\} \text{ для некоторого } a \in M\}.$$

На множество $M/{=^{\mathfrak{M}}}$ можно стандартным образом перенести функции и предикаты из интерпретации $\mathfrak{M}$. Полученная интерпретация является нормальной моделью теории T. □

Теорема 5.18. *Пусть T — некоторая теория первого порядка с равенством. Если каждое конечное подмножество множества T имеет нормальную модель, то и сама теория T имеет нормальную модель.*

(УВП, теорема 13, с. 88.)

Доказательство. Теорема непосредственно следует из теорем 5.16 и 5.17. □

5.6 Неразличимость конечного и бесконечного

[УВП, 4.5], [П1, 6.5]

Теорема 5.19. *Пусть T — теория первого порядка с равенством. Пусть для любого натурального числа n теория T имеет нормальную модель, содержащую не менее n элементов. Тогда теория T имеет бесконечную нормальную модель.*

(УВП, теорема 20, с. 91.)

Доказательство. Пусть теория T удовлетворяет условию теоремы. Рассмотрим теорию $T' = T \cup \{G_m \mid m \geqslant 2\}$, где $G_m = \neg\exists x_1 \ldots \exists x_{m-1} \forall y\, (y = x_1 \vee \ldots \vee y = x_{m-1})$. Очевидно, любое конечное подмножество множества T' имеет нормальную модель. Согласно теореме 5.18 множество T' имеет нормальную модель. Очевидно, она бесконечна и является нормальной моделью теории T. □

Упражнение 5.20. Существует ли бесконечная абелева группа, в которой каждый элемент является обратным самому себе?

Ответ 5.20. Да. Например, $\langle \mathcal{P}(\mathbb{N}), \triangle \rangle$.

Теорема 5.21. *Пусть Ω — некоторая сигнатура с равенством. Не существует замкнутой формулы, истинной во всех конечных нормальных интерпретациях сигнатуры Ω и ложной во всех бесконечных нормальных интерпретациях сигнатуры Ω.*

(УВП, теорема 21, с. 92.)

Доказательство. Пусть такая формула существует. Обозначим её через A. Применим теорему 5.19 к теории $\{A\}$. □

6 Теория алгоритмов

6.1 Частичные функции

[УВП, 5.1]

Определение 6.1 (частичная функция). Пусть $f \subseteq X \times Y$. Соответствие f называется *частичной функцией* из множества X в множество Y, если для любых $x \in X$, $y_1, y_2 \in Y$ из $\langle x, y_1 \rangle \in f$ и $\langle x, y_2 \rangle \in f$ следует $y_1 = y_2$. При этом пишут $f \colon X \to Y$.

(УВП, с. 94.)

Определение 6.2. Если f является частичной функцией из множества X в множество Y и для данного элемента $x \in X$ существует такой элемент $y \in Y$, что $\langle x, y \rangle \in f$, то этот элемент y называется *значением* функции f на x и обозначается $f(x)$. При этом говорят, что функция f *определена* на x и пишут $!\, f(x)$.

Определение 6.3 (всюду определённая функция). Частичная функция f из множества X в множество Y называется *всюду определённой функцией*, если для любого $x \in X$ функция f определена на x.

(УВП, с. 94.)

Определение 6.4 (условное равенство). Если α и β — какие-то выражения (возможно, включающие частичные функции), то через $\alpha \simeq \beta$ обозначается следующее утверждение: «α и β одновременно определены или не определены и если определены, то имеют одинаковые значения».

(УВП, с. 94.)

(К1, с. 9.)

Определение 6.5. *Областью определения* частичной функции f называется множество $\mathrm{D}\, f \rightleftharpoons \{x \mid f(x) \text{ определено}\}$.

(УВП, с. 96.)

Определение 6.6. *Множеством значений* частичной функции f называется множество $\mathrm{E}\, f \rightleftharpoons \{y \mid \exists x\, f(x) = y\}$.

6.2 Общее понятие алгоритма

[УВП, 5.1], [ВШ3, 1.1], [П2, 1], [Кли, 40], [КД, с. 167–168], [К1, с. 1]

6.7. *Алгоритм* — предписание выполнить точно определённую последовательность действий.

С каждым алгоритмом связаны *область возможных исходных данных* X и *область возможных значений* Y. При этом алгоритм вычисляет некоторую частичную функцию $f \colon X \to Y$. Процесс применения алгоритма $\mathcal{A}$ к исходному данному $x \in X$ всегда происходит по шагам. Каждый шаг обязательно заканчивается. Процесс применения алгоритма $\mathcal{A}$ к x либо будет продолжаться бесконечно, либо остановится после конечного числа шагов с результатом, либо остановится без результата.

В качестве области возможных исходных данных и области возможных значений обычно используют множества вида $\mathbb{N}^k$ или Σ^*, где Σ — конечный алфавит (эти множества — примеры *ансамблей конструктивных объектов*).

Определение 6.8 (область применимости/результативности алгоритма). *Область применимости* алгоритма $\mathcal{A}$ состоит из тех данных, при применении к которым алгоритма $\mathcal{A}$ процесс остановится с результатом.

6.9. В математике уточнения понятия алгоритма называются *вычислительными моделями*. Наиболее известные вычислительные модели: машины Тьюринга, частично рекурсивные функции, машины с неограниченными регистрами, нормальные алгорифмы Маркова, канонические системы Поста, лямбда-исчисление.

6.3 Машины Тьюринга

[К1, с. 3–8], **[П2, 2]**, **[ЛМ, III.2]**, **[КД, с. 169–175, 187–188]**, **[БДж, 3]**, **[УВП, 5.7]**, **[ВШЗ, 9.1–9.3]**, **[Кли, 41]**, [Bil, 10–12]

6.10. Образно говоря, *детерминированная машина Тьюринга* имеет бесконечную в обе стороны ленту, разделённую на ячейки. В каждой ячейке может быть записан любой символ из конечного алфавита, называемого *рабочим алфавитом* (или *ленточным алфавитом*) данной машины Тьюринга. Имеется управляющее устройство. Оно может находиться в одном из конечного множества *состояний*. Имеется одна читающе-записывающая головка, которая в каждый момент обозревает одну из ячеек ленты. Один такт работы состоит в следующем: машина читает символ в обозреваемой ячейке, выбирает из своей программы инструкцию, соответствующую текущему состоянию и прочитанному символу, и исполняет её. В инструкции сказано, какой символ следует записать в обозреваемую ячейку, каким будет новое состояние управляющего устройства и куда должна переместиться головка (на одну ячейку влево, на одну ячейку вправо или остаться на месте). Эти перемещения принято обозначать L, R и N соответственно (в некоторых учебниках вместо букв используют числа -1, 1 и 0).

В множестве состояний выделены два состояния — начальное (q_1) и заключительное (q_0). Попав в заключительное состояние машина останавливается. Один из символов рабочего алфавита выделен и называется *бланком* (или *пробелом*). Сначала почти вся лента заполнена бланками (только конечное число ячеек ленты может содержать символы, отличные от бланка).

(УВП, с. 109–110.)

Определение 6.11. *Детерминированная машина Тьюринга* (или просто *машина Тьюринга*) — это набор $\mathcal{M} = \langle Q, \Sigma, a_0, \delta, q_1, q_0 \rangle$, где Q и Σ — конечные множества, $a_0 \in \Sigma$, $q_1 \in Q$, $q_0 \in Q$ и $\delta\colon (Q \diagdown \{q_0\}) \times \Sigma) \to (Q \times \Sigma \times \{\mathrm{L}, \mathrm{N}, \mathrm{R}\})$. Здесь Q — *множество состояний*, Σ — *ленточный алфавит*, a_0 — *бланк* (*пробел, пустой символ*), δ — *таблица переходов*, q_1 — *начальное состояние*, q_0 — *заключительное состояние*.

6.12. Для удобства будем обозначать бланк символом $\#$ (в некоторых учебниках используют символ   или _).

6.13. Функцию δ принято записывать в виде множества команд P. Если $\delta\langle q, a \rangle = \langle r, b, \varkappa \rangle$, то этому соответствует команда $qa \to rb\varkappa$ (в некоторых учебниках пишут $qa \to b\varkappa r$). В упражнениях команды вида $qa \to qa\mathrm{N}$ можно не записывать.

Пример 6.14. Пример машины Тьюринга: $q_1\# \to q_2 1L, \quad q_2\# \to q_0 1L.$

Определение 6.15. В каждый момент имеется некоторая *конфигурация*, складывающаяся из содержимого ленты, положения головки и состояния управляющего устройства. Мы будем записывать конфигурацию в виде слова $uqav$, где q — текущее состояние, a — символ в обозреваемой ячейке, u — слово, записанное на ленте левее обозреваемой ячейки, v — слово, записанное на ленте правее обозреваемой ячейки. При этом все остальные ячейки (левее слова u и правее слова v) содержат только бланки.

(УВП, с. 111.)

Определение 6.16. Пусть $\Sigma_0 \subset \Sigma$ и $\# \notin \Sigma_0$. Пусть f — частичная функция из Σ_0^* в Σ_0^*. Машина Тьюринга $\mathcal{M} = \langle Q, \Sigma, \#, \delta, q_1, q_0 \rangle$ *вычисляет* функцию f, если для каждого слова $x \in \Sigma_0^*$ выполнены следующие условия.

1. Начав работу с конфигурации $q_1\#x$, машина $\mathcal{M}$ останавливается в том и только в том случае, если функция f определена на входе x.
2. Если машина $\mathcal{M}$ остановилась, начав работу с конфигурации $q_1\#x$, то заключительной конфигурацией является $q_0\#y$, где $f(x) = y$.

В некоторых учебниках такое определение вычисления называется «вычислением в сильном смысле» или «правильным вычислением».

(П2, с. 3.)

(ЛМ, с. 137.)

Определение 6.17. Пусть $1 \in \Sigma$ и $1 \neq \#$. Пусть f — частичная функция из $\mathbb{N}$ в $\mathbb{N}$. Машина Тьюринга $\mathcal{M} = \langle Q, \Sigma, \#, \delta, q_1, q_0 \rangle$ *вычисляет* функцию f, если для каждого числа $n \in \mathbb{N}$ выполнены следующие условия.

1. Начав работу с конфигурации $q_1\#1^n$, машина $\mathcal{M}$ останавливается в том и только в том случае, если функция f определена на входе n.
2. Если машина $\mathcal{M}$ остановилась, начав работу с конфигурации $q_1\#1^n$, то заключительной конфигурацией является $q_0\#1^{f(n)}$.

(П2, с. 3.)

(УВП, с. 118.)

Пример 6.18. Машина Тьюринга из примера 6.14 вычисляет функцию $f\colon \mathbb{N} \to \mathbb{N}$, заданную формулой $f(x) = x + 2$.

Упражнение 6.19. Функция $\mathrm{sg}\colon \mathbb{N} \to \mathbb{N}$ задаётся формулой

$$\mathrm{sg}(x) = \begin{cases} 0, & \text{если } x = 0, \\ 1, & \text{если } x > 0. \end{cases}$$

Построить машину Тьюринга, вычисляющую функцию sg.

Упражнение 6.20. Функция $\overline{\mathrm{sg}}\colon \mathbb{N} \to \mathbb{N}$ задаётся формулой

$$\overline{\mathrm{sg}}(x) = \begin{cases} 1, & \text{если } x = 0, \\ 0, & \text{если } x > 0. \end{cases}$$

Построить машину Тьюринга, вычисляющую функцию $\overline{\mathrm{sg}}$.

Определение 6.21. Пусть $1 \in \Sigma$ и $1 \neq \#$. Пусть f — частичная функция из $\mathbb{N}^k$ в $\mathbb{N}^m$. Машина Тьюринга $\mathcal{M} = \langle Q, \Sigma, \#, \delta, q_1, q_0 \rangle$ *вычисляет* функцию f, если для каждого кортежа $\langle n_1, n_2, \ldots, n_k \rangle \in \mathbb{N}^k$ выполнены следующие условия.

1. Начав работу с конфигурации $q_1\#1^{n_1}\#1^{n_2}\#\ldots\#1^{n_k}$, машина $\mathcal{M}$ останавливается в том и только в том случае, если функция f определена на входе $\langle n_1, n_2, \ldots, n_k \rangle$.

2. Если машина $\mathcal{M}$ остановилась, начав работу с конфигурации

$$q_1\#1^{n_1}\#1^{n_2}\#\ldots\#1^{n_k},$$

то заключительной конфигурацией является

$$q_0\#1^{l_1}\#1^{l_2}\#\ldots\#1^{l_m},$$

где $f\langle n_1, n_2, \ldots, n_k\rangle = \langle l_1, l_2, \ldots, l_m\rangle$.

(П2, с. 3.)

(ЛМ, с. 137.)

Пример 6.22. Машина Тьюринга из примера 6.14 вычисляет функцию $f\colon \mathbb{N}^2 \to \mathbb{N}^4$, заданную формулой $f\langle n_1, n_2\rangle = \langle n_1+2, n_2, 0, 0\rangle$.

Упражнение 6.23. Построить машину Тьюринга, вычисляющую функцию $f\colon \mathbb{N}\times\mathbb{N} \to \mathbb{N}$, где $f(x,y) = x+y+1$.

Упражнение 6.24. Построить машину Тьюринга, вычисляющую функцию $f\colon \mathbb{N}\times\mathbb{N} \to \mathbb{N}$, где $f(x,y) = x+y+3$.

Упражнение 6.25. Построить машину Тьюринга, вычисляющую двуместную функцию $\dot{-}$, где $x \mathbin{\dot{-}} y = \max(x-y, 0)$.

Упражнение 6.26. Построить машину Тьюринга, вычисляющую двуместную функцию f, где

$$f(x,y) = \begin{cases} y, & \text{если } x = 0, \\ 1, & \text{если } x > 0. \end{cases}$$

Упражнение 6.27. Построить машину Тьюринга, вычисляющую функцию $f\colon \mathbb{N} \to \mathbb{N}\times\mathbb{N}$, где $f(x) = \langle x, x\rangle$.

Ответ 6.27. $q_1\# \to q_2\#R$, $q_21 \to q_21R$, $q_2\# \to q_3\#L$, $q_3\# \to q_0\#R$, $q_31 \to q_4\#R$, $q_4\# \to q_51R$, $q_51 \to q_51R$, $q_5\# \to q_6\#R$, $q_61 \to q_61R$, $q_6\# \to q_71L$, $q_71 \to q_71L$, $q_7\# \to q_8\#L$, $q_81 \to q_81L$, $q_8\# \to q_3\#L$.

Определение 6.28. Через $\mathrm{Com}(\mathbb{N}^k, \mathbb{N}^m)$ обозначим множество всех вычислимых функций из $\mathbb{N}^k$ в $\mathbb{N}^m$. Через $\mathrm{TCom}(\mathbb{N}^k, \mathbb{N}^m)$ обозначим множество всех всюду определённых вычислимых функций из $\mathbb{N}^k$ в $\mathbb{N}^m$.

Теорема 6.29 (без доказательства).

1. *Пусть $f \in \mathrm{Com}(\Sigma_0^*, \Sigma_0^*)$ и $\# \notin \Sigma_0$. Тогда существует машина Тьюринга с бланком $\#$ и ленточным алфавитом $\Sigma_0 \cup \{\#\}$, вычисляющая функцию f.*
2. *Пусть $f \in \mathrm{Com}(\mathbb{N}^k, \mathbb{N}^m)$. Тогда существует машина Тьюринга с ленточным алфавитом $\{\#, 1\}$, вычисляющая функцию f.*

(К1, теорема 3.6, с. 8.)

6.4 Тезис Чёрча

[К1, с. 7], **[УВП, 5.9]**, **[Кли, 41]**, **[КД, с. 175–176]**, **[ВШ3, 9.3]**, [БДж, 3, 6]

6.30. *Тезисом Чёрча* (или *тезисом Тьюринга*) называется следующее неформальное утверждение: каждая вычислимая в интуитивном смысле частичная функция $f\colon \mathbb{N} \to \mathbb{N}$ вычислима на машине Тьюринга.

6.5 Композиция вычислимых функций

[К1, с. 6–7], **[УВП, 5.7]**, [Bil, 12]

Определение 6.31. Если f — частичная функция из X в Y и g — частичная функция из Y в Z, то через $g \circ f$ обозначается частичная функция из X в Z, определённая соотношением $(g \circ f)(x) \simeq g(f(x))$.

Теорема 6.32. *Если* $f \in \mathrm{Com}(\mathbb{N}, \mathbb{N})$ *и* $g \in \mathrm{Com}(\mathbb{N}, \mathbb{N})$, *то* $g \circ f \in \mathrm{Com}(\mathbb{N}, \mathbb{N})$.

(УВП, теорема 20, с. 118.)

Доказательство. Пусть машина Тьюринга $\mathcal{M} = \langle Q, \Sigma, a_0, \delta, q_1, q_0 \rangle$ вычисляет функцию f, а машина Тьюринга $\mathcal{M}' = \langle Q', \Sigma, a_0, \delta', q_1', q_0' \rangle$ вычисляет функцию g. Переименуем состояния машины Тьюринга $\mathcal{M}'$ так, чтобы $q_0 = q_1'$ и $Q \cap Q' = \{q_0\}$. Осталось объединить множества состояний двух машин Тьюринга, а также множества переходов. Начальным состоянием новой машины является q_1, а заключительным — переименованное состояние q_0'. □

6.6 Разрешимые множества

[УВП, 5.2], **[ВШЗ, 1.2]**, **[П2, 9]**, **[ЛМ, III.3]**, [К1, с. 1], [КД, с. 176–178], [Bil, 13]

Определение 6.33 (характеристическая функция). Пусть $A \subseteq \mathbb{N}$. *Характеристической функцией* множества A называется функция $\chi_A \colon \mathbb{N} \to \mathbb{N}$, определённая так:

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

(ВШЗ, с. 9.)

Замечание 6.34.

1. Функция sg совпадает с функцией $\chi_{\mathbb{N} \setminus \{0\}}$.
2. Функция $\overline{\mathrm{sg}}$ совпадает с функцией $\chi_{\{0\}}$.

Определение 6.35 (разрешимое множество). Пусть $A \subseteq \mathbb{N}$. Множество A называется *разрешимым* (или *рекурсивным*), если функция χ_A вычислима.

(ВШЗ, с. 9.)

Упражнение 6.36. Построить машину Тьюринга, вычисляющую функцию $\chi_{\{1,3\}}$.

Ответ 6.36. $q_1\# \to q_2\#R$, $q_2\# \to q_0\#N$, $q_21 \to q_3\#R$, $q_3\# \to q_01L$, $q_31 \to q_4\#R$, $q_4\# \to q_0\#N$, $q_41 \to q_5\#R$, $q_5\# \to q_01L$, $q_51 \to q_6\#R$, $q_6\# \to q_0\#N$, $q_61 \to q_6\#R$.

Теорема 6.37. *Каждое конечное множество разрешимо.*

(ВШЗ, с. 9.)

Доказательство. Пусть дано множество $A \subseteq \mathbb{N}$. По образцу упражнения 6.36 можно построить машину Тьюринга $\langle Q, \Sigma, a_0, \delta, q_1, q_0 \rangle$, вычисляющую функцию χ_A, причём $|Q| = 4 + \max A$, если $A \neq \varnothing$, и $|Q| = 3$, если $A = \varnothing$. □

Пример 6.38. Множества $\{2n \mid n \in \mathbb{N}\}$ и $\{n^2 \mid n \in \mathbb{N}\}$ разрешимы.

Лемма 6.39. *Пусть функция* $f\colon \mathbb{N} \to \mathbb{N}$ *вычислима. Тогда вычислима и функция из* $\mathbb{N}\times\mathbb{N}$ *в* $\mathbb{N}\times\mathbb{N}$*, отображающая пару* $\langle x, y\rangle$ *в* $\langle f(x), y\rangle$ *(её областью определения является* $\mathrm{D}\, f \times \mathbb{N}$*), а также функция из* $\mathbb{N}\times\mathbb{N}$ *в* $\mathbb{N}\times\mathbb{N}$*, отображающая пару* $\langle x, y\rangle$ *в* $\langle x, f(y)\rangle$ *(её областью определения является* $\mathbb{N}\times \mathrm{D}\, f$*).*

Доказательство. Приведём идею доказательства первого утверждения. Пусть машина Тьюринга $\mathcal{M}$ вычисляет функцию f. Добавим к ленточному алфавиту машины $\mathcal{M}$ новый символ $\triangleright$. Работа искомой машины Тьюринга состоит из следующих этапов.

- Заменить бланк между кодами двух аргументов на $\triangleright$.
- Запустить модифицированный вариант машины $\mathcal{M}$. Модификация заключается в том, что поведение новой машины на $\triangleright$ в основном такое же, как на бланке, но при попытке, обозревая $\triangleright$, сделать шаг вправо машина перед этим запустит подпрограмму, передвигающую символ $\triangleright$ и блок из 1 за ним на одну клетку вправо.
- Передвинуть код числа $f(x)$ направо до символа $\triangleright$, заменить $\triangleright$ на бланк и остановиться непосредственно слева от кода числа $f(x)$.

□

Лемма 6.40. *Пусть функции* $f\colon \mathbb{N} \to \mathbb{N}$ *и* $g\colon \mathbb{N} \to \mathbb{N}$ *вычислимы. Тогда вычислима и функция из* $\mathbb{N}\times\mathbb{N}$ *в* $\mathbb{N}\times\mathbb{N}$*, отображающая пару* $\langle x, y\rangle$ *в* $\langle f(x), g(y)\rangle$ *(её областью определения является* $\mathrm{D}\, f\times\mathrm{D}\, g$*).*

Доказательство. Искомая функция является композицией двух функций из $\mathbb{N}\times\mathbb{N}$ в $\mathbb{N}\times\mathbb{N}$, полученных из леммы 6.39. □

Теорема 6.41.

1. *Если множество* $A \subseteq \mathbb{N}$ *разрешимо, то и множество* $\mathbb{N} \setminus A$ *разрешимо.*
2. *Если множества* $A \subseteq \mathbb{N}$ *и* $B \subseteq \mathbb{N}$ *разрешимы, то и множество* $A \cup B$ *разрешимо.*
3. *Если множества* $A \subseteq \mathbb{N}$ *и* $B \subseteq \mathbb{N}$ *разрешимы, то и множество* $A \cap B$ *разрешимо.*

(УВП, теорема 1, с. 96.)

(ВШЗ, с. 9.)

Доказательство. Искомые машины Тьюринга можно построить из машин Тьюринга, вычисляющих функции χ_A и χ_B, и машин Тьюринга из упражнений 6.20 и 6.26, используя теорему 6.32 и лемму 6.40. □

6.7 Сигнализирующее множество

[K1, с. 2], [УВП, 5.4]

Определение 6.42 (сигнализирующее множество). Пусть $\mathcal{A}$ — алгоритм с областью возможных исходных данных X. Множество

$$\{\langle x, n\rangle \in X \times \mathbb{N} \mid \text{вычисление по алгоритму } \mathcal{A} \text{ на входе } x \text{ заканчивается за не более чем } n \text{ шагов}\}$$

называется *сигнализирующим множеством* алгоритма $\mathcal{A}$ и обозначается $\mathrm{S}_{\mathcal{A}}$.

Замечание 6.43. Для каждого алгоритма $\mathcal{A}$ его сигнализирующее множество разрешимо.

6.8 Полуразрешимые и перечислимые множества

[УВП, 5.3], **[ВШЗ, 1.3]**, **[П2, 9]**, **[ЛМ, III.3]**, [K1, с. 1], [КД, с. 178–180], [Bil, 14]

Определение 6.44 (полухарактеристическая функция). Пусть $A \subseteq \mathbb{N}$. *Полухарактеристической функцией* множества A называется частичная функция $\chi_A^*\colon \mathbb{N} \to \mathbb{N}$, определённая так:

$$\chi_A^*(x) \simeq \begin{cases} 1, & \text{если } x \in A, \\ \text{не определено}, & \text{если } x \notin A. \end{cases}$$

Определение 6.45 (полуразрешимое множество). Пусть $A \subseteq \mathbb{N}$. Множество A называется *полуразрешимым*, если функция χ_A^* вычислима.

Теорема 6.46. *Каждое разрешимое множество полуразрешимо.*

Доказательство. Пусть $\chi_A^* \in \mathrm{Com}(\mathbb{N}, \mathbb{N})$. Рассмотрим функцию $g\colon \mathbb{N} \to \mathbb{N}$, определённую так:

$$g(y) \simeq \begin{cases} y, & \text{если } y \geqslant 1, \\ \text{не определено}, & \text{если } y = 0. \end{cases}$$

Машина Тьюринга $q_1\# \to q_1\#R$, $q_11 \to q_01L$ вычисляет функцию g. Очевидно, $\chi_A^* = g \circ \chi_A$. Согласно теореме 6.32 $\chi_A^* \in \mathrm{Com}(\mathbb{N}, \mathbb{N})$. $\square$

Определение 6.47 (последовательность). *Последовательностью* элементов множества X называется произвольная всюду определённая функция из множества $\mathbb{N}$ в множество X.

Определение 6.48 (перечислимое множество). Пусть $A \subseteq \mathbb{N}$. Множество A называется *перечислимым* (или *рекурсивно перечислимым*), если A пусто или является множеством значений некоторой вычислимой последовательности натуральных чисел.

6.9 Нумерация кортежей натуральных чисел

[ЛМ, III.1.13–III.1.14], **[КД, с. 186]**, **[БДж, с. 208, 218]**

Определение 6.49 (канторовская нумерующая функция). Рассмотрим линейный порядок $\prec$ на $\mathbb{N}^2$, определённый следующим образом: $\langle x_1, y_1\rangle \prec \langle x_2, y_2\rangle$ тогда и только тогда, когда либо $x_1+y_1 < x_2+y_2$, либо $x_1+y_1 = x_2+y_2$ и $x_1 < x_2$. Очевидно,

$$\langle 0,0\rangle \prec \langle 0,1\rangle \prec \langle 1,0\rangle \prec \langle 0,2\rangle \prec \langle 1,1\rangle \prec \langle 2,0\rangle \prec \langle 0,3\rangle \prec \ldots.$$

Легко проверить, что для любой пары $\langle x, y\rangle \in \mathbb{N}^2$ множество пар, меньших чем $\langle x, y\rangle$ (в смысле отношения $\prec$), конечно. Следовательно, функция из $\mathbb{N}^2$ в $\mathbb{N}$, ставящая каждой паре из $\mathbb{N}^2$ в соответствие количество пар, меньших её (в смысле отношения $\prec$), является биекцией. Эта функция называется *канторовской нумерующей функцией* и обозначается c.

Пример 6.50. $c(0,0) = 0$, $c(0,1) = 1$, $c(1,0) = 2$.

Лемма 6.51. $c(0, y+1) = c(0, y) + y + 1$.

Лемма 6.52. $c(x, y) = c(0, x+y) + x$.

Лемма 6.53. $c(x,y) = \dfrac{(x+y)(x+y+1)}{2} + x.$
(БДж, лемма 14.1, с. 218.)

Определение 6.54. Всюду определённые функции $l\colon \mathbb{N} \to \mathbb{N}$ и $r\colon \mathbb{N} \to \mathbb{N}$ заданы соотношением $(\forall n \in \mathbb{N})\, c(l(n), r(n)) = n$.

Лемма 6.55.

1. $l(c(x,y)) = x$.
2. $r(c(x,y)) = y$.

Замечание 6.56. Функции c, l и r вычислимы.

Определение 6.57 (канторовская нумерация кортежей фиксированной длины). Для каждого $k \geqslant 1$ определим функцию $c^k\colon \mathbb{N}^k \to \mathbb{N}$ следующим образом:

$$\begin{aligned}
&c^1(x_1) \rightleftharpoons x_1,\\
&c^{n+1}(x_1,\ldots,x_n,x_{n+1}) \rightleftharpoons c(c^n(x_1,\ldots,x_n), x_{n+1}).
\end{aligned}$$

Определение 6.58. Всюду определённые функции $c_{ni}\colon \mathbb{N} \to \mathbb{N}$, где $1 \leqslant i \leqslant n$, заданы соотношением $(\forall x \in \mathbb{N})\, c^n(c_{n1}(x), \ldots, c_{nn}(x)) = x$.

Лемма 6.59. *Для любых n и i, удовлетворяющих условию $1 \leqslant i \leqslant n$, выполняется равенство $c_{ni}(c^n(x_1,\ldots,x_n)) = x_i$.*

Теорема 6.60. *Для каждого $k \geqslant 1$ существует вычислимая биекция из $\mathbb{N}^k$ в $\mathbb{N}$.*

Доказательство. Функция c^k является биекцией из $\mathbb{N}^k$ в $\mathbb{N}$. Можно доказать, что $c^k \in \mathrm{TCom}(\mathbb{N}^k, \mathbb{N})$. ☐

Теорема 6.61. *Для каждого непустого конечного множества Σ существует вычислимая биекция из Σ^* в $\mathbb{N}$.*

Доказательство. Обозначим через k количество элементов множества Σ. Если $k = 1$, то подходит биекция, ставящая в соответствие каждому слову его длину.

Пусть $k \geqslant 2$. Без ограничения общности можно считать, что $\Sigma = \{0, 1, \ldots, k-1\}$. Рассмотрим функцию, ставящую в соответствие слову $a_1 \ldots a_n$ в алфавите Σ натуральное число

$$\sum_{j=0}^{n-1} k^j + \sum_{i=1}^{n} a_i k^{n-i} = \sum_{i=1}^{n} (a_i+1) k^{n-i}.$$

Можно доказать, что эта функция вычислима и является биекцией из Σ^* в $\mathbb{N}$. ☐

Замечание 6.62. Функция из доказательства теоремы 6.61 соответствует линейному порядку на Σ^*, согласно которому при разных длинах более короткое слово меньше, чем более длинное, а при одинаковых длинах слова сравниваются лексикографически.

Пример 6.63. Рассмотрим биекцию между $\{0,1\}^*$ и $\mathbb{N}$, построенную в доказательстве теоремы 6.61. Слову 101 она ставит в соответствие число $(1+2+4) + (1\cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0) = 7 + 5 = 12$ (здесь $k = 2$ и $n = 3$).

Посчитаем слова, меньшие слова 101 в смысле порядка из замечания 6.62. Среди слов длины 3 имеется 5 таких слов. Общее количество слов меньшей длины равно $1 + 2 + 4 = 7$. Итого, существует 12 слов, меньших слова 101.

Определение 6.64. Функцию из доказательства теоремы 6.61 будем обозначать word_Σ.

6.10 Критерии перечислимости

[УВП, 5.4], **[ВШЗ, 1.4–1.5]**, **[П2, 9]**, **[ЛМ, III.3]**, [K1, с. 1–3]

Определение 6.65 (нигде не определённая функция). Частичная функция из $\mathbb{N}$ в $\mathbb{N}$, значение которой не определено ни при одном значении аргумента, называется *нигде не определённой функцией* и обозначается ζ.

Замечание 6.66. $\mathrm{D}\,\zeta = \varnothing$ и $\mathrm{E}\,\zeta = \varnothing$.

Лемма 6.67. *Функция ζ вычислима.*

Доказательство. Машина Тьюринга $q_1\# \to q_1\#N$ вычисляет функцию ζ. □

Определение 6.68. Пусть $A \subseteq X \times Y$. Тогда

$$\text{пр}_1\, A \rightleftharpoons \{x \in X \mid (\exists y \in Y)\, \langle x, y\rangle \in A\}$$

и

$$\text{пр}_2\, A \rightleftharpoons \{y \in Y \mid (\exists x \in X)\, \langle x, y\rangle \in A\}.$$

Замечание 6.69. Если алгоритм $\mathcal{A}$ вычисляет функцию f, то $\text{пр}_1\, \mathrm{S}_{\mathcal{A}} = \mathrm{D}\, f$.

Теорема 6.70. *Пусть $A \subseteq \mathbb{N}^k$. Тогда следующие условия равносильны:*

(1) $\chi^*_A \in \mathrm{Com}(\mathbb{N}^k, \mathbb{N})$ *(то есть A полуразрешимо)*;

(2) *существует такая функция $f \in \mathrm{Com}(\mathbb{N}^k, \mathbb{N})$, что $\mathrm{D}\, f = A$*;

(3) *существует такое разрешимое множество $B \subseteq \mathbb{N}^k \times \mathbb{N}$, что $\text{пр}_1\, B = A$*;

(4) *$A = \varnothing$ или существует такая функция $f \in \mathrm{TCom}(\mathbb{N}, \mathbb{N}^k)$, что $\mathrm{E}\, f = A$ (то есть A перечислимо)*;

(5) *существует такая функция $f \in \mathrm{Com}(\mathbb{N}, \mathbb{N}^k)$, что $\mathrm{E}\, f = A$.*

Доказательство. Докажем пять импликаций.

$(1) \longrightarrow (2)$. Положим $f = \chi^*_A$.

$(2) \longrightarrow (3)$. Пусть $\mathcal{M}$ — машина Тьюринга, вычисляющая функцию f. Положим $B = \mathrm{S}_{\mathcal{M}}$.

$(3) \longrightarrow (4)$. Проведём доказательство для случая $k = 1$. Пусть $a_0 \in A$. Положим

$$f(n) = \begin{cases} l(n), & \text{если } \langle l(n), r(n)\rangle \in B,\\ a_0 & \text{иначе.}\end{cases}$$

$(4) \longrightarrow (5)$. Если $A = \varnothing$, то положим $f \simeq \zeta$.

$(5) \longrightarrow (1)$. Проведём доказательство для случая $k = 1$. Пусть S — сигнализирующее множество машины Тьюринга, вычисляющей функцию f. Следующий алгоритм вычисляет по $x \in \mathbb{N}$ значение $\chi^*_A(x)$.

```
i = 0;
while (TRUE) {
  if (⟨l(i),r(i)⟩ ∈ S) {
    if (f(l(i)) == x) { return 1; }
  }
  i = i + 1;
}
```

□

6.11 Теорема Поста

[УВП, 5.4], **[ВШЗ, 1.4]**, **[П2, 9]**, **[ЛМ, III.3]**, [КД, с. 181], [К1, с. 1], [Bil, 14]

Лемма 6.71. *Функция $z\colon \mathbb{N} \to \mathbb{N}$, заданная формулой $z(x) = 0$, вычислима.*

Доказательство. Машина Тьюринга $q_1\# \to q_2\#R$, $q_21 \to q_2\#R$, $q_2\# \to q_0\#N$ вычисляет функцию z. $\square$

Теорема 6.72. *Пусть $A \subseteq \mathbb{N}^k$. Множество A разрешимо тогда и только тогда, когда A перечислимо и $\mathbb{N} \setminus A$ перечислимо.*

(УВП, теорема 10, с. 102.)

Доказательство. Необходимость следует из теорем 6.41 и 6.46. Докажем достаточность. Если $A = \varnothing$, то $\chi_A(x_1, \ldots, x_k) = 0$ при любых $x_1, \ldots, x_k$ и, следовательно, $\chi_A \in \mathrm{Com}(\mathbb{N}^k, \mathbb{N})$. Если $\mathbb{N} \setminus A = \varnothing$, то снова $\chi_A \in \mathrm{Com}(\mathbb{N}^k, \mathbb{N})$. Осталось рассмотреть случай, когда $A = \mathrm{E}\, f$ для некоторой функции $f \in \mathrm{TCom}(\mathbb{N}, \mathbb{N}^k)$ и $\mathbb{N} \setminus A = \mathrm{E}\, g$ для некоторой функции $g \in \mathrm{TCom}(\mathbb{N}, \mathbb{N}^k)$. Следующий алгоритм вычисляет по $x \in \mathbb{N}^k$ значение $\chi_A(x)$.

```
i = 0;
while (TRUE) {
  if (f(i) == x) { return 1; }
  if (g(i) == x) { return 0; }
  i = i + 1;
}
```

$\square$

6.12 Свойства перечислимых множеств

[УВП, 5.4], **[ВШЗ, 1.3, 1.5]**, **[П2, 9–10]**, **[ЛМ, III.3]**, [К1, с. 1–3]

Теорема 6.73. *Пусть $A \subseteq \mathbb{N}^k$ и $B \subseteq \mathbb{N}^k$. Если множества A и B перечислимы, то множество $A \cup B$ перечислимо.*

(УВП, теорема 9, с. 101.)

Доказательство. Если $A = \varnothing$, то $A \cup B = B$. Если $B = \varnothing$, то $A \cup B = A$. Осталось рассмотреть случай, когда $A = \mathrm{E}\, f$ для некоторой функции $f \in \mathrm{TCom}(\mathbb{N}, \mathbb{N}^k)$ и $\mathbb{N} \setminus A = \mathrm{E}\, g$ для некоторой функции $g \in \mathrm{TCom}(\mathbb{N}, \mathbb{N}^k)$. Определим функцию $h\colon \mathbb{N} \to \mathbb{N}^k$, положив $h(2m) = f(m)$ и $h(2m+1) = g(m)$ для каждого $m \in \mathbb{N}$. Очевидно, $h \in \mathrm{TCom}(\mathbb{N}, \mathbb{N}^k)$ и $\mathrm{E}\, h = \mathrm{E}\, f \cup \mathrm{E}\, g = A \cup B$. $\square$

Теорема 6.74. *Пусть $A \subseteq \mathbb{N}^k$ и $B \subseteq \mathbb{N}^k$. Если множества A и B перечислимы, то множество $A \cap B$ перечислимо.*

(УВП, теорема 9, с. 101.)

Доказательство. Следующий алгоритм вычисляет по $x \in \mathbb{N}^k$ значение $\chi^*_{A\cap B}(x)$.

```
if (χ*_A(x) == 1) {
  if (χ*_B(x) == 1) { return 1; }
}
```

$\square$

Определение 6.75. Пусть f — частичная функция из X в Y. *Графиком* функции f называется множество $\{\langle x, y\rangle \mid f(x) \simeq y\}$, обозначаемое $\mathrm{Гр}_f$.

Замечание 6.76. $\text{Гр}_\zeta = \varnothing$.

Замечание 6.77. $\text{пр}_1 \text{Гр}_f = \mathrm{D}\, f$.

Замечание 6.78. $\text{пр}_2 \text{Гр}_f = \mathrm{E}\, f$.

Теорема 6.79. *Пусть f — частичная функция из $\mathbb{N}$ в $\mathbb{N}$. Функция f вычислима тогда и только тогда, когда её график перечислим.*

(УВП, теорема 11, с. 103.)

Доказательство. Докажем необходимость. Согласно теореме 6.70 множество $\mathrm{D}\, f$ перечислимо. Если $\mathrm{D}\, f = \varnothing$, то $\text{Гр}_f = \varnothing$. Если $\mathrm{D}\, f \neq \varnothing$, то $\mathrm{D}\, f = \mathrm{E}\, g$ для некоторой функции $g \in \mathrm{TCom}(\mathbb{N}, \mathbb{N})$. Определим функцию $h\colon \mathbb{N} \to \mathbb{N} \times \mathbb{N}$, положив $h(n) = \langle g(n), f(g(n)) \rangle$ для каждого $n \in \mathbb{N}$. Очевидно, $h \in \mathrm{TCom}(\mathbb{N}, \mathbb{N}\times\mathbb{N})$ и $\mathrm{E}\, h = \text{Гр}_f$.

Докажем достаточность. Если $\text{Гр}_f = \varnothing$, то $f = \zeta$. Если $\text{Гр}_f \neq \varnothing$, то $\text{Гр}_f = \mathrm{E}\, h$ для некоторой функции $h \in \mathrm{TCom}(\mathbb{N}, \mathbb{N} \times \mathbb{N})$. Следующий алгоритм вычисляет по $x \in \mathbb{N}$ значение $f(x)$.

```
i = 0;
while (TRUE) {
  ⟨u,v⟩ = h(i);
  if (u == x) { return v; }
  i = i + 1;
}
```

□

Определение 6.80. Частичная функция $f\colon X \to Y$ называется *инъективной*, если $(\forall x_1 \in X)\,(\forall x_2 \in X)\,(!\, f(x_1) \wedge !\, f(x_2) \wedge f(x_1) = f(x_2) \to x_1 = x_2)$.

Определение 6.81. Пусть f — инъективная частичная функция из X в Y. Тогда через f^{-1} обозначается такая частичная функция из Y в X, что для любых $x \in X$ и $y \in Y$ условия $f(x) = y$ и $f^{-1}(y) = x$ равносильны.

Теорема 6.82. *Пусть f — инъективная частичная функция из $\mathbb{N}^k$ в $\mathbb{N}^m$. Если функция f вычислима, то и функция f^{-1} вычислима.*

(УВП, теорема 5, с. 98.)

Доказательство. Очевидно, $\text{Гр}_{f^{-1}} = \{\langle y, x\rangle \mid \langle x, y\rangle \in \text{Гр}_f\}$. Из перечислимости множества Гр_f следует перечислимость множества $\text{Гр}_{f^{-1}}$. □

Теорема 6.83. *Если f — вычислимая биекция из X в Y, то обратная биекция f^{-1} тоже вычислима.*

Теорема 6.84. *Пусть $A \subseteq \mathbb{N}^k$ и $B \subseteq \mathbb{N}^m$. Если множества A и B перечислимы, то множество $A \times B$ перечислимо.*

Доказательство. Если $A = \varnothing$ или $B = \varnothing$, то $A \times B = \varnothing$. Осталось рассмотреть случай, когда $A = \mathrm{E}\, f$ для некоторой функции $f \in \mathrm{TCom}(\mathbb{N}, \mathbb{N}^k)$ и $B = \mathrm{E}\, g$ для некоторой функции $g \in \mathrm{TCom}(\mathbb{N}, \mathbb{N}^m)$. Определим функцию $h\colon \mathbb{N} \to \mathbb{N}^k \times \mathbb{N}^m$, положив $h(n) = \langle f(l(n)), g(r(n))\rangle$ для каждого $n \in \mathbb{N}$. Очевидно, $h \in \mathrm{TCom}(\mathbb{N}, \mathbb{N}^k \times \mathbb{N}^m)$ и $\mathrm{E}\, h = \mathrm{E}\, f \times \mathrm{E}\, g = A \times B$. □

Теорема 6.85. *Пусть $A \subseteq \mathbb{N} \times \mathbb{N}$. Если множество A перечислимо, то и множество $\text{пр}_1 A$ перечислимо.*

(УВП, теорема 9, с. 101.)

Доказательство. Если $A = \varnothing$, то $\text{пр}_1 A = \varnothing$. Осталось рассмотреть случай, когда $A = \mathrm{E}\, f$ для некоторой функции $f \in \mathrm{TCom}(\mathbb{N}, \mathbb{N} \times \mathbb{N})$. Рассмотрим функцию $g\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, заданную формулой $g(x, y) = x$. Обозначим $h = g \circ f$. Очевидно, $h \in \mathrm{TCom}(\mathbb{N}, \mathbb{N})$ и $\mathrm{E}\, h = \text{пр}_1 \mathrm{E}\, f = \text{пр}_1 A$. □

Определение 6.86. Пусть f — частичная функция из X в Y. Пусть $A \subseteq X$. Тогда через $f(A)$ обозначается множество $\{y \in Y \mid (\exists x \in A)\, f(x) = y\}$.

Определение 6.87. Пусть f — частичная функция из X в Y. Пусть $A \subseteq Y$. Тогда через $f^{-1}(A)$ обозначается множество $\{x \in X \mid f(x) \in A\}$.

Теорема 6.88. *Пусть $A \subseteq \mathbb{N}^k$ и $f \in \mathrm{Com}(\mathbb{N}^k, \mathbb{N}^m)$. Если A перечислимо, то $f(A)$ перечислимо.*

(ВШ3, теорема 5, с. 15.)

Доказательство. Если $A = \mathrm{E}\,g$, где $g \in \mathrm{Com}(\mathbb{N}, \mathbb{N}^k)$, то $f(A) = \mathrm{E}(f \circ g)$. □

Теорема 6.89. *Пусть $A \subseteq \mathbb{N}^m$ и $f \in \mathrm{Com}(\mathbb{N}^k, \mathbb{N}^m)$. Если A перечислимо, то $f^{-1}(A)$ перечислимо.* (ВШ3, теорема 5, с. 15.)

Доказательство. Если $A = \mathrm{D}\,g$, где $g \in \mathrm{Com}(\mathbb{N}^m, \mathbb{N})$, то $f(A) = \mathrm{D}(g \circ f)$. □

6.13 Нумерация машин Тьюринга

[К1, с. 8–9], **[УВП, 5.8]**, **[КД, с. 187–188]**, **[ЛМ, III.2]**, [ВШ3, 2.1], [П2, 6], [БДж, 5], [Bil, 14]

Определение 6.90. *Алфавитом программ* называется алфавит

$$\text{Ы} \rightleftharpoons \{\to, \mathrm{L}, \mathrm{N}, \mathrm{R}, q, a, \mathbf{1}\}.$$

Определение 6.91 (код машины Тьюринга). Рассмотрим машину Тьюринга $\mathcal{M}$ с множеством состояний Q и ленточным алфавитом Σ. Пусть $Q = \{q_0, q_1, \ldots, q_s\}$ (то есть задан линейный порядок на множестве Q). Пусть $\Sigma = \{a_0, a_1, \ldots, a_r\}$ (то есть задан линейный порядок на множестве Σ). Пусть начальным состоянием является q_1, заключительным состоянием является q_0 и бланком является a_0. Поставим машине Тьюринга $\mathcal{M}$ в соответствие слово в алфавите программ, называемое *кодом* машины $\mathcal{M}$ (обозначение $\mathrm{Code}(\mathcal{M})$) и определяемое следующим образом. Кодом команды $q_i a_k \to q_j a_l \varkappa$, где $\varkappa \in \{\mathrm{L}, \mathrm{N}, \mathrm{R}\}$, является слово $q\mathbf{1}^i a\mathbf{1}^k \to q\mathbf{1}^j a\mathbf{1}^l \varkappa$. Кодом машины Тьюринга является конкатенация кодов всех команд этой машины (их ровно $s(r+1)$). Для определённости можно команды сначала отсортировать в алфавитном порядке, считая, что на алфавите Ы задан следующий линейный порядок:

$$\to < \mathrm{L} < \mathrm{N} < \mathrm{R} < q < a < \mathbf{1}.$$

Пример 6.92. Кодом простейшей машины Тьюринга, вычисляющей функцию $x \mapsto x+1$, является слово $q\mathbf{1}a{\to}qa\mathbf{1}\mathrm{L}q\mathbf{1}a\mathbf{1}{\to}q\mathbf{1}a\mathbf{1}\mathrm{N}$.

6.14 Лямбда-обозначения

[П2, 7]

6.93. Иногда функция задаётся путём выражения её значения через значения аргументов в виде именной формы. Например, говорят о функции x^2. Чтобы выражаться более аккуратно, обычно используют λ-обозначения. Например, функцию возведения в квадрат можно обозначить так: $\lambda x.x^2$.

Если t — некоторое выражение, а $v_1, \ldots, v_n$ — список различных переменных, то $\lambda v_1 \ldots v_n.t(v_1, \ldots, v_n)$ считается обозначением n-местной функции, которая каждому набору $a_1, \ldots, a_n$ значений переменных $v_1, \ldots, v_n$ ставит в соответствие объект, именем которого является $t(a_1, \ldots, a_n)$.

Пример 6.94. $\lambda x.\, x+1$.

Пример 6.95. $z = \lambda x.0$.

Пример 6.96. $\lambda x_1 x_2 x_3.x_2$.

Пример 6.97. $\lambda u.\, u+r$.

6.15 Универсальная машина Тьюринга

[K1, с. 9–10], [УВП, 5.8]

Теорема 6.98. *Пусть зафиксирована конечная последовательность различных символов $a_0, a_1, \ldots, a_r$, не принадлежащих алфавиту* Ы. *Обозначим через $\mathcal{C}_r$ класс всех машин Тьюринга с ленточным алфавитом $\Sigma = \{a_0, a_1, \ldots, a_r\}$, удовлетворяющих условиям определения* 6.91. *Рассмотрим функцию F из $(\text{Ы} \cup \Sigma)^*$ в Σ^*, определённую так: $F(x) = y$, если найдутся машина Тьюринга $\mathcal{M} \in \mathcal{C}_r$ и слово $v \in \{a_1, \ldots, a_r\}^*$, такие что $x = \mathrm{Code}(\mathcal{M})v$ и машина $\mathcal{M}$, начав работу с конфигурации $q_1\#x$, остановится в конфигурации $q_0\#y$, причём $y \in \{a_1, \ldots, a_r\}^*$. Функция F вычислима.* (*Машина Тьюринга, вычисляющая функцию F, называется* универсальной машиной Тьюринга *для класса $\mathcal{C}_r$.*)

(K1, теорема 3.8, с. 10.)

Доказательство. Универсальную машину Тьюринга можно построить следующим образом. Используем ленточный алфавит $\text{Ы} \cup \Sigma \cup \{\bar{\mathbf{1}}, a_0'\}$. Бланком является a_0. Работа универсальной машины Тьюринга состоит из следующих этапов.

- Проверить, что на ленте (от текущей ячейки до ближайшего справа бланка) записано слово вида $\mathrm{Code}(\mathcal{M})v$ для некоторых $\mathcal{M} \in \mathcal{C}_r$ и $v \in \{a_1, \ldots, a_r\}^*$. Если это не так, то зациклиться.
- Добавить между $\mathrm{Code}(\mathcal{M})$ и v символы $q\mathbf{1}a_0'$.
- Эмулировать процесс вычисления $\mathcal{M}$ на конфигурации, записанной справа от $\mathrm{Code}(\mathcal{M})$, используя вместо a_0 символ a_0'. При этом для сравнивания кодов состояний машины Тьюринга $\mathcal{M}$ разрешается заменять символы $\mathbf{1}$ и $\bar{\mathbf{1}}$ друг на друга.
- Проверить, что справа от $\mathrm{Code}(\mathcal{M})$ до ближайшего символа a_0 записано слово вида $a_0' \ldots a_0' q a_0' y a_0' \ldots a_0'$ для некоторого $y \in \{a_1, \ldots, a_r\}^*$. Если это не так, то зациклиться.
- Заменить всё, кроме слова y, на символы a_0 и остановиться непосредственно слева от y.

□

6.16 Универсальная вычислимая функция

[K1, с. 9–11], **[ВШ3, 2.1]**, **[УВП, 5.5, 5.8]**, **[П2, 8]**, **[ЛМ, III.1, III.2]**, [КД, с. 191–193, 194], [БДж, 5], [Bil, 14]

Определение 6.99. Функция $G\colon \mathbb{N} \times X \to Y$ называется *универсальной* для класса $\mathrm{Com}(X, Y)$, если для каждой частичной функции f из X в Y следующие два условия равносильны:

1) $f \in \mathrm{Com}(X, Y)$,
2) $(\exists i \in \mathbb{N})\,(\forall x \in X)\, f(x) \simeq G(i, x)$.

(ВШ3, с. 17.)

(УВП, с. 104.)

Определение 6.100 (индекс функции). Пусть G — универсальная функция для класса $\mathrm{Com}(X, Y)$. Пусть $f \in \mathrm{Com}(X, Y)$ — частичная функция из X в Y. Если $(\forall x \in X)\, f(x) \simeq G(i, x)$, то число i называется *индексом* функции f относительно универсальной функции G.

Теорема 6.101. *Существует функция* $U^1 \in \mathrm{Com}(\mathbb{N} \times \mathbb{N}, \mathbb{N})$, *являющаяся универсальной для класса* $\mathrm{Com}(\mathbb{N}, \mathbb{N})$.

(УВП, теорема 12', с. 105.)

Доказательство. Пусть символом 1 из определения 6.21 является a_1.

Определим искомую функцию U^1, положив $U^1(i,n) \simeq F(\mathrm{word}_{\text{Ы}}(i)a_1^n)$, где $\mathrm{word}_{\text{Ы}}$ — вычислимая биекция из $\mathbb{N}$ в Ы* (см. определение 6.64), а F — функция из теоремы 6.98 для случая $r = 2$ (то есть $\Sigma = \{a_0, a_1\}$, где $a_0 = \#$ и $a_1 = 1$).

Можно проверить, что функция U^1 вычислима. Очевидно, если для некоторой частичной функции f из $\mathbb{N}$ в $\mathbb{N}$ выполнено условие $(\exists i \in \mathbb{N})\,(\forall n \in \mathbb{N})\,f(n) \simeq U^1(i,n)$, то f вычислима. Осталось проверить, что для каждой частичной функции $f \in \mathrm{Com}(\mathbb{N}, \mathbb{N})$ существует такое число $i \in \mathbb{N}$, что для каждого $n \in \mathbb{N}$ выполнено условие $f(n) \simeq U^1(i,n)$. Положим $i = \mathrm{word}_{\text{Ы}}^{-1}(\mathrm{Code}(\mathcal{M}))$, где $\mathcal{M}$ — машина Тьюринга с ленточным алфавитом $\{a_0, a_1\}$ и множеством состояний $\{q_0, q_1, \ldots, q_s\}$ для некоторого $s \geqslant 1$. □

Пример 6.102. Вычислим натуральное число, соответствующее коду машины Тьюринга из примера 6.92:

$$\begin{aligned}
&\mathrm{word}_{\text{Ы}}^{-1}(q\mathbf{1}a{\to}qa\mathbf{1}\mathrm{L}q\mathbf{1}a\mathbf{1}{\to}q\mathbf{1}a\mathbf{1}\mathrm{N}) = \\
&\quad = 5\cdot 7^{17} + 7\cdot 7^{16} + 6\cdot 7^{15} + 1\cdot 7^{14} + 5\cdot 7^{13} + 6\cdot 7^{12} + 7\cdot 7^{11} + 2\cdot 7^{10} + \\
&\qquad + 5\cdot 7^{9} + 7\cdot 7^{8} + 6\cdot 7^{7} + 7\cdot 7^{6} + 1\cdot 7^{5} + 5\cdot 7^{4} + 7\cdot 7^{3} + 6\cdot 7^{2} + 7\cdot 7^{1} + 3\cdot 7^{0} = \\
&\quad = 1425528822986691.
\end{aligned}$$

Следовательно, $U^1(1425528822986691, 2000) = 2001$.

Пример 6.103. Значение $U^1(20, 2000)$ не определено, так как $\mathrm{word}_{\text{Ы}}(20) = \mathrm{L}a$ и слово $\mathrm{L}a$ не является кодом никакой машины Тьюринга из класса $\mathcal{C}_2$.

Теорема 6.104. *Для каждого* $k \geqslant 1$ *существует функция* $U^k \in \mathrm{Com}(\mathbb{N} \times \mathbb{N}^k, \mathbb{N})$, *являющаяся универсальной для класса* $\mathrm{Com}(\mathbb{N}^k, \mathbb{N})$.

(УВП, теорема 12', с. 105.)

Доказательство. Для $k = 1$ теорема уже доказана. При $k \geqslant 2$ положим

$$U^k(i, n_1, \ldots, n_k) \simeq U^1(i, c^k(n_1, \ldots, n_k)).$$

□

Определение 6.105. В дальнейшем для каждого $k \geqslant 1$ через U^k будем обозначать конкретную универсальную функцию, построенную в доказательстве теоремы 6.104. Для каждого $k \geqslant 1$ и каждого $i \in \mathbb{N}$ обозначим через φ_i^k функцию $\lambda n_1 \ldots n_k . U^k(i, n_1, \ldots, n_k)$.

Замечание 6.106. $\mathrm{Com}(\mathbb{N}^k, \mathbb{N}) = \{\varphi_0^k, \varphi_1^k, \varphi_2^k, \ldots\}$.

6.17 Перечислимое неразрешимое множество

[К1, с. 14–15], **[УВП, 5.5]**, **[ВШ3, 2.2–2.3]**, **[П2, 12]**, **[ЛМ, III.3]**, **[Кли, 42]**, [Мал, 6.3], [КД, с. 193–194, 195]

Определение 6.107. Пусть f и g — частичные функции из X в Y. Функция g называется *продолжением* (или *расширением*) функции f, если $\mathrm{D}\,f \subseteq \mathrm{D}\,g$ и $(\forall x \in \mathrm{D}\,f)\; f(x) = g(x)$.

Замечание 6.108. Каждая частичная функция является продолжением самой себя.

Замечание 6.109. У всюду определённой функции нет других продолжений, кроме неё самой.

Теорема 6.110. *Существует такая функция $f \in \mathrm{Com}(\mathbb{N}, \mathbb{N})$, что ни одна функция из $\mathrm{TCom}(\mathbb{N}, \mathbb{N})$ не является продолжением функции f.*

(K1, теорема 5.2, с. 14.)

(УВП, теорема 13, с. 106.)

Доказательство. Положим $f(n) \simeq U^1(n, n) + 1$. Функция f вычислима, так как она является композицией трёх вычислимых функций: $\lambda n.\langle n, n\rangle$, U^1 и $\lambda y.y + 1$.

Проведём доказательство от противного. Пусть функция $g \in \mathrm{TCom}(\mathbb{N}, \mathbb{N})$ является продолжением функции f. Тогда существует такое натуральное число m, что $g(n) \simeq U^1(m, n)$ для всех $n \in \mathbb{N}$. Так как $!\,g(m)$, то $!\,U^1(m, m)$ и $U^1(m, m) = g(m)$. Следовательно, $!\,f(m)$ и $f(m) = U^1(m, m) + 1 = g(m) + 1 \neq g(m)$. Мы видим, что функция g не является продолжением функции f. Противоречие. □

Теорема 6.111. *Существует перечислимое неразрешимое множество $K \subseteq \mathbb{N}$.*

(K1, следствие 5.3, с. 15.)

(УВП, теорема 14, с. 106.)

Доказательство. Положим $K = \mathrm{D}\, f$, где f — функция из теоремы 6.110.

Проведём доказательство от противного. Пусть множество K разрешимо. Тогда функция $g\colon \mathbb{N} \to \mathbb{N}$, заданная формулой

$$g(n) = \begin{cases} f(n), & \text{если } n \in K, \\ 0, & \text{если } n \notin K, \end{cases}$$

вычислима. Для вычисления $g(n)$ по данному $n \in \mathbb{N}$ можно использовать следующий алгоритм.

```
if (χ_K(n) == 1) { return f(n); }
return 0;
```

Очевидно, функция g является продолжением функции f. Противоречие. □

Теорема 6.112. *Существует перечислимое множество $K \subseteq \mathbb{N}$ с неперечислимым дополнением.*

(K1, следствие 5.4, с. 15.)

Доказательство. Рассмотрим перечислимое множество K из теоремы 6.111. Согласно теореме 6.72 множество $\mathbb{N} \setminus K$ неперечислимо. □

Упражнение 6.113. Существуют ли такие множества $A \subseteq \mathbb{N}^2$ и $B \subseteq \mathbb{N}$, что A и $\mathrm{пр}_1(A) \vartriangle B$ разрешимы, но B неперечислимо?

Ответ 6.113. Да.

6.18 Неразрешимость проблемы остановки

[K1, с. 16], **[П2, 12]**, **[ВШЗ, 2.3]**, **[УВП, 5.8]**, [КД, с. 195–196], [Bil, 14]

Определение 6.114 (проблема остановки). Пусть зафиксирован алфавит Σ_0, не содержащий бланка $\#$. *Массовой проблемой остановки* называется следующая задача: по коду $\mathrm{Code}(\mathcal{M})$ машины Тьюринга с ленточным алфавитом $\Sigma_0 \cup \{\#\}$ и слову $v \in \Sigma_0^*$ выяснить, остановится ли машина $\mathcal{M}$, начав работу с конфигурации $q_1\#v$.

(K1, определение 5.5, с. 16.)

Теорема 6.115. *Массовая проблема остановки алгоритмически неразрешима.*

(К1, следствие 5.7, с. 16.)

Доказательство. Без ограничения общности можно считать, что $1 \in \Sigma_0$. Пусть машина $\mathcal{M}_1$ вычисляет функцию f из теоремы 6.110. Из неразрешимости множества $\mathrm{D}\, f$ следует, что неразрешима даже следующая массовая проблема: по слову вида 1^n выяснить, остановится ли машина $\mathcal{M}_1$, начав работу с конфигурации $q_1\#1^n$. □

6.19 Главная универсальная вычислимая функция

[К1, с. 12–14], **[ВШ3, 3.1]**, **[П2, 7]**, [КД, с. 198]

Определение 6.116. Функция $G\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$ называется *главной универсальной функцией*, если выполнены следующие три условия:

1) G является универсальной функцией для класса $\mathrm{Com}(\mathbb{N},\mathbb{N})$,
2) $G \in \mathrm{Com}(\mathbb{N}\times\mathbb{N},\mathbb{N})$,
3) для каждой функции $g \in \mathrm{Com}(\mathbb{N}\times\mathbb{N},\mathbb{N})$ существует такая функция $s \in \mathrm{TCom}(\mathbb{N},\mathbb{N})$, что $g(i,n) \simeq G(s(i),n)$ для любых i и n.

(ВШ3, с. 24.)

Теорема 6.117. *Главные универсальные функции существуют.*

(ВШ3, теорема 15, с. 25.)

(К1, теорема 4.4, с. 12.)

Доказательство. Положим $G(m,n) \simeq U^2(l(m),r(m),n)$ для любых m и n.

Проверим, что так определённая функция G является универсальной для класса $\mathrm{Com}(\mathbb{N},\mathbb{N})$. Пусть дана функция $f \in \mathrm{Com}(\mathbb{N},\mathbb{N})$. Рассмотрим функцию f_2, определённую соотношением $f_2(x,y) \simeq f(y)$. Существует такое число $l_0 \in \mathbb{N}$, что $f_2(x,y) \simeq U^2(l_0,x,y)$ для любых x и y. Положим $i = c(l_0,0)$. Тогда $f(y) \simeq G(i,y)$ для любого y.

Проверим теперь пункт 3) из определения главной универсальной функции. Пусть дана функция $g \in \mathrm{Com}(\mathbb{N}\times\mathbb{N},\mathbb{N})$. Существует такое число $j_0 \in \mathbb{N}$, что $g(i,n) \simeq U^2(j_0,i,n)$ для любых i и n. Положим $s(i) = c(j_0,i)$ для любого i. □

Следующая теорема даёт другое доказательство теоремы 6.117.

Теорема 6.118. *Функция U^1 является главной универсальной функцией.*

Доказательство. Пусть дана функция $g \in \mathrm{Com}(\mathbb{N}\times\mathbb{N},\mathbb{N})$. Искомая функция s ставит числу i в соответствие номер кода машины Тьюринга, вычисляющей функцию $g \circ h_i$, где функция $h_i \in \mathrm{TCom}(\mathbb{N},\mathbb{N}\times\mathbb{N})$ определена соотношением $h_i(n) = \langle i,n\rangle$. Можно проверить, что так определённая функция s вычислима. □

Теорема 6.119. *Для любых $m \geqslant 1$, $n \geqslant 1$ и для каждой функции $g \in \mathrm{Com}(\mathbb{N}^{m+n},\mathbb{N})$ существует такая функция $s \in \mathrm{TCom}(\mathbb{N}^m,\mathbb{N})$, что*

$$g(i_1,\dots,i_m,x_1,\dots,x_n) \simeq U^n(s(i_1,\dots,i_m),x_1,\dots,x_n)$$

для любых $i_1,\dots,i_m,x_1,\dots,x_n$.

(К1, теорема 4.5, с. 13.)

Доказательство. Пусть даны $m \geqslant 1$, $n \geqslant 1$ и $g \in \mathrm{Com}(\mathbb{N}^{m+n},\mathbb{N})$. Рассмотрим функцию $g'\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$, определённую так:

$$g'(l,y) \simeq g(c_{m1}(l),\dots,c_{mm}(l),c_{n1}(y),\dots,c_{n1}(y)).$$

Согласно теореме 6.118 существует такая функция $s' \in \mathrm{TCom}(\mathbb{N},\mathbb{N})$, что $g'(l,y) \simeq U^1(s'(l),y)$ для любых l и y. Определим искомую функцию s так:

$$s(i_1,\ldots,i_m) = s'(c^m(i_1,\ldots,i_m)).$$

Тогда

$$g(i_1,\ldots,i_m,x_1,\ldots,x_n) \simeq g'(c^m(i_1,\ldots,i_m),c^n(x_1,\ldots,x_n)) \simeq \\ \simeq U^1(s'(c^m(i_1,\ldots,i_m)),c^n(x_1,\ldots,x_n)) \simeq U^n(s(i_1,\ldots,i_m),x_1,\ldots,x_n).$$

□

6.20 Теорема Райса

[К1, с. 16–18], [ВШ3, 4.1], [П2, 13], [ЛМ, III.4]

Теорема 6.120 (теорема Райса). *Пусть $\mathcal{A} \subset \mathrm{Com}(\mathbb{N},\mathbb{N})$, $\mathcal{A} \neq \varnothing$, $\mathcal{A} \neq \mathrm{Com}(\mathbb{N},\mathbb{N})$. Пусть $G\colon \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ является главной универсальной функцией. Тогда множество $I_{\mathcal{A}} = \{i \in \mathbb{N} \mid (\lambda x.G(i,x)) \in \mathcal{A}\}$ неразрешимо.*

(К1, теорема 5.9, с. 17.)

(ВШ3, теорема 21, с. 33.)

Доказательство. Рассмотрим нигде не определённую функцию ζ. Возможны два случая: $\zeta \in \mathcal{A}$ и $\zeta \notin \mathcal{A}$. Проведём доказательство для первого случая (второй случай разбирается аналогично).

Пусть $\zeta \in \mathcal{A}$. Так как $\mathcal{A} \neq \mathrm{Com}(\mathbb{N},\mathbb{N})$, существует функция $h \in \mathrm{Com}(\mathbb{N},\mathbb{N}) \setminus \mathcal{A}$. Рассмотрим функцию $g\colon \mathbb{N}\times\mathbb{N} \to \mathbb{N}$, заданную формулой

$$g(i,n) \simeq \begin{cases} h(n), & \text{если } i \in K, \\ \text{не определено}, & \text{если } i \notin K. \end{cases}$$

Очевидно, $g \in \mathrm{Com}(\mathbb{N}\times\mathbb{N},\mathbb{N})$. Для вычисления $g(i,n)$ по данным i и n можно использовать следующий алгоритм.

```
if (χ*_K(i) == 1) { return h(n); }
```

Согласно определению главной универсальной функции существует такая функция $s \in \mathrm{TCom}(\mathbb{N},\mathbb{N})$, что $g(i,n) \simeq G(s(i),n)$ для любых i и n. Докажем, что $\chi_{\mathbb{N}\setminus K}(i) = \chi_{I_{\mathcal{A}}}(s(i))$ для любого $i \in \mathbb{N}$. Действительно, если $\chi_{\mathbb{N}\setminus K}(i) = 0$, то $i \in K$ и, следовательно, для любого $n \in \mathbb{N}$ имеем $G(s(i),n) \simeq g(i,n) \simeq h(n)$, откуда получаем $(\lambda x.G(s(i),x)) = h \notin \mathcal{A}$ и $s(i) \notin I_{\mathcal{A}}$, то есть $\chi_{I_{\mathcal{A}}}(s(i)) = 0$. Если же $\chi_{\mathbb{N}\setminus K}(i) = 1$, то $i \notin K$ и, следовательно, для любого $n \in \mathbb{N}$ имеем $G(s(i),n) \simeq g(i,n) \simeq \zeta(n)$, откуда получаем $(\lambda x.G(s(i),x)) = h \in \mathcal{A}$ и $s(i) \in I_{\mathcal{A}}$, то есть $\chi_{I_{\mathcal{A}}}(s(i)) = 1$. Из равенства $\chi_{\mathbb{N}\setminus K}(i) = \chi_{I_{\mathcal{A}}}(s(i))$, вычислимости функции s и невычислимости функции $\chi_{\mathbb{N}\setminus K}$ следует невычислимость функции $\chi_{I_{\mathcal{A}}}$. □

Теорема 6.121. *Пусть $\mathcal{A} \subset \mathrm{Com}(\mathbb{N},\mathbb{N})$, $\mathcal{A} \neq \varnothing$, $\mathcal{A} \neq \mathrm{Com}(\mathbb{N},\mathbb{N})$. Тогда множество $I_{\mathcal{A}} = \{i \in \mathbb{N} \mid \varphi_i^1 \in \mathcal{A}\}$ неразрешимо.*

(К1, теорема 5.9, с. 17.)

Доказательство. Согласно определению $\varphi_i^1 = \lambda x.U^1(i,x)$. Осталось применить теорему 6.120. □

Упражнение 6.122. Разрешимо ли множество $\{i \in \mathbb{N} \mid !\,\varphi^1_i(7)\}$?
Ответ 6.122. Нет. Оно равно множеству $I_{\mathcal{A}}$, где $\mathcal{A} = \{f \in \mathrm{Com}(\mathbb{N}, \mathbb{N}) \mid !\,f(7)\}$.

Упражнение 6.123. Разрешимо ли множество

$$\{i \in \mathbb{N} \mid \text{при вычислении } \varphi^1_i(7) \text{ машина с номером } i \text{ остановится, сделав не больше трёх шагов}\}?$$

Ответ 6.123. Да.
Упражнение 6.124. Разрешимо ли множество $\{(i,j) \in \mathbb{N}^2 \mid \mathrm{E}\,\varphi^1_i \vartriangle \mathrm{E}\,\varphi^1_j = \mathbb{N}\}$?
Ответ 6.124. Нет.
Упражнение 6.125. Перечислимо ли множество

$$\{(i,j) \in \mathbb{N}^2 \mid i \notin \mathrm{D}\,\varphi^1_j \text{ и } j \notin \mathrm{D}\,\varphi^1_i\}?$$

Ответ 6.125. Нет.

7 Арифметика

7.1 Арифметические множества и функции

[П2, 24], [Мал, 13.3], [ВШ2, 3.4]

Определение 7.1. Множество $L \subseteq \mathbb{N}^k$ называется *арифметическим*, если в стандартной интерпретации языка арифметики выразим соответствующий ему k-местный предикат $\boldsymbol{L}$ на множестве $\mathbb{N}$, определённый соотношением

$$\boldsymbol{L}(a_1, \ldots, a_k) = \text{И тогда и только тогда, когда } \langle a_1, \ldots, a_k \rangle \in L.$$

Про арифметическую формулу A, выражающую предикат $\boldsymbol{L}$ (относительно списка переменных $v_1, \ldots, v_k$), говорят, что она *определяет* множество L (относительно списка переменных $v_1, \ldots, v_k$).

Пример 7.2. Множество $\{2n \mid n \in \mathbb{N}\}$ является арифметическим. Его определяет формула $\exists y\, (x = y + y)$ (относительно списка переменных x).

Пример 7.3. Множество $\{\langle x_1, x_2 \rangle \in \mathbb{N}^2 \mid x_1 \leqslant x_2\}$ является арифметическим. Его определяет формула $\exists x_3\, (x_1 = x_2 + x_3)$ (относительно списка переменных x_1, x_2).

Определение 7.4. Для каждого натурального числа m через $\overline{m}$ обозначается терм $\underbrace{S(\ldots S(}_{m \text{ раз}} 0) \ldots)$. Иногда этот терм называют *нумералом* для числа m.
(БДж, с. 213.)

Замечание 7.5. Если $\mathfrak{N}$ — стандартная интерпретация языка арифметики, то $[\overline{m}]^{\mathfrak{N}} = m$ для каждого $m \in \mathbb{N}$.

Замечание 7.6. Пусть $L \subseteq \mathbb{N}^k$ и A — арифметическая формула, причём $\mathrm{FV}(A) \subseteq \{v_1, \ldots, v_k\}$, где все переменные v_i различные. Тогда следующие условия равносильны.

1. Формула A определяет множество L относительно списка переменных $v_1, \ldots, v_k$.
2. Для любых $m_1, \ldots, m_k \in \mathbb{N}$ формула $A[\overline{m_1}/v_1] \ldots [\overline{m_k}/v_k]$ истинна в стандартной интерпретации языка арифметики тогда и только тогда, когда $\langle m_1, \ldots, m_k \rangle \in L$.

Пример 7.7. Множество $\{4^x \mid x \in \mathbb{N}\}$ является арифметическим. Относительно списка переменных x его определяет формула

$$\exists w_0\, (x = w_0 \cdot w_0 \wedge \forall x_0\, (\exists z_0\, (w_0 = x_0 \cdot z_0) \to x_0 = S(0) \vee \exists z_0\, (x_0 = z_0 + z_0))),$$

а также формула

$$\exists w_0\, (x = w_0 \cdot w_0 \wedge \neg \exists y_0\, \exists z_0\, (w_0 = y_0 \cdot S(S(S(z_0 + z_0))))).$$

Пример 7.8. Множество $\{\langle y, w \rangle \in \mathbb{N}^2 \mid w = 2^{\lfloor \log_2 (y+1) \rfloor}\}$ является арифметическим. Его определяет формула

$$\exists z_0\, (w + z_0 = S(y)) \wedge \exists z_0\, (S(S(y)) + z_0 = w + w) \wedge \forall x_0\, (\exists z_0\, (w = x_0 \cdot z_0) \to x_0 = S(0) \vee \exists z_0\, (x_0 = z_0 + z_0))$$

(относительно списка переменных y, w). Обозначим эту формулу $\mathrm{Len}(y, w)$.

Определение 7.9. Будем называть k-местную частичную функцию из $\mathbb{N}$ в $\mathbb{N}$ *арифметической*, если её график является арифметическим множеством.
(Мал, с. 271.)

Пример 7.10. Одноместная функция $\lambda y. 2^{\lfloor \log_2 (y+1) \rfloor}$ из $\mathbb{N}$ в $\mathbb{N}$ является арифметической.

Пример 7.11. Канторовская нумерующая функция c является арифметической. Её график можно определить, например, формулой $(x+y)\cdot S(x+y)+x+x=z+z$ (относительно списка переменных x, y, z). Обозначим эту формулу $\mathrm{Pair}(x,y,z)$.

7.2 Свойства замкнутости класса арифметических множеств

[П2, 24]

Теорема 7.12.

1. *Если множество $L \subseteq \mathbb{N}^k$ является арифметическим, то и множество $\mathbb{N}^k \setminus L$ является арифметическим.*
2. *Если множества $L_1 \subseteq \mathbb{N}^k$ и $L_2 \subseteq \mathbb{N}^k$ являются арифметическими, то и множество $L_1 \cup L_2$ является арифметическим.*
3. *Если множества $L_1 \subseteq \mathbb{N}^k$ и $L_2 \subseteq \mathbb{N}^k$ являются арифметическими, то и множество $L_1 \cap L_2$ является арифметическим.*

(П2, теорема 24.1, с. 29.)

Доказательство. Если формула G определяет множество L (относительно списка переменных $v_1, \ldots, v_k$), то формула $\neg G$ определяет множество $\mathbb{N}^k \setminus L$. Если формула G_1 определяет множество L_1 и формула G_2 определяет множество L_2, то формула $G_1 \vee G_2$ определяет множество $L_1 \cup L_2$ и формула $G_1 \wedge G_2$ определяет множество $L_1 \cap L_2$. □

Пример 7.13. Формула $x = S(0) \vee \exists y\,(x = y + y)$ определяет множество $\{1\} \cup \{2n \mid n \in \mathbb{N}\}$ (относительно списка переменных x).

Теорема 7.14. *Если множества $L_1 \subseteq \mathbb{N}$ и $L_2 \subseteq \mathbb{N}$ являются арифметическими, то и множество $L_1 \times L_2$ является арифметическим.*

Доказательство. Если формула G_1 определяет множество L_1 относительно списка переменных v_1 и формула G_2 определяет множество L_2 относительно списка переменных v_2, где v_1 и v_2 — различные переменные, то формула $G_1 \wedge G_2$ определяет множество $L_1 \times L_2$ относительно списка переменных v_1, v_2. □

Теорема 7.15. *Если множество $L \subseteq \mathbb{N}^2$ является арифметическим, то и множество $\mathrm{пр}_1 L$ является арифметическим.*

Доказательство. Если формула G определяет множество L относительно списка переменных v_1, v_2, то формула $\exists v_2\, G$ определяет множество $\mathrm{пр}_1 L$ относительно списка переменных v_1. □

7.3 Кодирование конечных множеств в арифметике

[ВШ2, 3.4]

Пример 7.16. Множество $\{\langle x,y,z\rangle \in \mathbb{N}^3 \mid \mathrm{word}_{\{0,1\}}(x) \circ \mathrm{word}_{\{0,1\}}(y) = \mathrm{word}_{\{0,1\}}(z)\}$ является арифметическим (здесь $\circ$ обозначает операцию конкатенации (соединения, склеивания) слов). Соответствующий предикат выражается формулой $\exists w\,(\mathrm{Len}(y,w) \wedge z = (x\cdot w)+y)$ (относительно списка переменных x, y, z).

Пример 7.17. Рассмотрим формулу

$$\exists z_1\,\exists z_2\,\exists w_1\,\exists w_2\,\exists w_3\,(\mathrm{Len}(y_1,w_1)\wedge \mathrm{Len}(z_2,w_2)\wedge \mathrm{Len}(x,w_3)\wedge \\ \wedge (y_2=(((z_1\cdot w_1+y_1)\cdot w_3+x)\cdot w_1+y_1)\cdot w_2+z_2)).$$

Относительно списка свободных переменных x, y_1, y_2 эта формула выражает трёхместный предикат $\mathbf{Set^{(3)}}$, обладающий следующими двумя свойствами.

1. Для любых $a_1, a_2 \in \mathbb{N}$ множество $\{x\in\mathbb{N} \mid \mathbf{Set^{(3)}}(x,a_1,a_2)\}$ конечно.
2. Для любого конечного множества натуральных чисел L найдутся такие $a_1,a_2\in\mathbb{N}$, что $\{x\in\mathbb{N}\mid \mathbf{Set^{(3)}}(x,a_1,a_2)\}=L$.

В учебнике [ВШ2, с. 102] этот предикат обозначается $S(x,a,b)$.

Пример 7.18. Рассмотрим формулу

$$\exists y_2\,\exists z_1\,\exists z_2\,\exists w_1\,\exists w_2\,\exists w_3\,(\forall x_3\,(\exists z_3\,(w_1=x_3\cdot z_3)\to x_3=S(0)\vee \exists z_3\,(x_3=z_3+z_3))\wedge y=S(y_2+y_2)\cdot w_1\wedge \\ \wedge \mathrm{Len}(z_2,w_2)\wedge \mathrm{Len}(x_3,w_3)\wedge (y_2=(S((S(z_1)\cdot(w_1+w_1)+w_1)\cdot w_3+x_3)\cdot(w_1+w_1)+w_1)\cdot w_2+z_2)).$$

Относительно списка свободных переменных x, y эта формула выражает двуместный предикат $\mathbf{Set^{(2)}}$, обладающий следующими двумя свойствами.

1. Для любого натурального числа a множество $\{x\in\mathbb{N}\mid \mathbf{Set^{(2)}}(x,a)\}$ конечно.
2. Для любого конечного множества натуральных чисел L существует такое натуральное число a, что $\{x\in\mathbb{N}\mid \mathbf{Set^{(2)}}(x,a)\}=L$.

Иными словами, функция $a\mapsto\{x\in\mathbb{N}\mid \mathbf{Set^{(2)}}(x,a)\}$ является сюръекцией из $\mathbb{N}$ в множество всех конечных подмножеств множества $\mathbb{N}$.

Обозначим рассмотренную формулу $\mathrm{Set}^{(2)}(x,y)$. Если в формуле $\mathrm{Set}^{(2)}(x,y)$ экономно вынести кванторы, то можно получить равносильную ей формулу с 15 кванторами (с кванторным префиксом $\exists^{10}\forall^2\exists^3$).

Пример 7.19. Функция $\lambda xy.x^y$ является арифметической (здесь мы считаем, что $0^0=1$). В сигнатуре $\langle 0,S,+,\cdot,c,=\rangle$, где функциональный символ c интерпретируется как канторовская нумерующая функция, относительно списка переменных x,y,z график функции $\lambda xy.x^y$ можно определить формулой

$$\exists w_4\,(\mathrm{Set}^{(2)}(c(y,z),w_4)\wedge\forall x_4\,(\mathrm{Set}^{(2)}(x_4,w_4)\to \\ \to x_4=c(0,S(0))\vee\exists y_1\,\exists z_1\,(\mathrm{Set}^{(2)}(c(y_1,z_1),w_4)\wedge x_4=c(S(y_1),z_1\cdot x))))$$

Так как канторовская нумерующая функция является арифметической, эту формулу можно заменить на некоторую формулу в сигнатуре $\langle 0,S,+,\cdot,=\rangle$. Например, подходит формула

$$\exists w_4\,\exists x_5\,(\mathrm{Pair}(y,z,x_5)\wedge\mathrm{Set}^{(2)}(x_5,w_4)\wedge\forall x_4\,(\mathrm{Set}^{(2)}(x_4,w_4)\to \\ \to x_4=S(0)\vee\exists y_1\,\exists z_1\,\exists x_6\,(\mathrm{Pair}(y_1,z_1,x_6)\wedge\mathrm{Set}^{(2)}(x_6,w_4)\wedge\mathrm{Pair}(S(y_1),z_1\cdot x,x_4)))).$$

Здесь учтено, что $c(0,1)=1$.

Пример 7.20. Функция $\lambda y.y!$ (факториал) является арифметической. График этой функции можно определить (относительно списка переменных y,z) формулой

$$\exists w_4\,\exists x_5\,(\mathrm{Pair}(y,z,x_5)\wedge\mathrm{Set}^{(2)}(x_5,w_4)\wedge\forall x_4\,(\mathrm{Set}^{(2)}(x_4,w_4)\to \\ \to x_4=S(0)\vee\exists y_1\,\exists z_1\,\exists x_6\,(\mathrm{Pair}(y_1,z_1,x_6)\wedge\mathrm{Set}^{(2)}(x_6,w_4)\wedge\mathrm{Pair}(S(y_1),z_1\cdot S(y_1),x_4)))).$$

7.4 Арифметичность перечислимых множеств и вычислимых функций (без доказательства)

[П2, 24], **[ВШ3, 10.3]**, **[К1, с. 18–19]**, **[Мен, 3.2–3.3]**, **[БДж, 14]**, [Bil, 17], [ВШ2, 3.4]

Теорема 7.21 (без доказательства). *Если* $f \in \mathrm{Com}(\mathbb{N}^k, \mathbb{N})$, *то функция* f *является арифметической.*

(П2, теорема 24.2, с. 29.)

Пример 7.22. Функции $\dot{-}$, c, l, r, $\lambda xyz.y$ являются арифметическими.

Определение 7.23. Для любых m и n, удовлетворяющих неравенствам $1 \leqslant m \leqslant n$, функция $\lambda x_1. \dots .\lambda x_n.x_m$ обозначается I_n^m.

Теорема 7.24. *Каждое перечислимое подмножество множества* $\mathbb{N}^k$ *является арифметическим.*

(П2, теорема 24.3, с. 31.)

(К1, теорема 6.2, с. 18.)

Доказательство. Пусть множество $L \subseteq \mathbb{N}^k$ перечислимо. Тогда существует такая функция $f \in \mathrm{Com}(\mathbb{N}^k, \mathbb{N})$, что $L = \mathrm{D}\, f$. Согласно теореме 7.21 существует арифметическая формула G, определяющая множество $\mathrm{Гр}_f$ относительно некоторого списка переменных $v_1, \dots, v_k, v_{k+1}$. Очевидно, формула $\exists v_{k+1}\, G$ определяет множество L относительно списка переменных $v_1, \dots, v_k$. □

Теорема 7.25. *Существует неперечислимое арифметическое подмножество множества* $\mathbb{N}$.

(П2, теорема 24.4, с. 31.)

Доказательство. Множество $\mathbb{N} \setminus K$ является неперечислимым и арифметическим. □

7.5 Представление арифметических формул словами в конечном алфавите

[К1, с. 18], **[П2, 25]**, **[Мал, 13.3]**, **[Кли, 43]**, [УВП, 5.6], [КД, с. 181–182, 189], [Bil, 16]

Определение 7.26. Предположим, что набором индивидных переменных языка арифметики является множество $\{x_1, x_2, x_3, \dots\}$. Обозначим через Ю алфавит $\{0, S, +, \cdot, =, \forall, \exists, \neg, \wedge, \vee, \rightarrow, x, \mathbf{1}, \mathbf{(}, \mathbf{)}, \mathbf{,}\}$. Каждую арифметическую формулу отождествим со словом в алфавите Ю, полученным заменой индивидных переменных x_i на выражения $x\mathbf{1}^i$.

Пример 7.27. Формула $\exists x_3\, (x_1 + x_3 = x_2)$ отождествляется со словом

$$\exists x\mathbf{111}{=}\mathbf{(}{+}\mathbf{(}x\mathbf{1,}x\mathbf{111}\mathbf{),}x\mathbf{11}\mathbf{)}.$$

Теорема 7.28.

1. *Множество всех термов языка арифметики разрешимо.*
2. *Множество всех формул языка арифметики разрешимо.*
3. *Множество всех замкнутых формул языка арифметики разрешимо.*

Теорема 7.28 является частным случаем приведённой ниже теоремы 7.30.

Определение 7.29. Сигнатура $\Omega = \langle \mathrm{Fn}, \mathrm{Pr} \rangle$ называется *конечной*, если множества Fn и Pr конечны.

Теорема 7.30. *Пусть Ω — конечная сигнатура.*

1. *Множество всех термов сигнатуры Ω разрешимо.*
2. *Множество всех формул сигнатуры Ω разрешимо.*
3. *Множество всех замкнутых формул сигнатуры Ω разрешимо.*

(УВП, теорема 15, с. 107.)

7.6 Неперечислимость множества арифметических истин

[К1, с. 19], [П2, 26, 27]

Теорема 7.31. *Множество всех замкнутых арифметических формул, истинных в стандартной интерпретации языка арифметики, неперечислимо.*

(П2, теорема 26.2, с. 32.)

(П2, второе доказательство теоремы 27.2, с. 33.)

(К1, следствие 6.3, с. 19.)

(Мал, следствие, с. 273.)

(ВШ3, теорема 72, с. 139.)

Доказательство. Обозначим через $\mathfrak{N}$ стандартную интерпретацию языка арифметики. Тогда множество $\mathrm{Th}(\mathfrak{N})$ состоит из всех замкнутых арифметических формул, истинных в стандартной интерпретации. Проведём доказательство от противного. Пусть множество $\mathrm{Th}(\mathfrak{N})$ полуразрешимо, то есть $\chi^*_{\mathrm{Th}(\mathfrak{N})} \in \mathrm{Com}(Ю^*, \mathbb{N})$.

Согласно теореме 6.112 существует перечислимое множество $K \subseteq \mathbb{N}$ с неперечислимым дополнением $\mathbb{N} \setminus K$. Согласно теореме 7.24 существует арифметическая формула G, определяющая множество K. Обозначим единственную свободную переменную формулы G через v_1.

Рассмотрим функцию h из $\mathbb{N}$ в $Ю^*$, ставящую числу n в соответствие формулу $\neg G[\overline{n}/v_1]$, рассматриваемую как слово в алфавите Ю. Можно проверить, что $h \in \mathrm{Com}(\mathbb{N}, Ю^*)$. Докажем, что $\chi^*_{\mathbb{N}\setminus K}(n) \simeq \chi^*_{\mathrm{Th}(\mathfrak{N})}(h(n))$ для любого $n \in \mathbb{N}$. Действительно,

$$\chi^*_{\mathbb{N}\setminus K}(n) \simeq 1 \iff n \in \mathbb{N} \setminus K \iff n \notin K \iff \mathfrak{N} \nvDash G[\overline{n}/v_1] \iff$$
$$\iff \mathfrak{N} \vDash \neg G[\overline{n}/v_1] \iff h(n) \in \mathrm{Th}(\mathfrak{N}) \iff \chi^*_{\mathrm{Th}(\mathfrak{N})}(h(n)) \simeq 1.$$

Следовательно, $\chi^*_{\mathbb{N}\setminus K} \in \mathrm{Com}(\mathbb{N}, \mathbb{N})$ и множество $\mathbb{N} \setminus K$ перечислимо. Противоречие. □

7.7 Перечислимость множества теорем

[УВП, 5.6], **[П2, 27]**, **[ВШ3, 10.5]**, **[БДж, 15]**, [КД, с. 183]

Определение 7.32 (разрешимо аксиоматизируемая теория). Теория первого порядка с конечной сигнатурой называется *разрешимо аксиоматизируемой*, если её множество аксиом разрешимо.

(УВП, с. 107.)

(БДж, с. 237.)

Теорема 7.33. *Множество теорем разрешимо аксиоматизируемой теории первого порядка является перечислимым.*

(УВП, теорема 16, с. 107.)

Доказательство. Полухарактеристическую функцию множества теорем можно вычислить методом перебора: алгоритм перебирает все выводы из аксиом данной теории и если последняя формула вывода совпадает с проверяемой замкнутой формулой, то возвращает единицу. □

7.8 Первая теорема Гёделя о неполноте формальной арифметики

[П2, 27], **[Мал, 13.3]**, **[ВШ2, 5.4]**, **[ВШ3, 10.4–10.5]**, **[Мен, 3.4–3.5]**, **[БДж, 15]**, **[Кли, 43]**, [УВП, 3.7], [КД, с. 189–191, 199–202], [Bil, 18]

Теорема 7.34. *Пусть T — разрешимо аксиоматизируемая теория в языке арифметики. Пусть все аксиомы теории T истинны в стандартной интерпретации языка арифметики. Тогда существует замкнутая арифметическая формула, истинная в стандартной интерпретации, но не являющаяся теоремой теории T.*

(П2, теорема 27.1, с. 33.)

Доказательство. Проведём доказательство от противного. Обозначим через $\mathfrak{N}$ стандартную интерпретацию языка арифметики. Пусть все истинные в $\mathfrak{N}$ замкнутые арифметические формулы являются теоремами теории T. Так как все аксиомы теории T истинны в $\mathfrak{N}$, то и все теоремы теории T истинны в $\mathfrak{N}$. Следовательно множество теорем теории T совпадает с множеством $\mathrm{Th}(\mathfrak{N})$. Согласно теореме 7.33 это множество перечислимо, а согласно теореме 7.31 оно неперечислимо. Противоречие. □

8 Приложения и обобщения

8.1 Изоморфизм интерпретаций

[ВШ2, 3.9], **[УВП, 2.13]**, [Bil, 9]

Определение 8.1. Пусть даны две (не обязательно различные) интерпретации $\mathfrak{L} = \langle L, \Omega \rangle$ и $\mathfrak{M} = \langle M, \Omega \rangle$ одной и той же сигнатуры Ω. Пусть φ — некоторая функция из L в M.

1. Говорят, что функция φ *сохраняет* n-местный функциональный символ f, если для всех $a_1, \ldots, a_n \in L$ выполнено $\varphi(f^{\mathfrak{L}}(a_1, \ldots, a_n)) = f^{\mathfrak{M}}(\varphi a_1, \ldots, \varphi a_n)$.
2. Говорят, что функция φ *сохраняет* n-местный предикатный символ P, если для всех $a_1, \ldots, a_n \in L$ выполнено $P^{\mathfrak{L}}(a_1, \ldots, a_n) = P^{\mathfrak{M}}(\varphi a_1, \ldots, \varphi a_n)$.
3. Функция φ называется *изоморфизмом из* $\mathfrak{L}$ *в* $\mathfrak{M}$, если φ является биекцией и сохраняет все функциональные и предикатные символы сигнатуры Ω.

(УВП, с. 46–47.)

Определение 8.2. Две интерпретации $\mathfrak{L}$ и $\mathfrak{M}$ одной и той же сигнатуры называются *изоморфными* (обозначение $\mathfrak{L} \simeq \mathfrak{M}$), если существует изоморфизм из $\mathfrak{L}$ в $\mathfrak{M}$.

(УВП, с. 47.)

Пример 8.3. Рассмотрим сигнатуру Ω, содержащую двуместный функциональный символ $\circ$ и двуместный предикатный символ $\leqslant$. Введём обозначение $\mathbb{R}_+ = \{a \in \mathbb{R} \mid a > 0\}$. Рассмотрим интерпретацию $\mathfrak{L} = \langle \mathbb{R}, \Omega \rangle$, где $a \circ^{\mathfrak{L}} b = a + b$, и интерпретацию $\mathfrak{M} = \langle \mathbb{R}_+, \Omega \rangle$ где $a \circ^{\mathfrak{M}} b = a \cdot b$. В обеих интерпретациях символу $\leqslant$ соответствует обычный предикат нестрогого порядка на действительных числах. Функция $\varphi\colon \mathbb{R} \to \mathbb{R}_+$, определённая равенством $\varphi(a) = e^a$, является изоморфизмом из $\mathfrak{L}$ в $\mathfrak{M}$, так как для любых $a, b \in \mathbb{R}$ выполняется равенство $\varphi(a \circ^{\mathfrak{L}} b) = \varphi(a) \circ^{\mathfrak{M}} \varphi(b)$ и условие $a \leqslant b$ равносильно условию $\varphi(a) \leqslant \varphi(b)$.

Теорема 8.4. *Отношение $\simeq$ рефлексивно, симметрично и транзитивно.*

(УВП, теорема 10, с. 47.)

Доказательство. Используем тождественное отображение, обратное отображение и композицию двух отображений. ☐

8.2 Плотные линейно упорядоченные множества без первого и последнего элемента

[Мен, с. 89]

Определение 8.5. Если к теории плотных линейно упорядоченных множеств добавить аксиомы $\forall x\, \exists y\, y < x$ и $\forall x\, \exists y\, x < y$, то получим *теорию плотных линейно упорядоченных множеств без первого и последнего элемента*. Модели этой теории называются *плотными линейно упорядоченными множествами без первого и последнего элемента*.

8.3 Элиминация кванторов

[ВШ2, 3.6], [Мен, с. 107]

8.6. В этом разделе мы разрешаем использовать в формулах логики предикатов нульместные пропозициональные связки $\bot$ и $\top$. При этом в определение истинностного значения замкнутой формулы добавляются следующие пункты: $[\bot]^{\mathfrak{M}} = $ Л, $[\top]^{\mathfrak{M}} = $ И.

Определение 8.7 (равносильность формул в интерпретации). Пусть A и B — формулы сигнатуры Ω, а $\mathfrak{M}$ — интерпретация сигнатуры Ω. Формулы A и B *равносильны в интерпретации* $\mathfrak{M}$, если замыкание формулы $(A \leftrightarrow B)$ истинна в интерпретации $\mathfrak{M}$.

Замечание 8.8. Формулы A и B сигнатуры Ω равносильны тогда и только тогда, когда они равносильны в каждой интерпретации сигнатуры Ω.

Теорема 8.9. *Каждая формула A сигнатуры упорядоченных множеств равносильна в стандартной интерпретации на множестве $\mathbb{Q}$ некоторой бескванторной формуле B, удовлетворяющей условию $\mathrm{FV}(B) \subseteq \mathrm{FV}(A)$.*

(ВШ2, теорема 30, с. 112.)

8.10. Прежде чем доказать теорему 8.9, докажем несколько лемм. Для удобства обозначим стандартную интерпретацию сигнатуры $\langle =, < \rangle$ на множестве $\mathbb{Q}$ буквой $\mathfrak{Q}$.

Лемма 8.11. *Пусть формула A имеет вид $\exists v\,(A_1 \wedge \ldots \wedge A_n)$, где $A_1, \ldots, A_n$ — атомарные формулы сигнатуры упорядоченных множеств. Тогда формула A равносильна в $\mathfrak{Q}$ некоторой бескванторной формуле B, удовлетворяющей условию* $\mathrm{FV}(B) \subseteq \mathrm{FV}(A)$.

Доказательство. Докажем лемму индукцией по n. Считаем, что при $n = 0$ запись $A_1 \wedge \ldots \wedge A_n$ обозначает формулу $\top$. (Очевидно, при любом $n \geqslant 1$ имеет место равносильность $A_1 \wedge \ldots \wedge A_n \sim (A_1 \wedge \ldots \wedge A_{n-1}) \wedge A_n$.)

Базис индукции (случай $n = 0$) очевиден. В доказательстве шага индукции рассмотрим несколько случаев. Для упрощения обозначений будем считать, что каждый раз интересующая нас атомарная формула находится в конце формулы $A_1 \wedge \ldots \wedge A_n$.

Если одна из атомарных формул, например A_n, не содержит переменную v, то используем равносильность

$$\exists v\,(A_1 \wedge \ldots \wedge A_{n-1} \wedge A_n) \sim A_n \wedge \exists v\,(A_1 \wedge \ldots \wedge A_{n-1}).$$

Если одна из атомарных формул, например A_n, имеет вид $v = v$, то заменим формулу $\exists v\,(A_1 \wedge \ldots \wedge A_{n-1} \wedge v = v)$ на более короткую формулу $\exists v\,(A_1 \wedge \ldots \wedge A_{n-1})$.

Если одна из атомарных формул A_i имеет вид $v < v$, то заменим формулу $\exists v\,(A_1 \wedge \ldots \wedge A_n)$ на бескванторную формулу $\bot$.

Если одна из атомарных формул, например A_n, имеет вид $v = u$, где u — отличная от v переменная, то заменим формулу $\exists v\,(A_1 \wedge \ldots \wedge A_{n-1} \wedge v = u)$ на бескванторную формулу $(A_1 \wedge \ldots \wedge A_{n-1})[u/v]$. Аналогично поступим, если одна из атомарных формул имеет вид $u = v$.

Если исключить все перечисленные выше случаи, то каждая атомарная формула A_i имеет вид $u_j < v$ или $v < w_k$, где все переменные u_j и w_k отличны от v. Без ограничения общности можно предположить, что формула $\exists v\,(A_1 \wedge \ldots \wedge A_n)$ имеет вид

$$\exists v\, \left(\bigwedge_{j=1}^{l} (u_j < v) \wedge \bigwedge_{k=1}^{m} (v < w_k) \right).$$

Если $l = 0$ или $m = 0$, то заменим формулу $\exists v\,(A_1 \wedge \ldots \wedge A_n)$ на бескванторную формулу $\top$. Если $l > 0$ и $m > 0$, то заменим формулу

$$\exists v\,\left(\bigwedge_j (u_j < v) \wedge \bigwedge_k (v < w_k)\right)$$

на бескванторную формулу

$$\bigwedge_j \bigwedge_k (u_j < w_k).$$

□

Пример 8.12. $\exists x\,(x < y_1 \wedge y_3 < x \wedge y_2 < y_5) \sim y_2 < y_5 \wedge \exists x\,(x < y_1 \wedge y_3 < x)$.

Пример 8.13. Формулы $\exists x\,(x < x \wedge y_1 < y_2)$ и $\perp$ равносильны в $\mathfrak{Q}$.

Пример 8.14. Формулы $\exists x\, x = x$ и $\top$ равносильны в $\mathfrak{Q}$.

Пример 8.15. Формулы $\exists x\,(x = x \wedge x < y_2)$ и $\exists x\,(x < y_2)$ равносильны в $\mathfrak{Q}$.

Пример 8.16. Формулы

$$\exists x\,(x < y_1 \wedge x = y_2 \wedge y_3 < x \wedge x = y_4)$$

и

$$y_4 < y_1 \wedge y_4 = y_2 \wedge y_3 < y_4$$

равносильны в $\mathfrak{Q}$.

Пример 8.17. Формулы $\exists x\,(y_1 < x \wedge y_2 < x)$ и $\top$ равносильны в $\mathfrak{Q}$.

Пример 8.18. Формулы

$$\exists x\,(y_1 < x \wedge y_2 < x \wedge x < y_3 \wedge x < y_4)$$

и

$$y_1 < y_3 \wedge y_1 < y_4 \wedge y_2 < y_3 \wedge y_2 < y_4$$

равносильны в $\mathfrak{Q}$.

Лемма 8.19. *Пусть C — бескванторная формула сигнатуры упорядоченных множеств. Тогда формула $\exists v\, C$ равносильна в $\mathfrak{Q}$ некоторой бескванторной формуле B, удовлетворяющей условию $\mathrm{FV}(B) \subseteq \mathrm{FV}(\exists v\, C)$.*

Доказательство. Приведём формулу C к дизъюнктивной нормальной форме (то есть к дизъюнкции конъюнкций атомарных формул и отрицаний атомарных формул). Затем заменим подформулы вида $\neg(u_1 = u_2)$ на $u_1 < u_2 \vee u_2 < u_1$ и подформулы вида $\neg(u_1 < u_2)$ на $u_1 = u_2 \vee u_2 < u_1$. Полученную формулу приведём снова к дизъюнктивной нормальной форме (используя только ассоциативность и дистрибутивность). Легко понять, что она имеет вид $K_1 \vee \ldots \vee K_m$, где $K_1, \ldots, K_m$ — конъюнкции атомарных формул. Согласно теореме 3.86

$$\exists v\,(K_1 \vee \ldots \vee K_m) \sim \exists v\, K_1 \vee \ldots \vee \exists v\, K_m.$$

Осталось применить лемму 8.11 к каждой из формул $\exists v\, K_i$. □

Пример 8.20. Следующие формулы равносильны в $\mathfrak{Q}$:

$$\begin{aligned}
&\exists x\,(x < y \wedge \neg(x < z)),\\
&\exists x\,(x < y \wedge (x = z \vee z < x)),\\
&\exists x\,(x < y \wedge x = z \vee x < y \wedge z < x)),\\
&\exists x\,(x < y \wedge x = z) \vee \exists x\,(x < y \wedge z < x)),\\
&z < y \vee z < y,\\
&z < y.
\end{aligned}$$

Доказательство теоремы 8.9. Без ограничения общности можно предположить, что формула A не содержит квантора всеобщности (так как $\forall v\, C \sim \neg\exists v\, \neg C$). Докажем теорему индукцией по числу кванторов в формуле A. Если это число равно нулю, то в качестве формулы B подходит сама формула A. Иначе рассмотрим самую короткую подформулу вида $\exists v\, C$ в формуле A. Очевидно, C — бескванторная формула. Заменим в формуле A рассматриваемую подформулу на эквивалентную бескванторную формулу (которая существует в силу леммы 8.19) и применим предположение индукции. □

Теорема 8.21. *Пусть A — некоторая формула сигнатуры упорядоченных множеств. Тогда существует бескванторная формула B той же сигнатуры, такая что $\mathrm{FV}(B) \subseteq \mathrm{FV}(A)$ и формулы A и B равносильны в каждом плотном линейно упорядоченном множестве без первого и последнего элемента.*

Доказательство. Бескванторная формула B, построенная в доказательстве теоремы 8.9, равносильна исходной формуле A не только в стандартной интерпретации на множестве $\mathbb{Q}$, но и во всех остальных плотных линейно упорядоченных множествах без первого и последнего элемента. □

8.4 Элементарная эквивалентность

[УВП, 2.13], **[ВШ2, 3.9]**, [Bil, 9]

Определение 8.22. Пусть $\mathfrak{L}$ и $\mathfrak{M}$ — интерпретации сигнатуры Ω. Говорят, что $\mathfrak{L}$ и $\mathfrak{M}$ *элементарно эквивалентны* (обозначение $\mathfrak{L} \cong \mathfrak{M}$), если для любой замкнутой формулы A сигнатуры Ω имеет место равенство $[A]^{\mathfrak{L}} = [A]^{\mathfrak{M}}$.

(УВП, с. 47.)

(ВШ2, с. 135.)

Упражнение 8.23. Верно ли, что интерпретации $\langle \mathbb{N}, < \rangle$ и $\langle \mathbb{Z}, < \rangle$ элементарно эквивалентны?

Ответ 8.23. Нет. Формула $\forall x\, \exists y\, (y < x)$ ложна в первой интерпретации, но истинна во второй.

Упражнение 8.24. Верно ли, что интерпретации $\langle \mathbb{Z}, +, = \rangle$ и $\langle \mathbb{Q}, +, = \rangle$ элементарно эквивалентны?

Ответ 8.24. Нет. Формула $\forall x\, \exists y\, (y + y = x)$ ложна в первой интерпретации, но истинна во второй.

Теорема 8.25. *Отношение $\cong$ рефлексивно, симметрично и транзитивно.*

Доказательство. Теорема непосредственно следует из определения элементарной эквивалентности. □

8.5 Элементарная эквивалентность всех плотных линейно упорядоченных множеств без первого и последнего элемента

[ВШ2, 3.6]

Теорема 8.26. *Все плотные линейно упорядоченные множества без первого и последнего элемента элементарно эквивалентны.*

(ВШ2, с. 114–115.)

Доказательство. Рассмотрим две интерпретации $\mathfrak{L}$ и $\mathfrak{M}$ сигнатуры упорядоченных множеств, представляющие собой плотные линейно упорядоченные множества без первого и последнего элемента. Рассмотрим произвольную замкнутую формулу A сигнатуры упорядоченных множеств. Применив теорему 8.21 к формуле A, получим бескванторную формулу B со следующими свойствами:

1) $\mathrm{FV}(B) = \varnothing$,
2) $[A]^{\mathfrak{L}} = [B]^{\mathfrak{L}}$,
3) $[A]^{\mathfrak{M}} = [B]^{\mathfrak{M}}$.

Так как формула B не содержит ни свободных, ни связанных вхождений переменных, то она не содержит ни одной атомарной формулы (то есть формула B составлена из пропозициональных связок $\perp$, $\top$, $\neg$, $\wedge$, $\vee$, $\to$ и скобок). Поэтому $[B]^{\mathfrak{L}} = [B]^{\mathfrak{M}}$. Следовательно, $[A]^{\mathfrak{L}} = [A]^{\mathfrak{M}}$, что и требовалось доказать. □

Замечание 8.27. Элементарная теория стандартной интерпретации сигнатуры $\langle =, < \rangle$ на $\mathbb{R}$ совпадает с элементарной теорией стандартной интерпретации сигнатуры $\langle =, < \rangle$ на $\mathbb{Q}$.

Упражнение 8.28. Являются ли элементарно эквивалентными линейно упорядоченные множества $[2;3]$ и $[2;3] \cup [4;5]$?

Ответ 8.28. Нет.

Упражнение 8.29. Являются ли элементарно эквивалентными линейно упорядоченные множества $(2;3)$ и $(2;3) \cup (4;5)$?

Ответ 8.29. Да.

8.6 Разрешимые теории первого порядка

[ВШ2, 5.3, 5.4], [КД, с. 106–110, 182–183], [Мен, с. 107], [ЛМ, II.5]

Определение 8.30. Теория первого порядка называется *разрешимой*, если множество её теорем разрешимо.

(ВШ2, с. 212.)

Теорема 8.31. *Полная разрешимо аксиоматизируемая теория разрешима.*

(ВШ2, теорема 67, с. 214.)

(УВП, теорема 17, с. 109.)

Доказательство. Рассмотрим разрешимо аксиоматизируемую теорию T. Согласно теореме 7.33 множество теорем теории T перечислимо. Так как теория T полна, то формула A не является теоремой теории T тогда и только тогда, когда формула A не замкнута или формула $\neg A$ является теоремой теории T. Следовательно, дополнение множества теорем теории T тоже перечислимо. Осталось применить теорему 6.72. □

Определение 8.32. Теория с сигнатурой $\langle = \rangle$ и аксиомами

1) $\forall x\, (x = x)$,

2) $\forall x\, \forall y\, (x = y \to y = x)$,

3) $\forall x \forall y \forall z\,(x = y \land y = z \to x = z)$

называется *теорией равенства*.

Теорема 8.33. *Теория равенства разрешима.*

(ВШ2, теорема 68, с. 226.)

Теорема 8.34 (о теории одноместных предикатов). *Пусть сигнатура Ω не содержит ни одного функционального символа, содержит лишь конечное число предикатных символов и все они одноместные. Тогда множество общезначимых замкнутых формул сигнатуры Ω разрешимо.*

(КД, с. 183.)

(ЛМ, Упражнение II.5.40.)

8.7 Разрешимость элементарной теории плотных линейно упорядоченных множеств без первого и последнего элемента

[ВШ2, 5.3], [КД, с. 108]

Теорема 8.35. *Элементарная теория плотных линейно упорядоченных множеств без первого и последнего элемента разрешима.*

(ВШ2, с. 215.)

Доказательство. Рассмотрим произвольную замкнутую формулу A сигнатуры упорядоченных множеств. Применив теорему 8.21 к формуле A, получим замкнутую бескванторную формулу B, эквивалентную формуле A во всех моделях теории плотных линейно упорядоченных множеств без первого и последнего элемента. Так как формула B не содержит ни свободных, ни связанных вхождений переменных, то она не содержит ни одной атомарной формулы (то есть формула B составлена из пропозициональных связок $\bot$, $\top$, $\neg$, $\land$, $\lor$, $\to$ и скобок). Такая формула равносильна либо формуле $\bot$, либо формуле $\top$, и по формуле легко вычислить, какой из этих случаев имеет место. Так как доказательство теоремы 8.21 конструктивно, то приведённые рассуждения дают алгоритм, выясняющий, истинна ли замкнутая формула A во всех моделях рассматриваемой теории. □

Теорема 8.36. *Элементарная теория плотных линейно упорядоченных множеств разрешима.*

Доказательство. Множество теорем этой теории является пересечением множеств теорем следующих четырёх теории:

1) элементарная теория плотных линейно упорядоченных множеств без первого и последнего элемента,
2) элементарная теория плотных линейно упорядоченных множеств с первым элементом, но без последнего элемента,
3) элементарная теория плотных линейно упорядоченных множеств с последним элементом, но без первого элемента,
4) элементарная теория плотных линейно упорядоченных множеств с первым и последним элементом.

Разрешимость первой теории доказана в теореме 8.35. Разрешимость остальных трёх теорий доказывается аналогично, но перед элиминацией кванторов надо добавить в сигнатуру константу для первого элемента (для второй и четвёртой теории) и константу для последнего элемента (для третьей и четвёртой теории). □

8.8 Неразрешимость множества арифметических истин

[К1, с. 19], [П2, 26, 27], [БДж, с. 234–235]

Теорема 8.37. *Элементарная теория стандартной интерпретации языка арифметики неразрешима.*

Доказательство. Эта теорема непосредственно следует из теоремы 7.31. □

8.9 Неразрешимость арифметики Пеано (без доказательства)

[КД, с. 205–207], [БДж, 14–15]

Теорема 8.38 (без доказательства). *Арифметика Пеано неразрешима.*

Теорема 8.39 (без доказательства). *Существует неразрешимая, конечно аксиоматизируемая теория в сигнатуре формальной арифметики.*

(БДж, с. 234.)

Доказательство. Этими свойствами обладает теория с аксиомами

1) $\forall x\,(x = x)$,
2) $\forall x\,\forall y\,(x = y \to y = x)$,
3) $\forall x\,\forall y\,\forall z\,(x = y \wedge y = z \to x = z)$,
4) $\forall x\,\forall y\,(x = y \to S(x) = S(y))$,
5) $\forall x\,\forall y\,(S(x) = S(y) \to x = y)$,
6) $\forall x\,\neg(S(x) = 0)$,
7) $\forall x\,(x + 0 = x)$,
8) $\forall x\,\forall y\,(x + S(y) = S(x + y))$,
9) $\forall x\,(x \cdot 0 = 0)$,
10) $\forall x\,\forall y\,(x \cdot S(y) = (x \cdot y) + x)$,
11) $\forall x\,(\neg\,(x = 0) \to \exists y\,(x = S(y)))$.

(БДж, с. 214.) □

8.10 Неразрешимость теории полугрупп (без доказательства)

Теорема 8.40 (без доказательства). *Теория полугрупп неразрешима.*

(ВШ2, теорема 69, с. 228.)

8.11 Теорема Чёрча

[КД, с. 102–103, 205–207], [БДж, с. 145, 234–235]

Определение 8.41. Обозначим через Э алфавит

$$\{\forall, \exists, \neg, \wedge, \vee, \rightarrow, x, f, P, \mathbf{1}, \mathbf{(}, \mathbf{)}, \mathbf{,}\}.$$

Каждую формулу сигнатуры со счётным числом функциональных и предикатных символов каждой арности отождествим словом в алфавите Э, полученным заменой индивидных переменных x_i на выражения $x\mathbf{1}^i$, функциональных символов f_i^j (арности j) на выражения $f\mathbf{1}^i$ и предикатных символов P_i^j (арности j) на выражения $P\mathbf{1}^i$.

Теорема 8.42 (теорема Чёрча). *Множество общезначимых формул сигнатуры со счётным числом функциональных и предикатных символов каждой арности неразрешимо.*

(КД, с. 102–103.)

(ВШ2, с. 201.)

Доказательство. Достаточно доказать, что существует неразрешимая, конечно аксиоматизируемая теория в конечной сигнатуре. Это следует, например, из теоремы 8.39 или теоремы 8.40. □

Замечание 8.43. Множество общезначимых формул сигнатуры со счётным числом функциональных и предикатных символов каждой арности перечислимо.

8.12 Языки второго порядка

[БДж, 18], [Мал, 13.4], [КД, с. 79–80]

Определение 8.44. Каждый *язык второго порядка* задаётся своей сигнатурой $\Omega = \langle \mathrm{Fn}, \mathrm{Pr} \rangle$, где Fn — множество *функциональных символов* и Pr — множество *предикатных символов*.

Определение 8.45. В языках второго порядка помимо индивидных переменных используются *функциональные переменные* и *предикатные переменные*. С каждой функциональной и предикатной переменной связано некоторое натуральное число — количество аргументов (или *валентность*) этой переменной. Валентность может быть нулевой. Во всяком языке второго порядка имеется счётный набор функциональных переменных каждой валентности и счётный набор предикатных переменных каждой валентности.

Определение 8.46 (терм второго порядка сигнатуры Ω).

1. Если v — индивидная переменная, то v — терм второго порядка сигнатуры Ω.
2. Если c — нульместный функциональный символ или нульместная предикатная переменная сигнатуры Ω, то c — терм второго порядка сигнатуры Ω.
3. Если f — n-местный функциональный символ или n-местная функциональная переменная сигнатуры Ω, где $n > 0$, и $t_1, \ldots, t_n$ — термы второго порядка сигнатуры Ω, то $f(t_1, \ldots, t_n)$ — терм второго порядка сигнатуры Ω.

Определение 8.47 (атомарная формула второго порядка сигнатуры Ω).

1. Если P — нульместный предикатный символ или нульместная предикатная переменная сигнатуры Ω, то P — атомарная формула второго порядка сигнатуры Ω.
2. Если P — n-местный предикатный символ или n-местная предикатная переменная сигнатуры Ω, где $n > 0$, и $t_1, \ldots, t_n$ — термы второго порядка сигнатуры Ω, то $P(t_1, \ldots, t_n)$ — атомарная формула второго порядка сигнатуры Ω.

Определение 8.48 (формула второго порядка сигнатуры Ω).

1. Если A — атомарная формула второго порядка сигнатуры Ω, то A — формула второго порядка сигнатуры Ω.
2. Если A — формула второго порядка сигнатуры Ω, то $\neg A$ — формула второго порядка сигнатуры Ω.
3. Если A и B — формулы второго порядка сигнатуры Ω, то $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ — формулы второго порядка сигнатуры Ω.
4. Если A — формула второго порядка сигнатуры Ω, а v — индивидная, функциональная или предикатная переменная, то $\forall v\, A$ и $\exists v\, A$ — формулы второго порядка сигнатуры Ω.

Замечание 8.49. Каждая формула первого порядка сигнатуры Ω является также формулой второго порядка сигнатуры Ω.

Замечание 8.50. Понятие подстановки вместо свободных вхождений переменной распространяются на функциональные и предикатные переменные естественным образом.

Определение 8.51. При интерпретации языка второго порядка требуется добавить в сигнатуру $\boldsymbol{\Omega(M)}$ новый функциональный символ $\underline{\boldsymbol{f}}$ для каждой функций $\boldsymbol{f}\colon M^n \to M$ и новый предикатный символ $\underline{\boldsymbol{P}}$ для каждого предиката $\boldsymbol{P}\colon M^n \to \{\text{И}, \text{Л}\}$. В определение истинностного значения замкнутой формулы добавляются следующие пункты.

9. Если g — n-местная функциональная переменная, то $[\exists g\, A]^{\mathfrak{M}} = \text{И}$ тогда и только тогда, когда найдётся такая функция $\boldsymbol{f}\colon M^n \to M$, что $[A[\underline{\boldsymbol{f}}/g]]^{\mathfrak{M}} = \text{И}$. Аналогично для $\forall g$.
10. Если Q — n-местная предикатная переменная, то $[\exists Q\, A]^{\mathfrak{M}} = \text{И}$ тогда и только тогда, когда найдётся такой предикат $\boldsymbol{P}\colon M^n \to \{\text{И}, \text{Л}\}$, что $[A[\underline{\boldsymbol{P}}/Q]]^{\mathfrak{M}} = \text{И}$. Аналогично для $\forall Q$.

Замечание 8.52. Понятия замкнутой формулы, модели и логического следствия распространяются на логику второго порядка естественным образом.

Определение 8.53. *Теорией второго порядка* в сигнатуре Ω называется произвольное множество замкнутых формул второго порядка сигнатуры Ω. Элементы этого множества называются *аксиомами* этой теории. *Теоремами* этой теории называются замкнутые формул второго порядка сигнатуры Ω, являющиеся логическими следствиями аксиом данной теории.

8.13 Невозможность распространения теоремы компактности на языки второго порядка

[БДж, 18], [Мал, 13.4], [КД, с. 79–80]

Теорема 8.54 (формула Лейбница). *Существует формула второго порядка, выражающая в любой интерпретации любой сигнатуры предикат равенства.*

(БДж, пример 18.1, с. 265.)

Доказательство. Проверим, что подходит формула $\forall Q\,(Q(x) \to Q(y))$, где Q — одноместная предикатная переменная. Рассмотрим произвольную интерпретацию $\mathfrak{M} = \langle M, \Omega \rangle$. Надо доказать, что для любых $a_1, a_2 \in M$ следующие два условия равносильны:

1) элементы a_1 и a_2 совпадают,
2) $[\forall Q\,(Q(x) \to Q(y))[\,\underline{a_1}\,/x][\,\underline{a_2}\,/y]]^{\mathfrak{M}} = \text{И}$.

Очевидно, $\forall Q\,(Q(x) \to Q(y))[\,\underline{a_1}\,/x][\,\underline{a_2}\,/y]$ является обозначением формулы $\forall Q\,(Q(\,\underline{a_1}\,) \to Q(\,\underline{a_2}\,))$. Если a_1 и a_2 совпадают, то формулы $Q(\,\underline{a_1}\,)$ и $Q(\,\underline{a_2}\,)$ совпадают и, следовательно, формула $\forall Q\,(Q(\,\underline{a_1}\,) \to Q(\,\underline{a_2}\,))$ истинна в интерпретации $\mathfrak{M}$.

Пусть теперь a_1 и a_2 не совпадают. Рассмотрим одноместный предикат $\boldsymbol{P}\colon M \to \{\text{И}, \text{Л}\}$, заданный так:

$$\boldsymbol{P}(b) = \begin{cases} \text{И}, & \text{если } b \text{ совпадает с } a_1, \\ \text{Л} & \text{иначе.} \end{cases}$$

Очевидно, формула $\underline{\boldsymbol{P}}\,(\,\underline{a_1}\,)$ истинна, а формула $\underline{\boldsymbol{P}}\,(\,\underline{a_2}\,)$ ложна в интерпретации $\mathfrak{M}$. Следовательно, формула $\underline{\boldsymbol{P}}\,(\,\underline{a_1}\,) \to \underline{\boldsymbol{P}}\,(\,\underline{a_2}\,)$ ложна в этой интерпретации. Согласно определению 8.51 формула $\forall Q\,(Q(\,\underline{a_1}\,) \to Q(\,\underline{a_2}\,))$ также ложна в интерпретации $\mathfrak{M}$. $\square$

Теорема 8.55. *Существует замкнутая формула A второго порядка пустой сигнатуры, истинная во всех конечных интерпретациях и ложная во всех бесконечных интерпретациях.*

(БДж, упражнение 18.3, с. 272.)

Доказательство. В сигнатуре с равенством конечность интерпретации можно выразить формулой

$$\forall g\,(\forall x\,\forall y\,(g(x) = g(y) \to x = y) \to \forall z\,\exists x\,g(x) = z),$$

где g — одноместная функциональная переменная. Эта формула утверждает, что каждая инъекция на носителе интерпретации является сюръекцией. Выразив равенство с помощью формулы из теоремы 8.54, получим искомую формулу A. $\square$

Теорема 8.56 (о невозможности распространения теоремы компактности на логику второго порядка). *Существует счётное множество Γ, состоящее из замкнутых формул второго порядка и обладающее следующими свойствами:*

1) *каждое конечное подмножество множества Γ имеет модель,*
2) *множество Γ не имеет модели.*

(БДж, следствие 18.3, с. 271.)

Доказательство. Рассмотрим множество $\Gamma = \{G_m \mid m \geqslant 2\} \cup \{A\}$, где

$$G_m = \neg\exists x_1 \ldots \exists x_{m-1}\,\forall y\,(x_1 = y \vee \ldots \vee x_{m-1} = y),$$

а формула A взята из теоремы 8.55.

Если выразить равенство с помощью формулы из теоремы 8.54, то получим счётное множество формул пустой сигнатуры. $\square$

8.14 Арифметика второго порядка

[БДж, 18], [Мал, 13.4], [КД, с. 80, 109, 126]

Определение 8.57. *Арифметикой второго порядка* называется теория второго порядка с сигнатурой $\langle 0, S, +, \cdot, = \rangle$ и аксиомами

1) $\forall x\,(x = x)$,
2) $\forall x\,\forall y\,(x = y \to y = x)$,
3) $\forall x\,\forall y\,\forall z\,(x = y \wedge y = z \to x = z)$,
4) $\forall x\,\forall y\,(x = y \to S(x) = S(y))$,
5) $\forall x\,\forall y\,(S(x) = S(y) \to x = y)$,
6) $\forall x\,\neg(S(x) = 0)$,
7) $\forall x\,(x + 0 = x)$,
8) $\forall x\,\forall y\,(x + S(y) = S(x + y))$,
9) $\forall x\,(x \cdot 0 = 0)$,
10) $\forall x\,\forall y\,(x \cdot S(y) = (x \cdot y) + x)$,
11) $\forall Q\,(Q(0) \wedge \forall x\,(Q(x) \to Q(S(x))) \to \forall x\,Q(x))$, где Q — одноместная предикатная переменная.

Теорема 8.58. *Рассмотрим теорию в сигнатуре* $\langle 0, S, = \rangle$ *с аксиомами* 1)–6), 11) *из определения 8.57. Все нормальные модели этой теории изоморфны друг другу.*

Доказательство. Обозначим через $\mathfrak{N}_0$ интерпретацию с носителем $\mathbb{N}$, где значением константы 0 является число нуль, значением функционального символа S является функция, прибавляющая единицу, и предикатный символ $=$ интерпретируется как совпадение аргументов. Рассмотрим любую модель той же теории. Обозначим эту модель через $\mathfrak{M}$, а её носитель через M. Достаточно установить, что интерпретации $\mathfrak{N}_0$ и $\mathfrak{M}$ изоморфны. Для этого докажем, что функция $\varphi\colon \mathbb{N} \to M$, заданная равенством $\varphi(m) = [\overline{m}]^{\mathfrak{M}}$, является изоморфизмом из $\mathfrak{N}_0$ в $\mathfrak{M}$. (Здесь используется обозначение из определения 7.4.)

Обозначим множество значений функции φ через P, а соответствующий ему предикат через $\boldsymbol{P}$. Если подставить имя этого предиката вместо предикатной переменной Q в формулу $Q(0) \wedge \forall x\,(Q(x) \to Q(S(x))) \to \forall x\,Q(x)$, получим формулу $\boldsymbol{P}(0) \wedge \forall x\,(\boldsymbol{P}(x) \to \boldsymbol{P}(S(x))) \to \forall x\,\boldsymbol{P}(x)$, истинную в $\mathfrak{M}$, так как аксиома 11) из определения 8.57 истинна в $\mathfrak{M}$. Очевидно, $\boldsymbol{P}(0)$ и $\forall x\,(\boldsymbol{P}(x) \to \boldsymbol{P}(S(x)))$ истинны в $\mathfrak{M}$. Следовательно, и формула $\forall x\,\boldsymbol{P}(x)$ истинна в $\mathfrak{M}$. Отсюда получаем, что $P = M$, то есть функция φ является сюръекцией.

Докажем теперь инъективность функции φ. Пусть $k \in \mathbb{N}$, $l \in \mathbb{N}$ и $k \neq l$. Без ограничения общности можно считать, что $k > l$. Формула $\neg(\overline{k - l} = 0)$ является логическим следствием шестой аксиомы. Используя пятую аксиому l раз, получим, что формула $\neg(\overline{k} = \overline{l})$ является теоремой рассматриваемой теории. Следовательно, $[\overline{k}]^{\mathfrak{M}}$ и $[\overline{l}]^{\mathfrak{M}}$ не совпадают. Мы установили, что функция φ является инъекцией.

Так как $\varphi(0) = 0^{\mathfrak{M}}$, то φ сохраняет функциональный символ 0. Чтобы доказать, что φ сохраняет функциональный символ S, необходимо проверить равенство $\varphi(k+1) = S^{\mathfrak{M}}(\varphi(k))$ для любого $k \in \mathbb{N}$. Это равенство непосредственно следует из того, что $\varphi(m) = \underbrace{S^{\mathfrak{M}}(\ldots S^{\mathfrak{M}}(}_{m \text{ раз}} 0^{\mathfrak{M}}) \ldots)$ для любого $m \in \mathbb{N}$.

Осталось проверить, что функция φ сохраняет предикатный символ $=$. Это означает, что для любых $k, l \in \mathbb{N}$ следующие два условия равносильны:

1) $k = l$,

2) формула $\overline{k} = \overline{l}$ истинна в $\mathfrak{M}$.

Очевидно, формула $\overline{k} = \overline{k}$ истинна при любом $k \in \mathbb{N}$. Если $k \neq l$, то формула $\overline{k} = \overline{l}$ ложна в $\mathfrak{M}$, так как формула $\neg(\overline{k} = \overline{l})$ является теоремой рассматриваемой теории. $\square$

Теорема 8.59. *Все нормальные модели теории из определения 8.57 изоморфны стандартной интерпретации языка арифметики.*

(БДж, теорема 18.1, с. 268.)

Доказательство. Рассмотрим любую модель этой теории. Обозначим эту модель через $\mathfrak{M}$, а её носитель через M. Докажем, что функция $\varphi\colon \mathbb{N} \to M$ из доказательства теоремы 8.58 является изоморфизмом из стандартной интерпретации $\mathfrak{N}$ в интерпретацию $\mathfrak{M}$. Для этого необходимо лишь проверить, что φ сохраняет функциональные символы $+$ и $\cdot$. Достаточно убедиться, что для любых $k, l \in \mathbb{N}$ формулы $\overline{k} + \overline{l} = \overline{k+l}$ и $\overline{k} \cdot \overline{l} = \overline{k \cdot l}$ являются теоремами рассматриваемой теории. Это легко доказать индукцией по l. $\square$

Замечание 8.60. Если добавить к арифметике второго порядка аксиому $\forall x\, \forall y\, (x = y \leftrightarrow \forall Q\, (Q(x) \to Q(y))$, то в теореме 8.59 можно отбросить условие нормальности.

Главы учебников по темам курса

Логика высказываний

- [ВШ2, 1.1–1.2]
- [УВП, 2.1–2.3]
- [П1, 2.1–2.11, 3.1–3.2]
- [ЛМ, II.1–II.2]

Логика предикатов

- [П1, 5.4–5.10]
- [УВП, 2.1, 2.4–2.12, 3.1–3.3, 3.7]
- [ВШ2, 3.1–3.4, 3.9, 4.1, 4.2, 4.6, 4.7, 5.1, 5.3]
- [Кли, 16–20]
- [ЛМ, II.4–II.5]

Исчисление высказываний

- [ВШ2, 2.1–2.3]
- [П1, 4.1–4.2]

Исчисление предикатов

- [П1, 6.1–6.4]
- [ВШ2, 4.2–4.7]
- [УВП, 3.4–3.6, 4.1–4.6]

Теория алгоритмов и арифметика

- [К1, 1–7]
- [П2, 1–14, 24–27]
- [УВП, 5.1–5.9]
- [ВШ3, 1.1–4.4, 9.1–9.3, 10.1–10.3, 10.5]
- [ЛМ, II.7, III.1–III.3]
- [Мен, 3.1–3.6]
- [БДж, 14–15, 17]

Приложения и обобщения

- [УВП, 2.13]
- [ВШ2, 3.6, 5.3]
- [БДж, 18]

Рекомендуемая литература

[БДж] *Булос Дж., Джеффри Р.* Вычислимость и логика. — М.: Мир, 1994. — 396 с.

[ВШ2] *Верещагин Н. К., Шень А.* Лекции по математической логике и теории алгоритмов. Часть 2. Языки и исчисления. — М.: МЦНМО, 2000. — 288 с.

[ВШ3] *Верещагин Н. К., Шень А.* Лекции по математической логике и теории алгоритмов. Часть 3. Вычислимые функции. — М.: МЦНМО, 1999. — 176 с.

[Кли] *Клини С. К.* Математическая логика. — М.: Мир, 1973. — 480 с.

[КД] *Колмогоров А. Н., Драгалин А. Г.* Математическая логика. — М.: УРСС, 2004. — 240 с.

[ЛМ] *Лавров И. А., Максимова Л. Л.* Задачи по теории множеств, математической логике и теории алгоритмов. — 3-е изд. — М.: Физматлит, 1995. — 256 с.

[Мен] *Мендельсон Э.* Введение в математическую логику. — М.: Наука, 1971. — 320 с.

[УВП] *Успенский В. А., Верещагин Н. К., Плиско В. Е.* Вводный курс математической логики. 2-е изд. — М.: Физматлит, 2002. — 128 с.

Конспекты из Интернета

[K1] *Крупский В. Н.* Лекции по теории алгоритмов для первого курса мехмата (2004). — 20 с. —
`http://lpcs.math.msu.su/~krupski/download/mm1/lect_kru.pdf`
`http://lpcs.math.msu.su/~krupski/download/mm1/lect_kru.ps`

[K2] *Крупский В. Н.* Подборка задач по теории алгоритмов. — 7 с. —
`http://lpcs.math.msu.su/~krupski/download/mm1/zad_alg.pdf`
`http://lpcs.math.msu.su/~krupski/download/mm1/zad_alg.ps`

[П1] *Плиско В. Е.* Математическая логика: Курс лекций. — 86 с. —
`http://lpcs.math.msu.su/~plisko/matlog.pdf`
`http://lpcs.math.msu.su/~plisko/matlog.ps`

[П2] *Плиско В. Е.* Теория алгоритмов: Курс лекций. — 38 с. —
`http://lpcs.math.msu.su/~plisko/ta.pdf`
`http://lpcs.math.msu.su/~plisko/ta.ps`

[Bil] *Bilaniuk S.* A Problem Course in Mathematical Logic. — 2003. — XII, 152 p. — `http://www.trentu.ca/mathematics/sb/pcml/`

Дополнительная литература

[Гин] *Гиндикин С. Г.* Алгебра логики в задачах. — М.: Наука, 1972. — 288 с.

[Гла] *Гладкий А. В.* Математическая логика. — М.: РГГУ, 1998. — 479 с.

[ЕП] *Ершов Ю. Л., Палютин Е. А.* Математическая логика. — 2-е изд., испр. и доп. — М.: Наука. Гл. ред. физ.-мат. лит., 1987. — 336 с.

[ЛПИ] Логический подход к искусственному интеллекту: От модальной логики к логике баз данных / Тейз А., Грибомон П., Юлен Г. и др. — М.: Мир, 1998. — 494 с.

[Мал] *Мальцев А. И.* Алгоритмы и рекурсивные функции. — 2-е изд. — М.: Наука, 1986. — 368 с.

[Сто] *Столл Р.* Множества, логика, аксиоматические теории. — М.: Просвещение, 1968. — 231 с.

[Фейс] *Фейс Р.* Модальная логика. — М.: Наука, 1974. — 520 с.

[ЧЛ] *Чень Ч., Ли Р.* Математическая логика и автоматическое доказательство теорем. — М.: Наука, 1983. — 360 с.

[Шён] *Шёнфилд Дж.* Математическая логика. — М.: Наука, 1975. — 528 с.

Оглавление