

**Петрова Л.П.**

**Конспект лекций с упражнениями по дисциплине  
Дискретная математика, математическая логика  
и их приложения в компьютерных науках**

**для студентов 1 курса математического факультета ВГУ  
специальности 010200 «Математика и компьютерные науки**

**2015 г.**

## Оглавление

|                                                                                          |             |
|------------------------------------------------------------------------------------------|-------------|
| <b>1. Логика высказываний .....</b>                                                      | <b>(4)</b>  |
| <b>1.1. Определение логического следствия .....</b>                                      | <b>(4)</b>  |
| 1.1.1. Определение высказывания и предиката .....                                        | (4)         |
| 1.1.2. Определение умозаключения, посылок и заключения .....                             | (4)         |
| 1.1.3. Определение интерпретации и контрпримера .....                                    | (4)         |
| 1.1.4. Определение логического следствия и следствия в теории .....                      | (5)         |
| 1.1.5. Упражнение .....                                                                  | (5)         |
| <b>1.2. Язык логики высказываний .....</b>                                               | <b>(6)</b>  |
| 1.2.1. Логические связки.....                                                            | (6)         |
| 1.2.2. Формулы логики высказываний .....                                                 | (6)         |
| 1.2.3. Упражнение .....                                                                  | (7)         |
| 1.2.4. Формализация в логике высказываний.....                                           | (7)         |
| 1.2.5. Упражнение .....                                                                  | (8)         |
| 1.2.6. Формализация необходимых и достаточных условий.....                               | (8)         |
| 1.2.7. Упражнение .....                                                                  | (8)         |
| <b>1.3. Следствие в логике высказываний .....</b>                                        | <b>(9)</b>  |
| 1.3.1. Стандартные интерпретации.....                                                    | (9)         |
| 1.3.2. Таблицы истинности.....                                                           | (9)         |
| 1.3.3. Упражнение.....                                                                   | (10)        |
| 1.3.4. Таблицы истинности и логическое следствие .....                                   | (10)        |
| 1.3.5. Направленная табличная процедура .....                                            | (10)        |
| 1.3.6. Примеры доказательств направленной процедурой .....                               | (11)        |
| 1.3.7. Примеры доказательств с разветвлением.....                                        | (11)        |
| 1.3.8. Упражнение .....                                                                  | (12)        |
| 1.3.9. Упражнение .....                                                                  | (12)        |
| 1.3.10. Определение логической эквивалентности, тавтологии и противоречия .....          | (13)        |
| 1.3.11. Упражнение .....                                                                 | (13)        |
| 1.3.12. Упражнение .....                                                                 | (13)        |
| 1.3.13. Упражнение.....                                                                  | (13)        |
| 1.3.14. Свойства логического следствия, эквивалентности, тавтологии и противоречия ..... | (14)        |
| 1.3.15. Упражнение.....                                                                  | (14)        |
| <b>1.4. Основные теоремы логики высказываний .....</b>                                   | <b>(14)</b> |
| 1.4.1. Теорема об отрицании, конъюнкции и дизъюнкции.....                                | (14)        |
| 1.4.2. Теорема об импликации и двойной импликации .....                                  | (15)        |
| 1.4.3. Упражнение.....                                                                   | (15)        |
| 1.4.4. Замечания об истории, терминологии и обозначениях .....                           | (15)        |
| 1.4.5. Упражнение.....                                                                   | (16)        |
| 1.4.6. Упражнение.....                                                                   | (16)        |
| <b>1.5. Принцип двойственности .....</b>                                                 | <b>(17)</b> |
| 1.5.1. Определение дополнительных логических связей.....                                 | (18)        |
| 1.5.2. Упражнение.....                                                                   | (18)        |
| 1.5.3. Упражнение.....                                                                   | (18)        |
| 1.5.4. Упражнение.....                                                                   | (20)        |
| 1.5.5. Упражнение.....                                                                   | (20)        |
| 1.5.6. Упражнение.....                                                                   | (20)        |
| 1.5.7. Упражнение.....                                                                   | (21)        |
| 1.5.8. Упражнение.....                                                                   | (21)        |
| <b>1.6. Разложение булевых функций по переменным. Совершенные.....</b>                   | <b>(21)</b> |
| <b>дизъюнктивная и конъюнктивная формы .....</b>                                         | <b>(21)</b> |

|                                                                       |             |
|-----------------------------------------------------------------------|-------------|
| 1.6.1. Упражнение.....                                                | (25)        |
| <b>1.7. Полнота и замкнутость систем булевых функций.....</b>         | <b>(26)</b> |
| 1.7.1. Основные определения и свойства.....                           | (26)        |
| 1.7.2. Упражнение.....                                                | (27)        |
| 1.7.3. Полином Жегалкина.....                                         | (27)        |
| 1.7.4. Упражнение.....                                                | (28)        |
| 1.7.5. Упражнение.....                                                | (28)        |
| 1.7.6. Пять важных замкнутых класса.....                              | (29)        |
| 1.7.7. Теоремы Поста .....                                            | (32)        |
| 1.7.8. Упражнение.....                                                | (37)        |
| 1.7.9. Упражнение.....                                                | (37)        |
| 1.7.10. Упражнение.....                                               | (38)        |
| 1.7.11. Упражнение.....                                               | (38)        |
| 1.7.12. Упражнение.....                                               | (39)        |
| 1.7.13. Упражнение.....                                               | (39)        |
| <b>2. Логика предикатов.....</b>                                      | <b>(40)</b> |
| <b>2.1. Язык прикладной логики предикатов .....</b>                   | <b>(40)</b> |
| 2.1.1. Элементы языка прикладной логики предикатов.....               | (40)        |
| 2.1.2. Кванторы. Свободные и связанные переменные .....               | (41)        |
| 2.1.3. Основные свойства кванторов .....                              | (41)        |
| 2.1.4. Ограниченные кванторы.....                                     | (42)        |
| 2.1.5. Упражнение .....                                               | (42)        |
| 2.1.6. Пример формализации в языке прикладной логики предикатов ..... | (43)        |
| 2.1.7. Упражнение .....                                               | (43)        |
| <b>2.2. Следствие в прикладной логике предикатов.....</b>             | <b>(44)</b> |
| 2.2.1. Применение правил общности .....                               | (44)        |
| 2.2.2. Обозначения сложных выражений. Ограниченные кванторы .....     | (44)        |
| 2.2.3. Пример с подстроками.....                                      | (45)        |
| 2.2.4. Применение правил существования .....                          | (45)        |
| 2.2.5. Обратное применение правил общности .....                      | (46)        |
| 2.2.6. Равенство как логический предикат .....                        | (46)        |
| 2.2.7. Квантор существования и единственности .....                   | (47)        |
| 2.2.8. Упражнение .....                                               | (47)        |
| 2.2.9. Упражнение .....                                               | (47)        |
| <b>2.3. Основные теоремы логики предикатов .....</b>                  | <b>(48)</b> |
| 2.3.1. Теорема о кванторах, отрицании, конъюнкции и дизъюнкции .....  | (48)        |
| 2.3.2. Теорема о кванторах и импликации .....                         | (49)        |
| 2.3.3. Упражнение .....                                               | (50)        |
| <b>Литература.....</b>                                                | <b>(51)</b> |

# 1. Логика высказываний

## 1.1. Определение логического следствия

### 1.1.1. Определение высказывания и предиката.

♦ **Высказывание** - это предложение, относительно которого имеет смысл утверждать, что оно *истинно* или *ложно*. ♣ Например, “ $5 > 3$ ”, “ $5 < 3$ ”, “Дюма-сын есть сын Дюма-отца”, “ $5^7 > 7^5$ ”. ♦ **Предикат** - предложение, относящееся к одному или нескольким неопределенным объектам, которое превращается в высказывание всякий раз, когда все входящие в него неопределенные объекты заменены их конкретными представителями. ♣ Например, “ $x < 3$ ”, “прямая  $l$  параллельна прямой  $m$ ”. ♦ Имена неопределенных объектов называются **переменными** данного предиката. Каждая переменная имеет свою **область изменения**, которая должна явно или неявно указываться при задании предиката. ♦ Если область изменения каждой переменной данного предиката состоит из единственного элемента, то предикат по существу является высказыванием; поэтому мы **будем считать высказывание частным случаем предиката**.

### 1.1.2. Определение умозаключения, посылок и заключения.

♦ Пусть  $A_1, A_2, \dots, A_n$  и  $B$  – предикаты. Утверждение типа “Из  $A_1, A_2, \dots, A_n$  следует  $B$ ” независимо от того, на чем оно основано, называют **умозаключением**, предикаты  $A_1, A_2, \dots, A_n$  – его **посылками**, предикат  $B$  – **заключением**. ♣ Например, “Из  $x < y, y < z$  следует, что  $x < z$ ”. ♣ В курсе математической логики, в основном, изучаются **логические умозаключения**, выражаемые словами “Из  $A_1, A_2, \dots, A_n$  логически следует  $B$ ” или формулой  $A_1, A_2, \dots, A_n \models B$ . В приведенном выше примере, как мы вскоре увидим, заключение не является **логическим следствием** посылок, но является **следствием в теории вещественных чисел**.

### 1.1.3. Определение интерпретации и контрпримера.

♦ **Интерпретацией** списка предикатов будем называть приращение всем его словам *произвольных* смысловых значений, при котором *форма* предикатов не меняется, а сами предикаты становятся высказываниями, т.е. определенно истинными или ложными предложениями. ♦ **Форма** предложения с точки зрения логики определяется следующими семью словами и словосочетаниями или их языковыми эквивалентами:

“не”, “и”, “или”, “если...то”, “если и только если”,  
“для любого”, “существует”

– этим выражениям во всех интерпретациях должны придаваться обычные смысловые значения. ♦ **Контрпримером** к умозаключению  $A_1, A_2, \dots, A_n \models B$  называется такая его интерпретация, в которой все посылки истинны, а заключение ложно. ♣ Например, к умозаключению  $x < y, y < z \models x < z$  можно приве-

сти следующий контрпример: Дюма-сын – сын Дюма-отца, Дюма-отец – сын Дюма-деда, следовательно (?!), Дюма-сын – сын Дюма-деда. “Словарь” этой интерпретации таков:  $x$  – Дюма-сын,  $y$  – Дюма-отец,  $z$  – Дюма-дед,  $<$  – является сыном.

#### 1.1.4. Определение логического следствия и следствия в теории.

♦ Будем говорить, что заключение  $B$  **логически следует** из посылок  $A_1, A_2, \dots, A_n$ , и писать  $A_1, A_2, \dots, A_n \models B$ , если к данному умозаключению не существует контрпримера. ♣ Например,  $x < y, y < z \models x < z$ , что показывает построенный выше контрпример. ♦ Пусть  $T$  – некоторая теория. Говорят, что **в этой теории из посылок  $A_1, A_2, \dots, A_n$  следует  $B$**  (и пишут  $A_1, A_2, \dots, A_n \Rightarrow_T B$ , или  $A_1, A_2, \dots, A_n \Rightarrow B$ ), если список посылок можно дополнить истинными в  $T$  утверждениями  $T_1, T_2, \dots, T_m$ , так, что из расширенного списка посылок предложение  $B$  *следует* логически:  $A_1, A_2, \dots, A_n, T_1, T_2, \dots, T_m \models B$ . Для аксиоматической теории  $T$  *истинность* того или иного предложения означает, что его можно доказать строго логически, т.е. в конечном счёте установить, что оно *логически следует* из аксиом и определений данной теории. Для иных теорий критерии истинности могут быть иными. Для констатации истинности иногда используется обозначение « $\Rightarrow_T B$ » или « $\Rightarrow B$ ». ♣ В арифметике вещественных чисел  $x < y, y < z \Rightarrow x < z$ . Действительно, эта теория включает в качестве аксиомы или теоремы (это зависит от конкретного способа её построения) следующее свойство транзитивности неравенств: “Если  $x < y$  и  $y < z$ , то  $x < z$ ”. Добавив его к двум посылкам рассматриваемого умозаключения, мы уже не сможем к полученному рассуждению найти контрпример, потому что добавленная посылка как раз означает, что в случае истинности первых двух посылок заключение не может быть ложно. (Напомним, что выражениям “если...то”, “и”, входящим в добавленную посылку, должны придаваться их обычные смысловые значения).

**1.1.5. Упражнение.** Доказать, что заключение не является логическим следствием посылок. Определить, является ли оно следствием в теории.

1. Неверно, что 7 делится на 2 и на 3. Следовательно, 7 не делится на 2 и не делится на 3.
2. Если число 9 делится на 4, то оно делится на 2. Следовательно, если 9 не делится на 4, то 9 не делится на 2.
3. Число  $n$  не делится на 2 или не делится на 3. Следовательно, неверно, что  $n$  делится на 2 или на 3.
4. Если число  $n$  делится на 2 и на 5, то  $n$  делится на 10.  $n$  не делится на 10. Следовательно,  $n$  не делится на 2 и не делится на 5.
5. В множестве  $A$  не существует числа  $a$ , которое удовлетворяет неравенству  $a > 3$ . Следовательно, для любого числа  $a$  из  $A$  справедливо неравенство  $a \leq 3$ .

6. Существует рациональное число, которое больше 0, и рациональное число, которое меньше 1. Следовательно, существует рациональное число, которое больше 0 и меньше 1.
7. Для любой фигуры из данного списка верно, что она является треугольником или квадратом. Следовательно, любая фигура из этого списка есть треугольник или все фигуры в данном списке являются квадратами.
8. Для любого числа  $a$  из множества  $A$  существует натуральное  $N$ , такое, что  $a < N$ . Следовательно, существует такое натуральное  $N$ , что для любого  $a$  из  $A$  выполнено неравенство  $a < N$ .

## 1.2. Язык логики высказываний

### 1.2.1. Логические связки.

♣ Как сказано выше, логическая *форма* предложения определяется семью перечисленными в 1.1.3 выражениями. ♦ Первые пять из них называются *логическими связками*; они изучаются в *логике высказываний*. Последние два - *квантором общности* и *квантором существования*; их изучением занимается *логика предикатов*. ♦ Логические связки и кванторы рассматриваются в логике как *операции*, с помощью которых из данных предикатов, называемых *операндами*, строятся более сложные предикаты. ♦ Для логических связок вводятся следующие обозначения и названия: «неверно, что  $A$ » –  $\neg A$  ( $\bar{A}$ ) – *отрицание*; « $A$  и  $B$ » –  $A \wedge B$  ( $AB, A \& B$ ) – *конъюнкция*; « $A$  или  $B$ » –  $A \vee B$  – *дизъюнкция*; «если  $A$ , то  $B$ » –  $A \rightarrow B$  – *импликация*; « $A$ , если и только если  $B$ » –  $A \leftrightarrow B$  – *двойная импликация*. ♦ Формальные определения логических связок задаются в виде *таблиц истинности*, определяющих *истинностные значения* сложных предикатов через истинностные значения операндов:

| $A$      | $B$      | $\neg A$ | $A \wedge B$ | $A \vee B$ | $A \rightarrow B$ | $A \leftrightarrow B$ |
|----------|----------|----------|--------------|------------|-------------------|-----------------------|
| <i>и</i> | <i>и</i> | <i>л</i> | <i>и</i>     | <i>и</i>   | <i>и</i>          | <i>и</i>              |
| <i>и</i> | <i>л</i> |          | <i>л</i>     | <i>и</i>   | <i>л</i>          | <i>л</i>              |
| <i>л</i> | <i>и</i> | <i>и</i> | <i>л</i>     | <i>и</i>   | <i>и</i>          | <i>л</i>              |
| <i>л</i> | <i>л</i> |          | <i>л</i>     | <i>л</i>   | <i>и</i>          | <i>и</i>              |

### 1.2.2. Формулы логики высказываний.

♦ В результате последовательного применения логических связок к простым предикатам, обозначенным буквами, получаются *формулы логики высказываний*. Порядок действий в них, как и в алгебраических формулах, задаётся с помощью скобок. ♣ Например, для формулы  $((\neg A) \rightarrow B) \wedge (A \rightarrow B) \rightarrow B$  действия в порядке их выполнения можно пронумеровать следующим образом:

$$\begin{array}{ccccccccc}
 ((\neg & A) & \rightarrow & B) & \wedge & (A & \rightarrow & B)) & \rightarrow & B \\
 1 & & 2 & & & 4 & & 3 & & 5
 \end{array}$$

♣ Словами данную формулу можно прочесть так: если отрицание  $A$  влечёт  $B$  и  $A$  влечёт  $B$ , то справедливо  $B$ . ♦ Как и в алгебре, в логике принято **соглашение о порядке действий**, в соответствии с которым при отсутствии скобок операции выполняются в следующем порядке:  $\neg, \wedge, \vee, \{\rightarrow, \leftrightarrow\}$  (импликация и двойная импликация считаются действиями одной ступени, то есть при отсутствии скобок они выполняются в порядке слева направо). ♣ Например, рассмотренную выше формулу можно записать в виде  $(\neg A \rightarrow B) \wedge (A \rightarrow B) \rightarrow B$ . Если же опустить и оставшиеся четыре скобки, то порядок действий и смысл формулы будет иной:

$$\begin{array}{ccccccccc} \neg & A & \rightarrow & B & \wedge & A & \rightarrow & B & \rightarrow & B \\ 1 & & 3 & & 2 & & 4 & & 5 & \end{array}$$

**1.2.3. Упражнение.** Записать формулу на обычном языке. Найти интерпретации предложений  $A, B, C$ , в которых она истинна и ложна.

- |                                                                                 |                                                                                           |
|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| 1. $A \wedge \neg B \leftrightarrow C \rightarrow \neg A$ .                     | 7. $(A \wedge B \rightarrow C) \rightarrow (\neg C \rightarrow A)$ .                      |
| 2. $(A \rightarrow (B \rightarrow C)) \rightarrow (A \wedge B \rightarrow C)$ . | 8. $(A \wedge \neg C \vee B) \wedge (B \rightarrow C) \wedge (A \vee \neg B)$ .           |
| 3. $\neg(A \rightarrow B) \leftrightarrow A \wedge \neg B$ .                    | 9. $(A \rightarrow C) \wedge (A \vee B \vee C) \wedge B \wedge \neg C$ .                  |
| 4. $(A \rightarrow B \vee C) \rightarrow (\neg B \rightarrow A)$ .              | 10. $(A \rightarrow B) \wedge A \wedge (\neg B \vee \neg C)$ .                            |
| 5. $A \vee (\neg B \leftrightarrow C) \rightarrow \neg A$ .                     | 11. $(\neg A \rightarrow B \vee C) \wedge (C \rightarrow B)$ .                            |
| 6. $(A \rightarrow B \wedge C) \wedge (B \vee (\neg C \rightarrow A))$ .        | 12. $(A \rightarrow C) \wedge (\neg B \rightarrow \neg C) \wedge \neg(A \rightarrow B)$ . |

#### 1.2.4. Формализация в логике высказываний.

♦ Сложности записи утверждения, сформулированного на обычном языке общения, в виде логической формулы аналогичны проблемам перевода с одного языка на другой. Правда, следует заметить, что язык формальной логики существенно беднее любого языка общения, что значительно облегчает задачу перевода, которую можно осуществлять, придерживаясь следующего алгоритма. В предложении следует выделить основную его форму ( “не верно, что ...”, “... и ...”, “... или ...”, “если ..., то ...”, “..., тогда и только тогда, когда ...” и т.п.), и заменить её на соответствующую логическую формулу ( $\neg A, A \wedge B, A \vee B, A \rightarrow B, A \leftrightarrow B$ ). Затем с каждой частью предложения, обозначенной в полученной формуле буквами  $A$  и  $B$ , и представляющей собой самостоятельное утверждение, проделать ту же процедуру, если только утверждение не оказывается простым высказыванием. После этого буквы  $A$  и  $B$  в первоначальной формуле заменяются на полученные вместо них формулы. Повторяем процесс формализации до тех пор, пока все буквы формулы не будут соответствовать простым высказываниям. В процессе формализации необходимо следить за тем, чтобы разные вхождения одного и того же высказывания обозначались одной буквой, а разные высказывания были обозначены разными буквами.

♣ Например, формализуем утверждение “Произведение  $ab$  положительно в том и только в том случае, когда  $a$  и  $b$  — оба положительны или оба отрицательны”. Основная форма этого предложения — “... в том и только в том случае, когда ...”, аналогичная форме “..., тогда и только тогда, когда...”. Заменим её на

формулу  $A \leftrightarrow X$ , где  $A$  – “Произведение  $ab$  положительно” и  $X$  – “ $a$  и  $b$  – оба положительны или оба отрицательны”.  $A$  является простым высказыванием, а  $X$  имеет форму “... или ...”, заменяем её на  $Y \vee Z$  в первоначальной формуле:  $A \leftrightarrow Y \vee Z$ . Высказывания  $Y$  – “ $a$  и  $b$  – оба положительны” и  $Z$  – “ $a$  и  $b$  – оба отрицательны” имеют одну и ту же форму, которую легче определить, переформулировав эти предложения без изменения смысла следующим образом.  $Y$  – “ $a$  – положительно и  $b$  – положительно”,  $Z$  – “ $a$  – отрицательно и  $b$  – отрицательно”. Форму “... и ...” этих предложений заменим на формулы  $B \wedge C$  и  $D \wedge E$ . Подставляя их в основную формулу вместо  $Y$  и  $Z$ , получим окончательно  $A \leftrightarrow B \wedge C \vee D \wedge E$ .  $B$  – “ $a$  – положительно”,  $C$  – “ $b$  – положительно”,  $D$  – “ $a$  – отрицательно”,  $E$  – “ $b$  – отрицательно” – простые высказывания.

**1.2.5. Упражнение.** Записать следующие утверждения в виде формул логики высказываний.

1. Положительное число  $T$  является периодом функции  $f$  в том и только в том случае, когда  $x$  принадлежит области определения  $f$  только вместе с  $x+T$  и выполнено равенство  $f(x+T) = f(x)$ .
2. Число  $x$  принадлежит области определения  $f$ , но  $f(x+T) \neq f(x)$ .
3. Неверно, что для вещественного числа  $x$  и для натурального числа  $n$  неравенства  $xn > 10n$  и  $x \leq 10$  выполнены одновременно.
4. Неверно, что утверждения  $x$  больше нуля, число  $a$  меньше нуля, их произведение  $ax > 0$  выполнены одновременно.
5. Функции  $f$  является возрастающей в том и только в том случае, когда для  $x_1 < x_2$  выполнено неравенство  $f(x_1) < f(x_2)$ .
6. Для  $x$  выполнено неравенство  $ax > 0$ , причём число  $a$  меньше нуля.

### 1.2.6. Формализация необходимых и достаточных условий.

♦ Остановимся особо на вопросе формализации предложений, содержащих слова “необходимо” и “достаточно” в качестве основной формы. Оба эти слова выражают импликацию, а в сочетании друг с другом двойную импликацию. Для того, чтобы правильно выбрать направление импликации в этом случае, нужно определить какой предикат в предложении играет роль необходимого (достаточного) условия. Тогда второй основной предикат предложения автоматически играет роль достаточного (необходимого) условия. **Правильное направление стрелки импликации – от достаточного условия к необходимому.**

♣ Например, в предложении “Справедливости неравенства  $a < 1$  достаточно для выполнения неравенства  $b < 0$ ” предикат  $A$  – “справедливо неравенства  $a < 1$ ” является достаточным условием, а предикат  $B$  – “выполнено неравенство  $b < 0$ ” автоматически определяем, как необходимое условие. Исходное предложение представимо импликацией  $A \rightarrow B$ .



**1.2.7. Упражнение.** Записать следующие утверждения в виде формул логики высказываний.

1. Для того, чтобы дробь  $\frac{a}{b}$  была меньше нуля, необходимо, чтобы  $b$  было отрицательно.
2. Для того, чтобы  $z$  не принадлежал  $D$ , необходимо, чтобы  $y$  не принадлежал  $C$ , а для того чтобы  $z$  принадлежал  $D$ , достаточно, чтобы  $x$  принадлежал  $B$ .
3. Неравенство  $d > 0$  необходимо для выполнения неравенства  $c > 1$  и достаточно для выполнения неравенства  $a < 1$ .
4. Для того, чтобы дробь  $\frac{x}{y}$  принадлежала множеству  $A$ , необходимо и достаточно, чтобы  $x$  принадлежал  $B$  и  $y$  принадлежал  $C$  или  $x$  принадлежал  $D$  и  $y$  принадлежал  $E$ .
5. Для того чтобы функция  $y(x)$  удовлетворяла первому и второму уравнениям системы, достаточно, чтобы оно удовлетворяло третьему, а для того чтобы  $y(x)$  не удовлетворяла второму уравнению, необходимо, чтобы  $y(x)$  не удовлетворяла первому уравнению.
6. *Выполнение утверждения  $E$  есть необходимое условие для выполнения утверждения  $A$ , а не выполнения  $D$  достаточно для не выполнения  $A$ .*

### 1.3. Следствие в логике высказываний

#### 1.3.1. Стандартные интерпретации.

♦ **Стандартной интерпретацией** предиката или списка предикатов будем называть придание всем входящим в них *простым предикатам истинностных значений* “и” или “л” – в отличие от рассматривавшейся ранее *смысловой интерпретации*, когда входящим в предикаты *словам* придавались различные *смысловые значения*. При этом различным *вхождениям* одного и того же простого предиката должны придаваться одинаковые истинностные значения.

♣ Например, если в сложном предикате или списке предикатов участвуют только простые предикаты  $A$  и  $B$ , то полный перечень стандартных интерпретаций можно записать в виде: *ии, ил, ли, лл* – *первая буква задаёт истинностное значение  $A$ , вторая –  $B$* . При наличии трёх простых предикатов  $A, B, C$  будет восемь стандартных интерпретаций; их принято располагать в алфавитном порядке: *иии, иил, или, илл, лии, лил, лли, ллл*. Заметим, что для последней по алфавиту буквы  $C$  значения чередуются через одно, для  $B$  – через 2, для  $A$  – через 4. Такой порядок всегда приводит к алфавитному расположению всех стандартных интерпретаций. Заметим также, что при увеличении числа простых предикатов на 1 количество стандартных интерпретаций увеличивается вдвое, так что для  $n$  простых предикатов будет  $2^n$  интерпретаций.

#### 1.3.2. Таблицы истинности.

Если задан сложный предикат, то с помощью определения логических операций можно во всех его стандартных интерпретациях найти истинностное зна-

чение самого предиката, т.е. получить *таблицу истинности* сложного предиката. Рассмотрим два примера.

|                    |                      |
|--------------------|----------------------|
| $\neg(A \wedge B)$ | $\neg A \vee \neg B$ |
| 4 2 3 1            | 3 2 5 4 1            |
| л и и и            | л и л л и            |
| и и л л            | л и и и л            |
| и л л и            | и л и л и            |
| и л л л            | и л и и л            |

Во вторых строчках обеих таблиц проставлены номера, указывающие на порядок заполнения столбцов. В столбцах 1 и 2 формируются стандартные интерпретации в алфавитном порядке – так, как описано в предыдущем пункте. Остальные столбцы заполняются последовательно с помощью таблиц истинности логических операций.

**1.3.3. Упражнение.** Построить таблицы истинности для формул из упражнения 1.2.3.

#### 1.3.4. Таблицы истинности и логическое следствие.

♦ Таблицы истинности дают полную информацию об истинностных значениях сложных предикатов во всех *стандартных* интерпретациях. Поскольку в каждой *смысловой* интерпретации все простые предикаты принимают определённые истинностные значения, она эквивалентна некоторой стандартной интерпретации. Поэтому с помощью таблиц истинности можно полностью решать вопрос о существовании или отсутствии контрпримеров для любого умозаключения в логике высказываний. ♣ Например, если в п. 1.3.2 сравнить результирующий столбец 4 в первой таблице с результирующим столбцом 5 второй, то мы увидим, что они одинаковы. Это означает, что  $\neg(A \wedge B) \models \neg A \vee \neg B$ , и наоборот,  $\neg(A \wedge B) \models \neg A \vee \neg B$ . Вместе эти два соотношения записывают в виде  $\neg(A \wedge B) \models \neg A \vee \neg B$  и говорят, что данные формулы *логически эквивалентны*.

#### 1.3.5. Направленная табличная процедура.

Поиск контрпримера путем перебора *всех* стандартных интерпретаций, т.е. построения полной таблицы истинности данного умозаключения, может оказаться слишком громоздким, так как число  $2^n$  всех стандартных интерпретаций очень быстро растёт с ростом  $n$ . Кроме того, в логике предикатов, как мы увидим, множество стандартных интерпретаций бесконечно, так что полный перебор вообще невозможен. Поэтому мы выработаем *направленную табличную процедуру*, не связанную с перебором всех стандартных интерпретаций. На первых шагах составляется *система логических уравнений*, приписывающая всем посылкам значение “и”, а заключению – “л”. Если с помощью таблиц истинности логических связок для этой системы будет найдено хотя бы одно решение, т.е. набор значений простых предикатов, удовлетворяющий этой системе, то мы получим контрпример к данному умозаключению; если же окажется, что система не имеет решений, то можно сделать вывод, что умозаключение *логично*. Методы решения систем логических уравнений рассмотрим на ряде примеров.

### 1.3.6. Примеры доказательств направленной процедурой.

♣ В следующих таблицах показано составление и решение систем логических уравнений для двух умозаключений.

$$A \vee B, \neg A \stackrel{x}{|=} B$$

|          |          |          |          |          |           |          |
|----------|----------|----------|----------|----------|-----------|----------|
| <i>л</i> | <i>и</i> | <i>и</i> | <i>и</i> | <i>л</i> | <i>да</i> | <i>л</i> |
| 5        | 1        | 6        | 2        | 4        |           | 3        |

$$A \rightarrow B, \neg A \stackrel{?}{\neq} B$$

|          |          |          |          |          |            |          |
|----------|----------|----------|----------|----------|------------|----------|
| <i>л</i> | <i>и</i> | <i>л</i> | <i>и</i> | <i>л</i> | <i>нет</i> | <i>л</i> |
| 5        | 1        | 6        | 2        | 4        |            | 3        |

На первых двух шагах посылкам присваивается значение «и», а на третьем – заключению значение «л»; тем самым составляется система логических уравнений для поиска контрпримера. Шаг 4 в обеих таблицах следует из 2 и определения отрицания, 5 – из 4 (перенос). Шаг 6 в левой таблице следует из 1, 5 и определения дизъюнкции. В правой – из 3 (перенос).

В левой таблице получено (и отмечено подчёркиванием) противоречие между шагами 6 и 3. Оно показывает, что контрпримера не существует, т.е. заключение логически следует из посылок; это зафиксировано словом «да» под знаком логического следствия.

В правой таблице противоречий нет, т.е. найден контрпример:  $A = B = л$ . Значит, заключение не следует логически из посылок; это отмечено словом «нет».

### 1.3.7. Примеры доказательств с разветвлением.

♣ Следующее табличное доказательство (левая таблица), в отличие от предыдущего, состоит не из одной строки истинностных значений, а из двух, поскольку на третьем шаге произошло *разветвление* процесса поиска контрпримера.

$$A \vee (B \wedge C) \stackrel{x}{|=} (A \vee B) \wedge (A \vee C)$$

|           |          |          |          |          |           |          |          |          |          |          |          |
|-----------|----------|----------|----------|----------|-----------|----------|----------|----------|----------|----------|----------|
| <i>?и</i> | <i>и</i> |          |          |          | <i>да</i> | <i>и</i> | <i>и</i> |          | <i>л</i> | <i>и</i> | <i>и</i> |
| 3         | 1        |          |          |          | 4         | 6        |          | 2        | 5        | 7        |          |
| <i>\л</i> | <i>и</i> | <i>и</i> | <i>и</i> | <i>и</i> |           | <i>и</i> | <i>и</i> | <i>л</i> |          | <i>и</i> | <i>и</i> |
| 3         | 1        | 5        | 4        | 6        |           | 9        | 7        | 2        |          | 10       | 8        |

$$A \vee (B \wedge C) \stackrel{?}{\neq} (A \vee B) \wedge (A \wedge C)$$

|           |          |           |          |          |            |          |          |          |          |          |          |          |
|-----------|----------|-----------|----------|----------|------------|----------|----------|----------|----------|----------|----------|----------|
| <i>?и</i> | <i>и</i> | <i>?и</i> | <i>л</i> | <i>л</i> | <i>нет</i> | <i>и</i> | <i>и</i> | <i>и</i> | <i>л</i> | <i>и</i> | <i>л</i> | <i>л</i> |
| 3         | 1        | 11        | 10       | 9        |            | 4        | 6        | 12       | 2        | 5        | 7        | 8        |

Дело в том, что после шага 1 (дизъюнкция истинна) и шага 2 (конъюнкция ложна) мы не можем сделать определённого вывода о значениях операндов. На третьем шаге вопросительным знаком отмечено *предположение*, исходя из которого происходит дальнейшее заполнение строки, приводящее в конце к противоречию между 2, 6 и 7 шагами. Отметим, что на шагах 6 и 7 значение дизъюнкции найдено по значению *одного* операнда – поскольку он оказался истинным, дизъюнкция будет истинна независимо от значения второго операнда.

Рассмотрение альтернативного значения для  $A$  проведено в следующей строке. Значения первых двух шагов перенесены из предыдущей строки, а на третьем шаге косой чертой отмечено начало рассмотрения нового случая. Поскольку и здесь получено противоречие (между шагами 2, 9 и 10), можно сде-

лать окончательный вывод о том, что заключение следует логически из посылки; это отмечено словом «да» под знаком логического следствия.

♣ На правой таблице изображена направленная табличная процедура для несколько изменённого умозаключения: в последней скобке вместо дизъюнкции поставлена конъюнкция. Отличие от предыдущей таблицы начинается с шага 7: из шагов 2 и 6 мы сделали вывод, что конъюнкция ложна, а затем (шаг 8), что  $C = л$ . На шаге 11 вновь пришлось сделать предположение, поскольку предыдущие шаги не определяют однозначно значение  $B$ . Результатом в этом случае явился контрпример:  $A = B = и, C = л$ , так как никаких противоречий не появилось. Поскольку одного контрпримера достаточно для обоснования отрицательного ответа, рассматривать прочие значения для  $A$  и  $B$  уже не нужно, построение таблицы на этом закончено.

**1.3.8. Упражнение.** Проверить, является ли заключение логическим следствием посылок.

- |                                                                                        |                                                                             |
|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| 1. $A \rightarrow (B \rightarrow C) \models A \wedge B \rightarrow C$ .                | 5. $\neg A \rightarrow B \vee C, C \rightarrow B \models A \rightarrow B$ . |
| 2. $A \rightarrow B \vee C \models \neg B \rightarrow A$ .                             | 6. $A \rightarrow C, B \vee C \vee A \models B \rightarrow C$ .             |
| 3. $\neg(A \rightarrow B) \models A \wedge \neg B$ .                                   | 7. $\neg A \vee B, B \rightarrow C \models \neg C \rightarrow \neg A$ .     |
| 4. $\neg C \rightarrow (\neg A \vee \neg B) \models A \rightarrow (B \rightarrow C)$ . | 8. $A \rightarrow B, \neg C \rightarrow \neg B \models \neg A \vee C$ .     |

**1.3.9. Упражнение.** Формализовать умозаключения и проверить их логичность.

- Число  $n$  меньше 100 или неверно, что  $n$  делится на 2 и на 3. Если  $n$  меньше 100, то  $n$  – двузначное число. Следовательно, чтобы число  $n$  не было двузначным, необходимо, чтобы  $n$  не делилось на 2 или не делилось на 3.
- Если сумма  $n + m$  не делится на 3, то  $n$  не делится на 3 или  $m$  не больше 2. Сумма  $n + m$  не делится на 3 или  $n \cdot m$  больше 4. Следовательно, чтобы  $n$  делилось на 3, а  $m$  было больше 2, необходимо, чтобы  $n \cdot m$  было больше 4.
- Число  $n$  не является простым или  $n > 100$ . Если  $n > 100$ , то  $k$  делится на 2 и больше 3. Следовательно, чтобы  $n$  не было простым, достаточно, чтобы  $k$  не делилось на 2 или было не больше 3.
- Для того, чтобы произведение  $n \cdot m$  делилось на 6, достаточно, чтобы  $n$  делилось на 2, а  $m$  – на 3. Если  $m$  не больше 2, то  $n \cdot m$  не делится на 6. Следовательно,  $n$  не делится на 2, или  $m$  не делится на 3, или  $m$  больше 2.
- Если  $x + y$  – четное число, то  $x = 3$  или  $y = 7$ . Если  $x = 3$ , то  $y = 7$ . Для равенства  $y = 7$  необходима четность суммы  $x + y$ . Следовательно,  $x + y$  четно тогда и только тогда, когда  $y = 7$ .
- Верно, что  $x < 0$ , или  $x = 0$ , или  $x > 0$ . Если  $x > 0$  или  $x = 0$ , то  $x = 0$ . Для равенства  $x = 0$  необходимо, чтобы условие  $x < 0$  было нарушено. Следовательно, условие  $x < 0$  нарушается тогда и только тогда, когда  $x = 0$ .
- Если  $x$  – не натуральное число, то  $x < 0$  или  $x = 1/2$ .  $x = 1/2$  или неверно, что  $x < 0$ . Если  $x = 1/2$ , то  $x$  – не натуральное число. Следовательно, для того, чтобы равенство  $x = 1/2$  не выполнялось, необходимо и достаточно, чтобы  $x$  было натуральным числом.

8. Число  $x$  делится на 8, или сумма его цифр равна 13, или  $x=0$ . Если равенство  $x=0$  не выполнено, то сумма цифр числа  $x$  не равна 13. Если  $x=0$ , то  $x$  делится на 8. Следовательно, для справедливости равенства  $x=0$  необходимо и достаточно, чтобы  $x$  делилось на 8.

### 1.3.10. Определение логической эквивалентности, тавтологии и противоречия.

♦ Как уже отмечалось в п.1.3.4, предикаты  $A$  и  $B$  называются **логически эквивалентными** ( $A \models B$ ), если  $A \models B$  и  $B \models A$ . ♦ Предикат  $B$  называется **тавтологией** ( $\models B$ ), если он истинен в любой интерпретации. ♣ Например, очевидно,  $\models A \rightarrow A$ . ♦ Список предикатов  $S$  называется **логически противоречивым** (или **противоречием**), если входящие в него предикаты не могут быть одновременно истинными ни в какой интерпретации. Обозначение:  $S \models$ . ♣ Например,  $A, \neg A \models$ .

♣ В следующих трёх таблицах показано применение направленной табличной процедуры для доказательства логической эквивалентности, тавтологии и противоречия. Первая состоит из доказательства двух логических следствий, проведённого в единой таблице. Во второй и третьей таблицах отличие от доказательства логического следствия заключается в том, что при доказательстве тавтологии на первом шаге всему предикату присваивается значение «л», а при доказательстве противоречия на первых шагах каждому из предикатов данного списка присваивается значение «и».

|                                                                                                                                                       |                                                                                                      |                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| $A \rightarrow B \models \neg B \rightarrow \neg A$                                                                                                   | $\models A \vee B \rightarrow (\neg A \rightarrow B)$                                                | $A \wedge B, \neg A \vee \neg B \models$                                                                     |
| $\begin{array}{cccc} и & и & л & \\ \hline 7 & 1 & 8 & \end{array} \models \begin{array}{cccc} и & л & л & л \\ \hline 3 & 5 & 2 & 4 & 6 \end{array}$ | $\begin{array}{cccc} да & л & и & л & л & л & л \\ \hline 7 & 2 & 8 & 1 & 4 & 6 & 3 & 5 \end{array}$ | $\begin{array}{cccc} и & и & и & л & и & и & л & и & да \\ \hline 3 & 1 & 4 & 7 & 5 & 2 & 8 & 6 \end{array}$ |
| $\begin{array}{ccc} и & л & л \\ \hline 3 & 2 & 4 \end{array} \models \begin{array}{ccc} и & л & и & л & и \\ \hline 7 & 5 & 1 & 8 & 6 \end{array}$   |                                                                                                      |                                                                                                              |

### 1.3.11. Упражнение. Проверить логическую эквивалентность.

- $\neg(A \vee B) \models \neg A \wedge \neg B$ .
- $A \wedge (B \wedge C) \models (A \wedge B) \wedge C$ .
- $A \rightarrow B \models \neg A \vee B$ .
- $A \rightarrow B \models \neg B \rightarrow \neg A$ .
- $A \leftrightarrow B \models (A \rightarrow B) \wedge (B \rightarrow A)$ .
- $A \vee (B \wedge C) \models (A \vee B) \wedge (A \vee C)$ .
- $A \rightarrow (B \rightarrow C) \models (A \wedge B) \rightarrow C$ .
- $A \rightarrow B \vee C \models (A \rightarrow B) \vee (A \rightarrow C)$ .

### 1.3.12. Упражнение. Проверить, является ли формула тавтологией.

- $\models \neg(A \rightarrow B) \vee (\neg A \vee B \wedge C)$ .
- $\models (A \wedge B \rightarrow C) \rightarrow (\neg C \rightarrow \neg A \vee \neg B)$ .
- $\models (\neg A \rightarrow B \vee C) \wedge (C \rightarrow B) \rightarrow (A \rightarrow B)$ .
- $\models (A \rightarrow C) \wedge (\neg B \rightarrow \neg C) \rightarrow (A \rightarrow B)$ .

### 1.3.13. Упражнение. Проверить, противоречив ли данный набор формул.

- $\neg(A \rightarrow B), \neg B \rightarrow \neg A \models$ .
- $A \wedge B, \neg A \vee \neg B \models$ .
- $(A \rightarrow B) \rightarrow C, \neg C \wedge (\neg A \vee B) \models$ .
- $A \rightarrow (B \wedge C), B \vee (\neg C \rightarrow A) \models$ .

**1.3.14. Свойства логического следствия, эквивалентности, тавтологии и противоречия.** Пусть  $A, B, C$  – предикаты,  $S$  – список предикатов (возможно, пустой). Тогда справедливы следующие утверждения.

1.  $(A, B, S \models C) \leftrightarrow (A \wedge B, S \models C)$  (объединение посылок).
2.  $(A, B, S \models C) \leftrightarrow (B, S \models A \rightarrow C)$  (перенос посылки, теорема о дедукции).
3.  $(A \models B) \leftrightarrow (\models A \rightarrow B)$  (сведение следствия к тавтологии).
4.  $(A \models B) \leftrightarrow (A, \neg B \models)$  (сведение следствия к противоречию).
5.  $(\models B) \leftrightarrow (\neg B \models)$  (сведение тавтологии к противоречию).
6.  $(\models B) \rightarrow (A \models B)$  (тавтология следует из любой посылки).
7.  $(S \models) \rightarrow (S \models B)$  (из противоречия следует любое заключение).
8.  $(A \models B) \wedge (B \models C) \rightarrow (A \models C)$  (транзитивность логического следствия).
9.  $(A \models B) \wedge (B \models C) \rightarrow (A \models C)$  (транзитивность логической эквивалентности).

♥ Например, докажем утверждение 2. Пусть верна левая часть двойной импликации, а правая ложна. Тогда найдется интерпретация, в которой предикаты  $B, S$  истинны, а импликация  $A \rightarrow C$  ложна. Последнее означает, что  $A$  истинно, а  $C$  ложно. Итак, в найденной интерпретации все предикаты в левой части соотношения  $A, B, S \models C$  истинны, а  $C$  ложно. Мы получили противоречие с тем, что левая часть двойной импликации верна.

Наоборот, пусть  $B, S \models A \rightarrow C$ , но  $A, B, S \not\models C$ . Тогда существует интерпретация, в которой  $A, B, S$  истинны, а  $C$  ложно. Но в этой интерпретации ложна и импликация  $A \rightarrow C$  при истинных  $B, S$ , чего не может быть по предположению. Утверждение 2 доказано.

**1.3.15. Упражнение.** Доказать остальные свойства. Сформулировать и доказать аналогичные свойства следствия, эквивалентности, истинности и противоречия в теории.

## 1.4. Основные теоремы логики высказываний

В следующих двух теоремах собраны соотношения логики высказываний, наиболее часто встречающиеся в практике математических рассуждений.

### 1.4.1. Теорема об отрицании, конъюнкции и дизъюнкции.

1) Закон тождества:

$$A \models A.$$

2) Закон двойного отрицания:

$$\neg\neg A \models A.$$

3) Правила удаления и введения  $\wedge$  и  $\vee$ :

$$A \wedge B \models A,$$

$$A \vee B, \neg A \models B,$$

$$A, B \models A \wedge B,$$

$$A \models A \vee B,$$

$$A \wedge A \models A$$

$$A \models A \vee A.$$

4) Действия с константами – тавтологией (и) и противоречивым предикатом (л):

$$A \wedge \text{л} \models \text{л},$$

$$A \wedge \text{и} \models A,$$

$$A \vee \text{и} \models \text{и},$$

$$A \vee \text{л} \models A.$$

5) Коммутативность:

$$A \wedge B \models B \wedge A,$$

$$A \vee B \models B \vee A.$$

6) Ассоциативность:

$$A \wedge (B \wedge C) \models (A \wedge B) \wedge C,$$

$$A \vee (B \vee C) \models (A \vee B) \vee C.$$

7) Дистрибутивность:

$$A \wedge (B \vee C) \models (A \wedge B) \vee (A \wedge C), \quad A \vee (B \wedge C) \models (A \vee B) \wedge (A \vee C).$$

8) Законы де Моргана:

$$\neg(A \wedge B) \models \neg A \vee \neg B,$$

$$\neg(A \vee B) \models \neg A \wedge \neg B.$$

9) Закон противоречия:

$$A, \neg A \models .$$

10) Закон исключенного третьего:

$$\models B \vee \neg B.$$

#### 1.4.2. Теорема об импликации и двойной импликации.

1) Правила удаления и введения:

$$A \rightarrow B, A \models B,$$

$$B \models A \rightarrow B,$$

$$A \rightarrow A \models \text{и}.$$

$$A \leftrightarrow B \models (A \rightarrow B) \wedge (B \rightarrow A).$$

2) Действия с константами:

$$A \rightarrow \text{и} \models \text{и}, \quad \text{и} \rightarrow A \models A, \quad \text{л} \rightarrow B \models \text{и}, \quad A \rightarrow \text{л} \models \neg A,$$

3) Закон контрапозиции:

$$A \rightarrow B \models \neg B \rightarrow \neg A.$$

4) Выражение  $\rightarrow$  через  $\neg$  и  $\vee$ :

$$A \rightarrow B \models \neg A \vee B.$$

5) Транзитивность:

$$A \rightarrow B, B \rightarrow C \models A \rightarrow C,$$

$$A \leftrightarrow B, B \leftrightarrow C \models A \leftrightarrow C.$$

#### 1.4.3. Упражнение. Доказать сформулированные утверждения.

#### 1.4.4. Замечания об истории, терминологии и обозначениях.

♣ Основы логики как науки о формах правильных умозаключений заложены в трудах Аристотеля в четвёртом веке до новой эры. Используя современный язык, можно сказать, что основные исследования Аристотеля относились к логике предикатов, которая излагается во второй главе данного курса. Найденные Аристотелем и некоторыми его последователями *фигуры силлогизмов* (правильных логических умозаключений) были настолько простыми и общими, что до середины девятнадцатого столетия логика считалась наукой завершённой и преподавалась практически в неизменном виде.

♣ В середине 19 века в работах ирландского математика Джорджа Буля и шотландского математика Августа де Моргана для описания и исследования логи-

ческих законов начинает применяться алгебраическая символика. Появляется *алгебра логики*, которая позже становится *математической логикой*, т.е. теорией логических доказательств, широко применяющей математическую символику и математические методы и направленной, главным образом, на исследование *оснований математики*.

♣ Существует очевидная аналогия между алгеброй высказываний и алгеброй множеств. Подобного рода *булевы* структуры имеют в настоящее время развитую общую теорию и разнообразные приложения.

♣ В начале 20 века математика переживала *кризис оснований*, связанный с открытием и исследованием *парадоксов теории множеств*. В этот период логические законы подверглись всестороннему критическому обсуждению, которое и привело к созданию современной математической логики как *теории доказательств*. Оживлённые дискуссии велись, в частности, по вопросу о границах применимости закона исключённого третьего, на котором основываются в математике многочисленные неконструктивные теоремы о существовании тех или иных объектов.

♣ Со второй половины 19 века математическая логика начинает применяться для описания и исследования таких технических объектов, как *контактные схемы, схемы из функциональных элементов, конечные автоматы*.

♣ В технических приложениях формулы логики высказываний рассматривают как *двузначные функции от нескольких двузначных переменных* - функции и их аргументы принимают значения в множестве  $\{и, л\}$ . Такие функции и переменные называются *булевыми (булевыми)*. При рассмотрении булевых функций часто вместо “и”, ”л” пишут, соответственно, “1” и ”0”, конъюнкцию  $A \wedge B$  обозначают  $AB$ , отрицание  $\neg A - \bar{A}$ , а вместо знака логической эквивалентности пишут знак равенства. В дальнейшем мы будем иногда использовать такие обозначения.

**1.4.5. Упражнения.** Упростить формулы применяя теоремы логики высказываний.

- |                                                                                              |                                                                                                |
|----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| 1) $(A \rightarrow B) \rightarrow A \wedge B$ ;                                              | 2) $\neg(A \rightarrow B) \vee A \wedge B$ ;                                                   |
| 3) $(A \vee \neg B \rightarrow A \wedge C) \vee (\neg A \vee C \rightarrow A \wedge B)$ ;    | 4) $\neg A \wedge B \vee A \wedge C \vee ((\neg A \vee \neg B) \rightarrow A \wedge \neg C)$ ; |
| 5) $A \wedge (A \vee \neg B \vee C) \rightarrow C$ ;                                         | 6) $A \rightarrow ((A \vee \neg B \vee C) \rightarrow C)$ ;                                    |
| 7) $(A \rightarrow \neg B) \rightarrow \neg(A \rightarrow B)$ ;                              | 8) $\neg(A \rightarrow \neg B) \vee \neg(A \rightarrow B)$ ;                                   |
| 9) $(\neg A \vee \neg C \rightarrow \neg A \wedge B) \vee A \wedge \neg C \vee A \wedge B$ ; | 10) $(\neg A \wedge C \rightarrow A \wedge B) \vee ((A \vee \neg B) \rightarrow A \wedge C)$ ; |
| 11) $A \wedge \neg C \rightarrow \neg A \wedge B \wedge \neg C$ ;                            | 12) $\neg C \rightarrow (A \rightarrow \neg A \wedge B \wedge \neg C)$ .                       |

**1.4.6. Упражнения.** Проверить логическое следствие предварительно упростив посылки и заключение.

- $\neg A \wedge B \vee ((A \vee B) \rightarrow C), (B \rightarrow A \wedge C) \vee \neg A \wedge C \models \neg A \wedge \neg B \vee C$ ;
- $(\neg A \vee B) \wedge (B \rightarrow C), (B \rightarrow A) \wedge (B \vee \neg C) \models (\neg A \vee C) \wedge (A \vee \neg C)$ ;



- 3)  $(\neg B \vee C) \rightarrow (A \rightarrow B \wedge C), (A \vee B) \rightarrow (\neg C \rightarrow \neg A \wedge B) \models A \rightarrow B \wedge C;$
- 4)  $(A \wedge \neg C) \rightarrow (\neg B \vee A \wedge C), (A \vee B) \rightarrow (\neg A \wedge B \vee C) \models \neg C \rightarrow \neg A \wedge \neg B;$
- 5)  $(\neg B \vee C) \wedge (A \rightarrow B), (A \vee \neg B) \wedge (C \rightarrow B) \models A \wedge B \vee \neg A \wedge \neg C;$
- 6)  $A \rightarrow (\neg B \vee C \rightarrow B \wedge C), (A \vee \neg B) \rightarrow (\neg A \wedge \neg B \vee C) \models \neg B \vee \neg C \rightarrow \neg A;$
- 7)  $(\neg C \rightarrow \neg A \wedge B) \vee \neg A \wedge \neg B, B \rightarrow (A \wedge C \vee \neg A \wedge C) \models A \wedge B \rightarrow C;$
- 8)  $\neg A \wedge \neg B \vee \neg A \wedge C \vee B \wedge C, (B \rightarrow A) \wedge (C \rightarrow B) \models \neg(A \wedge \neg C) \wedge (C \rightarrow A);$
- 9)  $A \wedge (\neg B \vee \neg C) \rightarrow B \wedge \neg C, (A \vee B) \wedge \neg C \rightarrow \neg A \wedge B \models (\neg A \vee B) \wedge (\neg A \vee C);$
- 10)  $((A \vee B) \wedge \neg C) \rightarrow \neg A \wedge B, B \wedge (A \vee \neg C) \rightarrow A \wedge C \models \neg C \rightarrow \neg A \wedge \neg B;$
- 11)  $(B \rightarrow C) \wedge (A \rightarrow B), A \wedge B \vee A \wedge \neg C \vee \neg B \wedge \neg C \models (A \vee C) \rightarrow A \wedge C;$
- 12)  $A \wedge (\neg B \vee C) \rightarrow B \wedge C, \neg(\neg A \wedge B \vee C) \rightarrow \neg A \wedge \neg B \models (A \rightarrow B) \wedge (A \rightarrow C).$

### 1.5. Принцип двойственности

Будем обозначать  $x_1, x_2, \dots, x_n$  - **логические переменные**, принимающие значения из множества констант  $E = \{0, 1\}$ . **Функцией алгебры логики** от переменных  $x_1, x_2, \dots, x_n$  будем называть любую функцию  $f: \underbrace{\{0, 1\} \times \{0, 1\} \times \dots \times \{0, 1\}}_n \rightarrow \{0, 1\}$ . Каждой формуле логики высказываний

соответствует определённая функция алгебры логики, определяемая таблицей истинности для данной формулы. Но функция алгебры логики может выражаться различными формулами, логически эквивалентными между собой.

**Определение.** Функция  $[f(x_1, \dots, x_n)]^*$ , равная  $\bar{f}(\bar{x}_1, \dots, \bar{x}_n)$ , называется **двойственной функцией к функции  $f(x_1, \dots, x_n)$** .

Очевидно, что таблица для двойственной функции (при выбранном порядке наборов) получается из таблицы для функции  $f(x_1, \dots, x_n)$  инвертированием (т. е. заменой 0 на 1 и 1 на 0) столбца функции и его переворачиванием (см. табл. 6).

Т а б л и ц а 6

| $x_1$ | $x_2$ | $x_3$ | $f(x_1, x_2, x_3)$ | $[f(x_1, x_2, x_3)]^*$ |
|-------|-------|-------|--------------------|------------------------|
| 0     | 0     | 0     | 1                  | 0                      |
| 0     | 0     | 1     | 1                  | 1                      |
| 0     | 1     | 0     | 0                  | 0                      |
| 0     | 1     | 1     | 0                  | 1                      |
| 1     | 0     | 0     | 0                  | 1                      |
| 1     | 0     | 1     | 1                  | 1                      |
| 1     | 1     | 0     | 0                  | 0                      |
| 1     | 1     | 1     | 1                  | 0                      |

Обозначение:  $[f(x_1, \dots, x_n)]^* = f^*(x_1, \dots, x_n)$ .

$$f^{**} = (f^*)^* = f,$$

Очевидно,

### 1.5.1. Определение дополнительных логических связей.

- 1)  $x \oplus y = \overline{x \leftrightarrow y}$  - сложение по модулю два (порядок выполнения как  $y \leftrightarrow x$ );
- 2)  $x | y = \overline{x \wedge y}$  - штрих Шеффера (по порядку выполнения стоит между  $\wedge$  и  $\vee$ );
- 3)  $x \downarrow y = \overline{x \vee y}$  - стрелка Пирса (по порядку выполнения стоит между  $\vee$  и  $\rightarrow$ );

1.5.2. Упражнение Доказать следующие свойства сложения по модулю два.

- 1)  $x \oplus y = y \oplus x$  (коммутативность);
- 2)  $x \oplus (y \oplus z) = (x \oplus y) \oplus z$  (ассоциативность);
- 3)  $1 \oplus x = \bar{x}$  (выражение отрицания);
- 4)  $0 \oplus x = x$
- 5)  $x \wedge (y \oplus z) = x \wedge y \oplus x \wedge z$  (дистрибутивность).

### 1.5.3. Упражнение Найти функции, двойственных к данным:

1)  $1^*$ ; 2)  $0^*$ ; 3)  $x^*$ ; 4)  $\bar{x}^*$ ; 5)  $(x \wedge y)^*$ ; 6)  $(x \vee y)^*$ ; 7)  $(x \rightarrow y)^*$ ; 8)  $(x \leftrightarrow y)^*$  9)  $(x \oplus y)^*$ .

Пусть заданы функции  $f(y_1, y_2, \dots, y_m)$ ,  $f_1(x_{11}, x_{12}, \dots, x_{1p_1})$ ,  $f_2(x_{21}, x_{22}, \dots, x_{2p_2})$ , ...,  $f_m(x_{m1}, x_{m2}, \dots, x_{mp_m})$ . Обозначим через  $x_1, x_2, \dots, x_n$  объединённое множество переменных функций  $f_1, f_2, \dots, f_m$ .

**Теорема 2.** Если

$$\Phi(x_1, \dots, x_n) = f(f_1(x_{11}, \dots, x_{1p_1}), \dots, f_m(x_{m1}, \dots, x_{mp_m})),$$

то

$$\Phi^*(x_1, \dots, x_n) = f^*(f_1^*(x_{11}, \dots, x_{1p_1}), \dots, f_m^*(x_{m1}, \dots, x_{mp_m})).$$

**Доказательство.**

$$\begin{aligned} \Phi^*(x_1, \dots, x_n) &= \overline{\Phi}(\bar{x}_1, \dots, \bar{x}_n) = \\ &= \bar{f}(f_1(\bar{x}_{11}, \dots, \bar{x}_{1p_1}), \dots, f_m(\bar{x}_{m1}, \dots, \bar{x}_{mp_m})) = \\ &= \bar{f}(\bar{f}_1(\bar{x}_{11}, \dots, \bar{x}_{1p_1}), \dots, \bar{f}_m(\bar{x}_{m1}, \dots, \bar{x}_{mp_m})) = \\ &= \bar{f}(\bar{f}_1^*(x_{11}, \dots, x_{1p_1}), \dots, \bar{f}_m^*(x_{m1}, \dots, x_{mp_m})) = \\ &= f^*(f_1^*(x_{11}, \dots, x_{1p_1}), \dots, f_m^*(x_{m1}, \dots, x_{mp_m})). \end{aligned}$$

Из теоремы вытекает

**Принцип двойственности.** Если формула  $\mathfrak{A} = C[f_1, \dots, f_s]$  реализует функцию  $f(x_1, \dots, x_n)$ , то формула  $C[f_1^*, \dots, f_s^*]$ , т. е. формула, полученная из  $\mathfrak{A}$  заменой функций  $f_1, \dots, f_s$  соответственно на  $\bar{f}_1^*, \dots, \bar{f}_s^*$ , реализует функцию  $f^*(x_1, \dots, x_n)$ .

Эту формулу мы будем называть формулой, двойственной к  $\mathfrak{A}$ , и обозначать через  $\mathfrak{A}^*$ . Таким образом,

$$\mathfrak{A}^* = C[f_1^*, \dots, f_s^*].$$

Для формул над множеством  $\mathfrak{P} = \{0, 1, \bar{x}, x_1 \& x_2, x_1 \vee x_2\}$  принцип двойственности может быть сформулирован так: для получения формулы  $\mathfrak{A}^*$ , двойственной к формуле  $\mathfrak{A}$ , нужно в формуле  $\mathfrak{A}$  всюду заменить

0 на 1, 1 на 0, & на  $\vee$ ,  $\vee$  на &.

**1.5.4. Упражнение** По функциям  $f(x_1, x_2)$  и  $g(x_1, x_2)$ , заданными векторами  $\tilde{\alpha}_f$  и  $\tilde{\alpha}_g$  значений в таблице истинности, построить функцию  $h$ .

1)  $\tilde{\alpha}_f = (1011), \tilde{\alpha}_g = (0111),$

a)  $h(\tilde{x}^2) = f(x_1, g(x_1, x_2));$       б)  $h(\tilde{x}^2) = g(x_2, f(x_2, x_1));$

в)  $h(\tilde{x}^2) = f(f(x_1, g(x_1, x_2)), g(x_1, x_2));$

г)  $h(\tilde{x}^3) = g(x_1, x_2) \oplus f(x_3, g(x_1, x_2));$

д)  $h(\tilde{x}^3) = f(x_2, g(x_3, x_1)) \leftrightarrow g(x_1, g(x_2, x_3)).$

2)  $\tilde{\alpha}_f = (1010), \tilde{\alpha}_g = (0110),$

a)  $h(\tilde{x}^3) = f(x_3, g(x_1, x_2));$       б)  $h(\tilde{x}^3) = g(g(x_3, x_2), f(x_1, x_3));$

в)  $h(\tilde{x}^3) = f(f(x_3, g(x_1, x_2)), g(x_1, x_2));$

г)  $h(\tilde{x}^3) = f(f(x_1, x_2), g(x_3, x_1)) \rightarrow g(x_1, g(x_1, x_2)).$

**1.5.5. Упражнение** Перечислить все существенные и фиктивные переменные у следующих функций.

1)  $f(\tilde{x}^3) = (10101010);$

2)  $f(\tilde{x}^3) = (10011001);$

3)  $f(\tilde{x}^3) = (00111100);$

4)  $f(\tilde{x}^4) = (0101111101011111);$

5)  $f(\tilde{x}^4) = (1100110000110011);$

6)  $f(\tilde{x}^4) = (1011010110110101);$

7)  $f(\tilde{x}^2) = ((x_1 \vee x_2) \rightarrow x_1 \cdot x_2) \oplus (x_1 \rightarrow x_2) \cdot (x_2 \rightarrow x_1);$

8)  $f(\tilde{x}^2) = (x_1 \cdot x_2 \oplus (x_1 \rightarrow x_2)) \rightarrow (x_1 \leftrightarrow x_1 \cdot x_2);$

9)  $f(\tilde{x}^3) = ((x_1 \rightarrow \overline{x_2}) \oplus (x_2 \rightarrow \overline{x_3})) \oplus (x_2 \rightarrow x_3);$

10)  $f(\tilde{x}^3) = ((x_1 \vee x_2 \cdot \overline{x_3}) \rightarrow (x_2 \rightarrow x_1 \cdot x_3)) \rightarrow (x_1 \vee x_3);$

11)  $f(\tilde{x}^3) = ((x_1 \downarrow (x_2 \mid x_3)) \downarrow (x_2 \downarrow (x_1 \mid x_3))) \downarrow (x_1 \mid x_2).$

**1.5.6. Упражнение** Показать, что  $x_1$  фиктивная переменная функции  $f$ , реализовав функцию эквивалентной формулой, не содержащей  $x_1$ .

1)  $f(\tilde{x}^2) = (x_2 \rightarrow x_1) \cdot (x_2 \downarrow x_2);$

2)  $f(\tilde{x}^2) = (x_1 \leftrightarrow x_2) \vee (x_1 \mid x_2);$

$$3) f(\tilde{x}^3) = ((x_1 \oplus x_2) \rightarrow x_3) \cdot \overline{(x_3 \rightarrow x_2)};$$

$$4) f(\tilde{x}^3) = ((x_1 \vee x_2 \cdot \overline{x_3}) \leftrightarrow (\overline{x_1} \rightarrow \overline{x_2} \cdot x_3)) \cdot (x_2 \downarrow x_3);$$

$$5) f(\tilde{x}^3) = ((x_1 \vee x_2 \vee \overline{x_3}) \rightarrow (x_1 x_2 \mid x_3)) \oplus (x_2 \rightarrow x_1) \cdot x_3.$$

**1.5.7. Упражнение** Используя непосредственно определение двойственности булевых функций, а также основные тождества, выяснить, является ли функция  $g$  двойственной к функции  $f$ :

$$1) f = x \oplus y, g = x \leftrightarrow y;$$

$$2) f = x \mid y, g = x \downarrow y;$$

$$3) f = x \rightarrow y, g = \overline{x} \cdot y;$$

$$4) f = x \cdot y \rightarrow z, g = \overline{x} \cdot \overline{y} \cdot z;$$

$$5) f = (\overline{x} \rightarrow \overline{y}) \rightarrow (y \rightarrow x), g = (x \rightarrow y) \cdot (\overline{y} \rightarrow \overline{x});$$

$$6) f = x \cdot y \vee z, g = x \cdot (y \vee z).$$

**1.5.8. Упражнение** Используя принцип двойственности, построить и упростить формулу, реализующую функцию, двойственную к функции  $f$ :

$$1) f = (x \vee y \vee z) \cdot (y \oplus z) \vee x \cdot y \cdot z;$$

$$2) f = (x \vee (1 \rightarrow y)) \vee y \cdot \overline{z} \vee (\overline{x} \mid \overline{y \downarrow \overline{z}});$$

$$3) f = (x \downarrow y) \oplus ((x \mid y) \downarrow (\overline{x} \leftrightarrow y \cdot z));$$

$$4) f = (\overline{x} \vee \overline{y} \vee (y \cdot \overline{z} \oplus 1)) \downarrow z;$$

$$5) f = (x \cdot (y \cdot z \vee 0) \leftrightarrow (z \cdot 1 \vee \overline{x} \cdot y)) \vee \overline{y} \cdot z;$$

$$6) f = (x \downarrow z) \oplus ((x \vee y) \leftrightarrow (\overline{x} \downarrow (y \vee \overline{z}))).$$

**1.6. Разложение булевых функций по переменным.**  
**Совершенные дизъюнктивная и конъюнктивная**  
**нормальная форма.**

Введем обозначение

$$x^\sigma = x\sigma \vee \overline{x\sigma},$$

где  $\sigma$  — параметр, равный либо 0, либо 1. Очевидно, что

$$x^\sigma = \begin{cases} \overline{x} & \text{при } \sigma = 0, \\ x & \text{при } \sigma = 1. \end{cases}$$

Легко видеть, что  $x^\sigma = 1$  тогда и только тогда, когда  $x = \sigma$ , т. е. значение «основания» равно значению «показателя».

И  $x^\sigma = 0$  тогда и только тогда, когда  $x \neq \sigma$  или  $x = \neg\sigma$ .

**Теорема 3** (о разложении функций по переменным). *Каждую функцию алгебры логики  $f(x_1, \dots, x_n)$  при любом  $m$  ( $1 \leq m \leq n$ ) можно представить в следующей форме:*

$$f(x_1, \dots, x_m, x_{m+1}, \dots, x_n) = \bigvee_{(\sigma_1, \dots, \sigma_m)} x_1^{\sigma_1} \& \dots \& x_m^{\sigma_m} \& f(\sigma_1, \dots, \sigma_m, x_{m+1}, \dots, x_n), (*)$$

где дизъюнкция берется по всевозможным наборам значений переменных  $x_1, \dots, x_m$ .

Это представление называется *разложением функции по  $m$  переменным  $x_1, \dots, x_m$* .

**Доказательство.** Рассмотрим произвольный набор констант  $\alpha_1, \alpha_2, \dots, \alpha_n$  и покажем, что на нём левая и правая части равенства (\*) совпадают. Левая часть равна  $f(\alpha_1, \alpha_2, \dots, \alpha_n)$ , а правая

$$\bigvee_{(\sigma_1, \dots, \sigma_m)} \alpha_1^{\sigma_1} \wedge \dots \wedge \alpha_m^{\sigma_m} \wedge f(\sigma_1, \dots, \sigma_m, \alpha_{m+1}, \dots, \alpha_n),$$

по свойству  $x^\sigma$  отличной от

нуля будет только одна конъюнкция  $\alpha_1^{\alpha_1} \wedge \dots \wedge \alpha_m^{\alpha_m} = 1$ , а при всех других наборах констант  $(\sigma_1, \dots, \sigma_m)$   $\alpha_1^{\sigma_1} \wedge \dots \wedge \alpha_m^{\sigma_m} = 0$ . Тогда по теоремам логики высказываний

$$\bigvee_{(\sigma_1, \dots, \sigma_m)} \alpha_1^{\sigma_1} \wedge \dots \wedge \alpha_m^{\sigma_m} \wedge f(\sigma_1, \dots, \sigma_m, \alpha_{m+1}, \dots, \alpha_n) = f(\alpha_1, \dots, \alpha_m, \alpha_{m+1}, \dots, \alpha_n).$$

Что и требовалось доказать.

В качестве следствий получаем два специальных случая разложения.

1) Разложение по переменной:

$$f(x_1, \dots, x_{n-1}, x_n) = \\ = x_n \& f(x_1, \dots, x_{n-1}, 1) \vee \bar{x}_n \& f(x_1, \dots, x_{n-1}, 0).$$

Функции  $f(x_1, \dots, x_{n-1}, 0)$  и  $f(x_1, \dots, x_{n-1}, 1)$  называются *компонентами разложения*. Данное разложение полезно, когда какие-либо свойства булевых функций устанавливаются по индукции.

2) Разложение по всем  $n$  переменным:

$$f(x_1, \dots, x_n) = \bigvee_{(\sigma_1, \dots, \sigma_n)} x_1^{\sigma_1} \& \dots \& x_n^{\sigma_n} \& f(\sigma_1, \dots, \sigma_n).$$

При  $f(x_1, \dots, x_n) \not\equiv 0$  оно может быть преобразовано

$$\bigvee_{(\sigma_1, \dots, \sigma_n)} x_1^{\sigma_1} \& \dots \& x_n^{\sigma_n} \& f(\sigma_1, \dots, \sigma_n) = \\ = \bigvee_{\substack{(\sigma_1, \dots, \sigma_n) \\ f(\sigma_1, \dots, \sigma_n) = 1}} x_1^{\sigma_1} \& \dots \& x_n^{\sigma_n}.$$

В результате окончательно получим

$$f(x_1, \dots, x_n) = \bigvee_{\substack{(\sigma_1, \dots, \sigma_n) \\ f(\sigma_1, \dots, \sigma_n) = 1}} x_1^{\sigma_1} \& \dots \& x_n^{\sigma_n}. \quad (**)$$

Такое разложение носит название *совершенной дизъюнктивной нормальной формы* (совершенной д. н. ф.).

**Теорема 4.** *Каждая функция алгебры логики может быть выражена в виде формулы через отрицание, конъюнкцию и дизъюнкцию.*

**Доказательство.** 1) Пусть  $f(x_1, \dots, x_n) \equiv 0$ . Тогда, очевидно,

$$f(x_1, \dots, x_n) = x_1 \& \bar{x}_1.$$

2) Пусть  $f(x_1, \dots, x_n) \not\equiv 0$ . Представим ее в совершенной д. н. ф.:

$$f(x_1, \dots, x_n) = \bigvee_{\substack{(\sigma_1, \dots, \sigma_n) \\ f(\sigma_1, \dots, \sigma_n) = 1}} x_1^{\sigma_1} \& \dots \& x_n^{\sigma_n}.$$

Данная теорема носит конструктивный характер, так как она позволяет для каждой функции фактически построить формулу, ее реализующую (в виде совершенной д. н. ф.): в таблице для функции  $f(x_1, \dots, x_n)$  ( $f \not\equiv 0$ ) отмечаем все строки  $(\sigma_1, \dots, \sigma_n)$ , в которых  $f(\sigma_1, \dots, \sigma_n) = 1$ , для каждой такой строки образуем логическое произведение

$$x_1^{\sigma_1} \& \dots \& x_n^{\sigma_n},$$

и затем все полученные конъюнкции соединяем знаком **дизъюнкции**.

Покажем, что для функции  $f \not\equiv 0$  существует представление в виде «совершенной конъюнктивной нормальной формы» (СКНФ). В этих условиях  $f^* \not\equiv 0$ , поэтому для неё существует СДНФ

$$f^*(x_1, \dots, x_n) = \bigvee_{\substack{(\sigma_1, \dots, \sigma_n) \\ f^*(\sigma_1, \dots, \sigma_n) = 1}} x_1^{\sigma_1} \& \dots \& x_n^{\sigma_n}.$$

Возьмем тождество для двойственных формул

$$f^{**}(x_1, \dots, x_n) = \bigwedge_{\substack{(\sigma_1, \dots, \sigma_n) \\ f^*(\sigma_1, \dots, \sigma_n) = 1}} (x_1^{\sigma_1} \vee \dots \vee x_n^{\sigma_n}).$$



Левая часть есть  $f(x_1, \dots, x_n)$ , а правая может быть преобразована далее:

$$\begin{aligned} \bigwedge_{\substack{(\sigma_1, \dots, \sigma_n) \\ f(\sigma_1, \dots, \sigma_n)=1}} (x_1^{\sigma_1} \vee \dots \vee x_n^{\sigma_n}) &= \bigwedge_{\substack{(\sigma_1, \dots, \sigma_n) \\ f(\bar{\sigma}_1, \dots, \bar{\sigma}_n)=0}} (x_1^{\sigma_1} \vee \dots \vee x_n^{\sigma_n}) = \\ &= \bigwedge_{\substack{(\sigma_1, \dots, \sigma_n) \\ f(\sigma_1, \dots, \sigma_n)=0}} (x_1^{\bar{\sigma}_1} \vee \dots \vee x_n^{\bar{\sigma}_n}). \end{aligned}$$

Таким образом, получаем разложение

$$f(x_1, \dots, x_n) = \bigwedge_{\substack{(\sigma_1, \dots, \sigma_n) \\ f(\sigma_1, \dots, \sigma_n)=0}} (x_1^{\bar{\sigma}_1} \vee \dots \vee x_n^{\bar{\sigma}_n}).$$

**Упражнение 1.6.1.** Построить СДНФ и СКНФ для функций, заданных следующими формулами.

а)

- 1)  $f(\tilde{x}^3) = x_1 \bar{x}_2 \vee \bar{x}_2 x_3 \vee (x_1 \rightarrow x_2 x_3)$ ;
- 2)  $f(\tilde{x}^3) = (x_1 \leftrightarrow \bar{x}_2) \vee (x_1 x_3 \oplus (x_2 \rightarrow x_3))$ ;
- 3)  $f(\tilde{x}^3) = (\bar{x}_1 \cdot x_2 \oplus x_3) \cdot (x_1 \cdot x_3 \rightarrow x_2)$ ;
- 4)  $f(\tilde{x}^3) = (\bar{x}_1 \vee \bar{x}_2 \vee \bar{x}_3) \cdot (x_1 \cdot x_2 \vee x_3)$ ;
- 5)  $f(\tilde{x}^3) = (x_1 \rightarrow x_2) \oplus (x_1 \mid x_2 \cdot x_3)$ ;
- 6)  $f(\tilde{x}^3) = (\bar{x}_1 \cdot x_2 \rightarrow x_3) \cdot ((x_1 \rightarrow x_3) \rightarrow x_2)$ .

б)

- 1)  $f(\tilde{x}^3) = \bar{x}_1 \cdot x_2 \vee \bar{x}_3$ ;
- 2)  $f(\tilde{x}^3) = \bar{x}_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_3$ ;
- 3)  $f(\tilde{x}^3) = x_1 \vee x_2 \cdot x_3 \vee \bar{x}_2 \cdot \bar{x}_3$ .

в)

- 1)  $f(\tilde{x}^3) = \bar{x}_1 \cdot (\bar{x}_2 \vee x_3)$ ;
- 2)  $f(\tilde{x}^3) = (x_1 \vee x_2) \cdot (\bar{x}_2 \vee x_3) \cdot \bar{x}_3$ ;
- 3)  $f(\tilde{x}^3) = (\bar{x}_1 \vee x_2) \cdot (x_1 \vee \bar{x}_3) \cdot (x_2 \vee x_3)$ .

## 1.7. Полнота и замкнутость систем булевых функций.

### 1.7.1. Определения, критерий полноты.

**О п р е д е л е н и е.** Система функций  $\{f_1, f_2, \dots, f_n, \dots\}$  из  $P_2$  называется (функционально) *полной*, если любая булева функция может быть записана в виде формулы через функции этой системы.

Примеры:

1. Система  $P_2$  — множество всех булевых функций — является полной системой.

2. Система  $\mathfrak{P} = \{\bar{x}, x_1 \& x_2, x_1 \vee x_2\}$  представляет полную систему.

**Т е о р е м а 5.** Пусть даны две системы функций из  $P_2$ :

$$\mathfrak{P} = \{f_1, f_2, \dots\}, \quad (\text{I})$$

$$\mathfrak{D} = \{g_1, g_2, \dots\}, \quad (\text{II})$$

относительно которых известно, что система I полна и каждая ее функция выражается в виде формулы через функции системы II. Тогда система II является полной.

**Доказательство.** Пусть  $h$  — произвольная функция из  $P_2$ . В силу полноты системы I можно выразить  $h$  формулой над  $\mathfrak{P}$ , т. е.

$$h = C[f_1, f_2, \dots, f_n, \dots]$$

(в скобках мы выписываем все функции системы  $\mathfrak{P}$ , хотя в формуле фактически встречается лишь конечное их число). По условию теоремы

$$f_1 = C_1[g_1, g_2, \dots],$$

$$f_2 = C_2[g_1, g_2, \dots],$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

Поэтому мы можем в формуле  $C[f_1, f_2, \dots]$  исключить вхождения функций  $f_1, f_2, \dots$ , заменив их формулами над  $\Omega^*$ ). Это можно записать так:

$$C[f_1, f_2, \dots] = C[C_1[g_1, g_2, \dots], C_2[g_1, g_2, \dots], \dots].$$

Последнее выражение определяет формулу над  $\Omega$  со строением  $C'$ . Мы получаем

$$C[C_1[g_1, g_2, \dots], C_2[g_1, g_2, \dots], \dots] = C'[g_1, g_2, \dots],$$

или, окончательно,

$$h = C'[g_1, g_2, \dots],$$

т. е. мы выразили  $h$  в виде формулы над  $\Omega$ . Теорема доказана.

**1.7.2. Упражнения.** Показать, что следующие системы булевых функций являются полными.

$$\{\neg, \wedge\}; \{\neg, \vee\}; \{\downarrow\}; \{\downarrow, \neg\}; \{1, \oplus, \wedge\}.$$

### 1.7.3. Полином Жегалкина.

**Определение полинома Жегалкина.** Элементарная конъюнкция называется *монотонной*, если она не содержит отрицаний переменных. *Константа* 1 (т. е. элементарная конъюнкция нулевого ранга) считается по определению *монотонной* элементарной конъюнкцией. Выражение вида

$$K_1 \oplus K_2 \oplus \dots \oplus K_s, \quad (15)$$

где  $K_i$  ( $i = 1, 2, \dots, s$ ) — попарно различные монотонные элементарные конъюнкции над фиксированным множеством переменных (в частности, над множеством  $X^n$ ,  $n \geq 1$ ), называется *полиномом Жегалкина* (или *полиномом по модулю 2*). Рассматривается также полином Жегалкина, соответствующий  $s = 0$ . Такой полином обозначают через 0 (независимо от множества переменных) и считают по определению, что он равен константе 0. Наибольший из рангов элементарных конъюнкций, входящих в полином, называется *степенью* этого полинома. Степень полинома 0 считается *неопределенной*. Число  $s$  называется *длиной полинома* (15). Справедлива следующая

**Теорема 6.** *Каждая функция из  $P_2$  может быть выражена при помощи полинома по mod 2 (полинома Жегалкина).*

**Доказательство.** Поскольку система  $\{1, \oplus, \wedge\}$  является полной, и конъюнкция дистрибутивна относительно сложения по модулю 2, то, очевидно, лю-

бая булева функция представима в виде полинома Жегалкина. Причем это представление единственно.

**Подсчитаем число полиномов Жегалкина от переменных  $x_1, \dots, x_n$ , т. е. число выражений вида**

$$\sum_{(i_1, \dots, i_s)} a_{i_1 \dots i_s} x_{i_1} \dots x_{i_s}.$$

**Число членов  $x_{i_1} \dots x_{i_s}$  равно количеству подмножеств  $(i_1, \dots, i_s)$  из  $n$  чисел  $(1, \dots, n)$ , т. е.  $2^n$ . Поскольку  $a_{i_1 \dots i_s}$  равно 0 или 1, искомое число полиномов равно  $2^{2^n}$ , т. е. числу всех булевых функций от тех же переменных. Отсюда, как следствие, получаем *единственность представления функций посредством полиномов Жегалкина*.**

**Упражнение 1.7.4.** Методом неопределённых коэффициентов найти полиномы Жегалкина для следующих функций.

- 1)  $f(\tilde{x}^2) = x_1 \mid x_2$ ; 2)  $f(\tilde{x}^2) = (0100)$ ; 3)  $f(\tilde{x}^3) = x_1(x_2 \vee \bar{x}_3)$ ;
- 4)  $f(\tilde{x}^3) = x_1 \rightarrow (x_2 \rightarrow x_3)$ ; 5)  $f(\tilde{x}^3) = (01101001)$ ;
- 6)  $f(\tilde{x}^3) = (10001110)$ ; 7)  $f(\tilde{x}^3) = (00000111)$ ;
- 8)  $f(\tilde{x}^3) = (01100110)$ ; 9)  $f(\tilde{x}^4) = (1000000000000001)$ ;
- 10)  $f(\tilde{x}^4) = (0000100010010000)$ .

**Упражнение 1.7.5.**

**2.24.** Представив функцию  $f(\tilde{x}^n)$  формулой над множеством связок  $\{\&, -\}$ , преобразовать затем полученную формулу в полином Жегалкина функции  $f(\tilde{x}^n)$  (используя эквивалентности  $\bar{A} = A \oplus 1$ ,  $A \cdot (B \oplus C) = A \cdot B \oplus A \cdot C$ ,  $A \cdot A = A$ ,  $A \cdot 1 = A$ ,  $A \oplus A = 0$  и  $A \oplus \oplus 0 = A$ ):

- 1)  $f(\tilde{x}^2) = x_1 \rightarrow (x_2 \rightarrow \bar{x}_1 x_2)$ ; 2)  $f(\tilde{x}^2) = x_1 \cdot (x_2 \sim x_1 \bar{x}_2)$ ;
- 3)  $f(\tilde{x}^3) = (x_1 \downarrow x_2) \mid (x_2 \downarrow x_3)$ ; 4)  $f(\tilde{x}^3) = (x_1 \vee x_2) \cdot (x_2 \mid x_3)$ ;
- 5)  $f(\tilde{x}^3) = x_1 \downarrow ((x_1 \rightarrow \bar{x}_2) \vee \bar{x}_3)$ ;
- 6)  $f(\tilde{x}^3) = (x_1 \rightarrow (x_2 \rightarrow x_3)) \cdot ((x_1 \rightarrow x_2) \rightarrow x_3)$ ;
- 7)  $f(\tilde{x}^3) = (x_1 \oplus x_2) \vee (x_2 \downarrow x_3)$ ;
- 8)  $f(\tilde{x}^4) = (x_1 \rightarrow x_2) \rightarrow (x_3 \rightarrow x_1 x_4)$ ;
- 9)  $f(\tilde{x}^4) = x_1 \vee (x_2 \rightarrow ((x_3 \rightarrow x_2) \rightarrow x_4))$ ;
- 10)  $f(\tilde{x}^4) = (x_1 \vee x_2 \vee x_3) x_4 \vee x_1 x_2 x_3$ .

**Определение.** Пусть  $\mathfrak{M}$  — некоторое подмножество функций из  $P_2$ . *Замыканием*  $\mathfrak{M}$  называется множество всех булевых функций, представимых в виде формул через функции множества  $\mathfrak{M}$ . Замыкание множества  $\mathfrak{M}$  обозначается через  $[\mathfrak{M}]$ . Легко видеть, что замыкание инвариантно относительно операций введения и удаления фиктивных переменных.

**Пример 13.**

1)  $\mathfrak{M} = P_2$ . Очевидно, что  $[\mathfrak{M}] = P_2$ .

2)  $\mathfrak{M} = \{1, x_1 + x_2\}$ . Замыканием этого множества будет класс  $L$  всех линейных функций, т. е. функций, имеющих вид

$$f(x_1, \dots, x_n) = c_0 + c_1x_1 + \dots + c_nx_n,$$

где  $c_i = 0, 1$  ( $i = 0, \dots, n$ ); существенные переменные входят с коэффициентом 1, фиктивные — с коэффициентом 0.

Отметим некоторые свойства замыкания:

- 1)  $[\mathfrak{M}] \equiv \mathfrak{M}$ ;
- 2)  $[[\mathfrak{M}]] = [\mathfrak{M}]$ ;
- 3) если  $\mathfrak{M}_1 \subseteq \mathfrak{M}_2$ , то  $[\mathfrak{M}_1] \subseteq [\mathfrak{M}_2]$ ;
- 4)  $[\mathfrak{M}_1 \cup \mathfrak{M}_2] \equiv [\mathfrak{M}_1] \cup [\mathfrak{M}_2]$ .

**Определение.** Класс (множество)  $\mathfrak{M}$  называется (функционально) *замкнутым*, если  $[\mathfrak{M}] = \mathfrak{M}$ .

**Пример 14.**

- 1) Класс  $\mathfrak{M} = P_2$  является замкнутым классом.
- 2) Класс  $\mathfrak{M} = \{1, x_1 + x_2\}$  не замкнут.
- 3) Класс  $L$  замкнут, так как линейное выражение, составленное из линейных выражений, является линейным. Легко видеть, что всякий класс  $[\mathfrak{M}]$  будет замкнутым. Это дает возможность получать многочисленные примеры замкнутых классов.

В терминах замыкания и замкнутого класса можно дать другое определение полноты (эквивалентное исходному):  $\mathfrak{M}$  — полная система, если  $[\mathfrak{M}] = P_2$ .

#### 1.7.6. Пять важных замкнутых классов.

1. Обозначим через  $T_0$  класс всех булевых функций  $f(x_1, \dots, x_n)$ , сохраняющих константу 0, т. е. функций, для которых выполнено равенство

$$f(0, \dots, 0) = 0.$$

Легко видеть, что функции 0,  $x$ ,  $x_1 \& x_2$ ,  $x_1 \vee x_2$ ,  $x_1 + x_2$  принадлежат классу  $T_0$ , а функции 1,  $\bar{x}$  не входят в  $T_0$ .

и поэтому  $T_0$  не является полной системой.

Покажем, что  $T_0$  — замкнутый класс. Пусть  $\Phi = f(f_1, \dots, f_m)$ , где  $f, f_1, \dots, f_m$  принадлежат классу  $T_0$ . Тогда, т.к.  $0 \in T_0$ , то

$$\begin{aligned} \Phi(0, \dots, 0) &= f(f_1(0, \dots, 0), \dots, f_m(0, \dots, 0)) = \\ &= f(0, \dots, 0) = 0. \end{aligned}$$

2. Обозначим через  $T_1$  класс всех булевых функций  $f(x_1, \dots, x_n)$ , сохраняющих константу 1, т. е. функций, для которых выполнено равенство

$$f(1, \dots, 1) = 1.$$

Легко видеть, что функции 1,  $x$ ,  $x_1 \& x_2$ ,  $x_1 \vee x_2$  принадлежат классу  $T_1$ , а функции 0,  $\bar{x}$  не входят в  $T_1$ .

Значит  $T_1$  тоже не является полной системой. Так же, как для  $T_0$ , доказывается, что  $T_1$  замкнутый класс.

3. Обозначим через  $S$  класс всех самодвойственных функций, т. е. функций  $f$  из  $P_2$  таких, что  $f^* = f$ .

Для самодвойственной функции имеет место тождество

$$\bar{f}(\bar{x}_1, \dots, \bar{x}_n) = f(x_1, \dots, x_n);$$

иначе говоря, на наборах  $(\alpha_1, \dots, \alpha_n)$  и  $(\bar{\alpha}_1, \dots, \bar{\alpha}_n)$ , которые мы будем называть *противоположными*, самодвойственная функция принимает противоположные значения. Отсюда следует, что самодвойственная функция полностью определяется своими значениями на первой половине строк (см. табл. 1). Поэтому число самодвойственных функций, зависящих от переменных  $x_1, \dots, x_n$ , равно  $2^{2^{n-1}} = \sqrt{2^{2^n}}$ .

Из этого следует, что класс  $S$  не является полным. Его замкнутость вытекает из очевидного для самодвойственных функций  $f, f_1, \dots, f_m$  тождества  $\Phi^* = f^*(f_1^*, \dots, f_m^*) = f(f_1, \dots, f_m) = \Phi$ .

**Определение.** Для двух наборов  $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$  и  $\tilde{\beta} = (\beta_1, \dots, \beta_n)$  выполнено отношение предшествования  $\tilde{\alpha} \preceq \tilde{\beta}$ , если

$$\alpha_1 \leq \beta_1, \dots, \alpha_n \leq \beta_n.$$

Например,  $(0, 1, 0, 1) \preceq (1, 1, 0, 1)$ .

Очевидно, что если  $\tilde{\alpha} \preceq \tilde{\beta}$  и  $\tilde{\beta} \preceq \tilde{\gamma}$ , то  $\tilde{\alpha} \preceq \tilde{\gamma}$ . Следует отметить, что не любые пары наборов находятся в отношении предшествования, например, наборы  $(0, 1)$  и  $(1, 0)$  в таком отношении не находятся. Таким образом, множество всех наборов длины  $n$  по отношению к операции предшествования  $\preceq$  является частично упорядоченным.

**Определение.** Функция  $f(x_1, \dots, x_n)$  называется *монотонной*, если для любых двух наборов  $\tilde{\alpha}$  и  $\tilde{\beta}$  таких, что  $\tilde{\alpha} \preceq \tilde{\beta}$ , имеет место неравенство

$$f(\tilde{\alpha}) \leq f(\tilde{\beta}).$$

Монотонными функциями, очевидно, будут  $0, 1, x, x_1 \& x_2$  и  $x_1 \vee x_2$ .

А импликация и двойная импликация не являются монотонными. Поэтому класс булевых функций  $M$ , состоящий из всех монотонных функций не является полным. Покажем, что он замкнут.

Пусть  $\Phi = f(f_1, \dots, f_m)$ , где  $f, f_1, \dots, f_m$  монотонны. Обозначим

$$\begin{aligned}\tilde{x} &= (x_1, \dots, x_n), \tilde{x}^1 = (x_{11}, \dots, x_{1p_1}), \dots, \tilde{x}^m = \\ &= (x_{m1}, \dots, x_{mp_m})\end{aligned}$$

— наборы переменных функций  $\Phi, f_1, \dots, f_m$ , причем множество переменных функции  $\Phi$  состоит из тех и только тех переменных, которые встречаются у функций  $f_1, \dots, f_m$ . Пусть  $\tilde{\alpha}$  и  $\tilde{\beta}$  — два набора длины  $n$  значений переменных  $x$ , причем  $\tilde{\alpha} \preceq \tilde{\beta}$ . Эти наборы определяют наборы  $\tilde{\alpha}^1, \tilde{\beta}^1, \dots, \tilde{\alpha}^m, \tilde{\beta}^m$  значений переменных  $x^1, \dots, x^m$  такие, что  $\tilde{\alpha}^1 \preceq \tilde{\beta}^1, \dots, \tilde{\alpha}^m \preceq \tilde{\beta}^m$ . В силу монотонности функций  $f_1, \dots, f_m$

$$f_1(\tilde{\alpha}^1) \leq f_1(\tilde{\beta}^1), \dots, f_m(\tilde{\alpha}^m) \leq f_m(\tilde{\beta}^m).$$

Поэтому

$$(f_1(\tilde{\alpha}^1), \dots, f_m(\tilde{\alpha}^m)) \preceq (f_1(\tilde{\beta}^1), \dots, f_m(\tilde{\beta}^m)),$$

и в силу монотонности  $f$  имеем

$$f(f_1(\tilde{\alpha}^1), \dots, f_m(\tilde{\alpha}^m)) \leq f(f_1(\tilde{\beta}^1), \dots, f_m(\tilde{\beta}^m)),$$

откуда получаем

$$\begin{aligned}\Phi(\tilde{\alpha}) &= f(f_1(\tilde{\alpha}^1), \dots, f_m(\tilde{\alpha}^m)) \leq f(f_1(\tilde{\beta}^1), \dots, f_m(\tilde{\beta}^m)) = \\ &= \Phi(\tilde{\beta}).\end{aligned}$$

**Определение.** Ксассом линейных функций  $L$  назовём множество всех булевых функций, представление которых в виде полинома Жегалкина не содержит конъюнкций более чем из одной переменной.

Очевидно, полином Жегалкина  $x \wedge y$  не является линейной функцией, поэтому класс  $L$  не является полным. Замкнутость  $L$  очевидна, т.к.  $\Phi = f(f_1, f_2, \dots, f_m)$ , где  $f, f_1, f_2, \dots, f_m$  — линейные функции, является подстановкой в линейное выражение вместо переменных линейных выражений, из которой после сложения одинаковых констант и переменных может получиться только линейный вид полинома Жегалкина.

### 1.7.7. Теорема Поста.



**Лемма 1.** Если  $f(x_1, \dots, x_n) \notin S$ , то из нее путем подстановки функций  $x$  и  $\bar{x}$  можно получить несамодвойственную функцию одного переменного, т. е. константу.

**Доказательство.** Так как  $f \notin S$ , то найдется набор  $(\alpha_1, \dots, \alpha_n)$  такой, что

$$f(\bar{\alpha}_1, \dots, \bar{\alpha}_n) = f(\alpha_1, \dots, \alpha_n).$$

Рассмотрим функции  $\varphi_i(x) = x^{\alpha_i}$  ( $i = 1, \dots, n$ ) и положим

$$\varphi(x) = f(\varphi_1(x), \dots, \varphi_n(x)).$$

Мы имеем

$$\begin{aligned} \varphi(0) &= f(\varphi_1(0), \dots, \varphi_n(0)) = f(0^{\alpha_1}, \dots, 0^{\alpha_n}) = \\ &= f(\bar{\alpha}_1, \dots, \bar{\alpha}_n) = f(\alpha_1, \dots, \alpha_n) = f(1^{\alpha_1}, \dots, 1^{\alpha_n}) = \\ &= f(\varphi_1(1), \dots, \varphi_n(1)) = \varphi(1). \end{aligned}$$

Лемма доказана.

**Лемма 2.** Если  $f(x_1, \dots, x_n) \notin M$ , то из нее путем подстановки констант 0 и 1 и функции  $x$  можно получить функцию  $\bar{x}$ .

**Доказательство.** Сначала покажем, что найдется пара соседних наборов  $\tilde{\alpha}$  и  $\tilde{\beta}$  таких, что  $\tilde{\alpha} \leq \tilde{\beta}$  и

$$f(\tilde{\alpha}) > f(\tilde{\beta}).$$

В самом деле, так как  $f \notin M$ , то существуют наборы  $\tilde{\alpha}^1$  и  $\tilde{\beta}^1$  такие, что  $\tilde{\alpha}^1 \leq \tilde{\beta}^1$  и  $f(\tilde{\alpha}^1) > f(\tilde{\beta}^1)$ . Если наборы  $\tilde{\alpha}^1$  и  $\tilde{\beta}^1$  — соседние, то наша цель достигнута. Если  $\tilde{\alpha}^1$  и  $\tilde{\beta}^1$  не являются соседними, то набор  $\tilde{\beta}^1$  отличается от набора  $\tilde{\alpha}^1$  в  $t$  координатах, где  $t > 1$ , причем эти  $t$  координат в наборе  $\tilde{\alpha}^1$  имеют значение 0, а в наборе  $\tilde{\beta}^1$  —

значение 1. В силу этого между  $\hat{\alpha}^1$  и  $\hat{\beta}^1$  можно вставить  $t-1$  промежуточных наборов  $\tilde{\alpha}^2, \tilde{\alpha}^3, \dots, \tilde{\alpha}^t$  таких, что

$$\tilde{\alpha}^1 \leq \tilde{\alpha}^2 \leq \dots \leq \tilde{\alpha}^t \leq \tilde{\beta}^1.$$

Очевидно, что наборы, стоящие в этой цепочке рядом, будут соседними. Так как  $f(\tilde{\alpha}^1) > f(\tilde{\beta}^1)$ , то по крайней мере на одной из этих пар соседних наборов — обозначим их через  $\tilde{\alpha}$  и  $\tilde{\beta}$  ( $\tilde{\alpha} \leq \tilde{\beta}$ ) — будет  $f(\tilde{\alpha}) > f(\tilde{\beta})$ . Предположим, что данные наборы имеют соседство по  $i$ -й координате и, следовательно,

$$\begin{aligned}\tilde{\alpha} &= (\alpha_1, \dots, \alpha_{i-1}, 0, \alpha_{i+1}, \dots, \alpha_n), \\ \tilde{\beta} &= (\alpha_1, \dots, \alpha_{i-1}, 1, \alpha_{i+1}, \dots, \alpha_n).\end{aligned}$$

Рассмотрим функцию

$$\varphi(x) = f(\alpha_1, \dots, \alpha_{i-1}, x, \alpha_{i+1}, \dots, \alpha_n).$$

Мы имеем

$$\begin{aligned}\varphi(0) &= f(\alpha_1, \dots, \alpha_{i-1}, 0, \alpha_{i+1}, \dots, \alpha_n) = f(\tilde{\alpha}) > f(\tilde{\beta}) = \\ &= f(\alpha_1, \dots, \alpha_{i-1}, 1, \alpha_{i+1}, \dots, \alpha_n) = \varphi(1).\end{aligned}$$

Последнее означает, что  $\varphi(0) = 1$ , а  $\varphi(1) = 0$ , т. е.  $\varphi(x) = \bar{x}$ . Лемма доказана.

**Лемма 3.** Если  $f(x_1, \dots, x_n) \neq L$ , то из нее путем подстановки констант 0 и 1 и функций вида  $x$  и  $\bar{x}$ , а также, быть может, путем навешивания отрицания над  $f$ , можно получить функцию  $x_1 \& x_2$ .

**Доказательство.** Возьмем полином Жегалкина для  $f$ :

$$f(x_1, \dots, x_n) = \sum_{(i_1, \dots, i_s)} a_{i_1 \dots i_s} x_{i_1} \dots x_{i_s}.$$

В силу нелинейности полинома в нем найдется член, содержащий не менее двух множителей. Без ограничения общности можно считать, что среди этих множителей присутствуют  $x_1$  и  $x_2$ . Тогда можно преобразовать полином следующим образом:

$$\begin{aligned}\sum_{(i_1, \dots, i_s)} a_{i_1 \dots i_s} x_{i_1} \dots x_{i_s} &= x_1 x_2 f_1(x_3, \dots, x_n) + \\ &+ x_1 f_2(x_3, \dots, x_n) + x_2 f_3(x_3, \dots, x_n) + f_4(x_3, \dots, x_n),\end{aligned}$$

где в силу единственности полинома  $f_1(x_3, \dots, x_n) \neq 0$ .

Пусть  $\alpha_3, \dots, \alpha_n$  таковы, что  $f_1(\alpha_3, \dots, \alpha_n) = 1$ . Тогда

$$\varphi(x_1, x_2) = f(x_1, x_2, \alpha_3, \dots, \alpha_n) = x_1 x_2 + \alpha x_1 + \beta x_2 + \gamma,$$

где  $\alpha, \beta, \gamma$  — константы, равные 0 или 1. Рассмотрим функцию  $\psi(x_1, x_2)$ , получаемую из  $\varphi(x_1, x_2)$  следующим образом:

$$\psi(x_1, x_2) = \varphi(x_1 + \beta, x_2 + \alpha) + \alpha\beta + \gamma.$$

Очевидно, что

$$\begin{aligned} \varphi(x_1 + \beta, x_2 + \alpha) + \alpha\beta + \gamma &= \\ &= (x_1 + \beta)(x_2 + \alpha) + \alpha(x_1 + \beta) + \\ &\quad + \beta(x_2 + \alpha) + \gamma + \alpha\beta + \gamma = x_1 x_2. \end{aligned}$$

Следовательно,

$$\psi(x_1, x_2) = x_1 \& x_2.$$

Лемма доказана полностью.

В заключение заметим, что замкнутые классы  $T_0, T_1, S, M$  и  $L$  попарно различны, что видно из табл. 8, в которой знак  $+$  означает, что функция содержится в классе, а знак  $-$  обозначает противоположную ситуацию.

Т а б л и ц а 8

|           | $T_0$ | $T_1$ | $S$ | $M$ | $L$ |
|-----------|-------|-------|-----|-----|-----|
| 0         | +     | -     | -   | +   | +   |
| 1         | -     | +     | -   | +   | +   |
| $\bar{x}$ | -     | -     | +   | -   | +   |

Пусть  $\mathfrak{F} = \{f_1, f_2, \dots, f_n, \dots\}$  некоторая произвольная система булевых функций. Тогда справедлива следующая теорема Поста.

**Теорема 7 (о функциональной полноте).** Для того чтобы система функций  $\mathfrak{F}$  была полной, необходимо и достаточно, чтобы она целиком не содержалась ни в одном из пяти замкнутых классов  $T_0, T_1, S, M$  и  $L$ .

**Доказательство. Необходимость.** Пусть  $\mathfrak{F}$  полна, т. е.  $[\mathfrak{F}] = P_2$ . Допустим, что  $\mathfrak{F}$  содержится в одном из указанных классов — обозначим его через  $\mathfrak{K}$ , т. е.  $\mathfrak{F} \subseteq \mathfrak{K}$ . Тогда в силу свойств замыкания и замкнутости  $\mathfrak{K}$  имеем

$$P_2 = [\mathfrak{P}] \equiv [\mathfrak{N}] = \mathfrak{N}.$$

Значит  $\mathfrak{N} = P_2$ , что не так. Необходимость доказана.

**Достаточность.** Пусть  $\mathfrak{P}$  целиком не содержится ни в одном из пяти указанных классов. Тогда из  $\mathfrak{P}$  можно выделить подсистему  $\mathfrak{P}'$ , содержащую не более пяти функций, которая также обладает этим свойством. Для этого возьмем в  $\mathfrak{P}$  функции  $f_i, f_j, f_k, f_m, f_l$ , которые не принадлежат соответственно классам  $T_0, T_1, S, M$  и  $L$ , и положим

$$\mathfrak{P}' = \{f_i, f_j, f_k, f_l, f_m\}.$$

Можно считать, что все эти функции зависят от одних и тех же переменных  $x_1, \dots, x_n$  (см. замечание из § 1).

Доказательство достаточности будем проводить в три этапа.

I. Построение при помощи функций  $f_i, f_j$  и  $f_k$  констант 0 и 1.

Рассмотрим функцию  $f_i \notin T_0$ . Возможны два случая:

1.  $f_i(1, \dots, 1) = 1$ . Тогда  $\varphi(x) = f_i(x, \dots, x)$  есть константа 1, ибо

$$\varphi(0) = f_i(0, \dots, 0) = 1, \quad \varphi(1) = f_i(1, \dots, 1) = 1.$$

Вторая константа получается из  $f_j$ :  $f_j(1, \dots, 1) = 0$ .

2.  $f_i(1, \dots, 1) = 0$ . Тогда  $\varphi(x) = f_i(x, \dots, x)$  есть  $\bar{x}$ , ибо

$$\varphi(0) = f_i(0, \dots, 0) = 1, \quad \varphi(1) = f_i(1, \dots, 1) = 0.$$

Возьмем  $f_k$  ( $f_k \notin S$ ). Так как мы имеем  $\bar{x}$ , то в силу леммы 1 из  $f_k$  мы можем получить константу. Поскольку мы располагаем  $\bar{x}$ , то находим и вторую константу. Итак, в обоих случаях мы получаем константы 0 и 1.

II. Построение при помощи констант 0, 1 и функции  $f_m$  функции  $\bar{x}$ . Это осуществляется на основе леммы 2.

III. Построение при помощи констант 0, 1 и функций  $\bar{x}$  и  $f_l$  функции  $x_1$  &  $x_2$ . Это осуществляется на основе леммы 3.

Таким образом, мы при помощи формул над  $\mathfrak{P}'$  (а значит и над  $\mathfrak{P}$ ) реализовали функции  $\bar{x}$  и  $x_1$  &  $x_2$ . Этим достаточность доказана.

**Следствие 1.** *Всякий замкнутый класс  $\mathfrak{M}$  функций из  $P_2$  такой, что  $\mathfrak{M} \neq P_2$ , содержится по крайней мере в одном из построенных классов.*

**Определение.** Класс  $\mathfrak{M}$  функций из  $P_2$  называется *предполным* (или *максимальным*), если  $\mathfrak{M}$  неполный, а для любой функции  $f (f \in P_2, f \notin \mathfrak{M})$  класс  $\mathfrak{M} \cup \{f\}$  — полный.

Из определения следует, что предполный класс является замкнутым.

**Следствие 2.** В алгебре логики существует только пять предполных классов, а именно:  $T_0$ ,  $T_1$ ,  $S$ ,  $M$  и  $L$ .

**Теорема 8.** Из всякой полной в  $P_2$  системы  $\mathfrak{F}$  функций можно выделить полную подсистему, содержащую не более четырех функций.

**Доказательство.** Мы видели, что из  $\mathfrak{F}$  можно выделить полную подсистему  $\mathfrak{F}'$ , содержащую не более пяти функций. Оказывается, что функция  $f_i \notin T_0$ , кроме того, либо не самодвойственна (случай 1), так как  $f_i(0, \dots, 0) = f_i(1, \dots, 1)$ , либо не сохраняет 1 и не монотонна (случай 2):  $f_i(0, \dots, 0) > f_i(1, \dots, 1)$ . Поэтому полной будет либо система  $\{f_i, f_j, f_m, f_l\}$ , либо система  $\{f_i, f_k, f_l\}$ .

### 1.7.8. Упражнение.

**1.12.** Сведением к заведомо полным системам в  $P_2$  показать, что множество  $A$  является полной системой в  $P_2$ :

- 1)  $A = \{x \downarrow y\}$ ; 2)  $A = \{xy \oplus z, (x \sim y) \oplus z\}$ ;
- 3)  $A = \{x \rightarrow y, \overline{x \oplus y \oplus z}\}$ ; 4)  $A = (x \rightarrow y, f = (01011110))$ ;
- 5)  $A = \{0, m(\tilde{x}^3) = x_1x_2 \vee x_2x_3 \vee x_3x_1, x \oplus y \oplus 1\}$ ;
- 6)  $A = \{x \sim y, x \oplus y, xy \oplus z\}$ ; 7)  $A = \{xy \vee \overline{xz}, f = (01111110)\}$ ;
- 8)  $A = \{xy \oplus zt \oplus 1, f = (10110110)\}$ ;
- 9)  $A = \{0, 1, x \oplus y \oplus z, xy \oplus zx \oplus zy\}$ ; 10)  $A = \{\overline{x} \overline{y} \vee z, x \oplus y\}$ .

### 1.7.9. Упражнение.

Выяснить, является ли функция  $f$  самодвойственной:

а)

- 1)  $f = x_1x_2 \vee x_2x_3 \vee x_3x_1$ ; 2)  $f = x_1 \vee x_2$ ; 3)  $f = x_1 \oplus x_2 \oplus x_3 \oplus 1$ ;
- 4)  $f = (x \vee \overline{y} \vee z)t \vee x\overline{y}z$ ; 5)  $f = (x \vee \overline{y} \vee z)t \vee xyz$ ;
- 6)  $f = (x_1 \rightarrow x_2)$ ; 7)  $f(x_1 \oplus x_2)$ ;
- 8)  $f = x_1x_2 \oplus x_2x_3 \oplus x_3x_1 \oplus x_2 \oplus x_3$ ; 9)  $f = x_1x_2 \vee x_3$ ;
- 10)  $f = x_1 \oplus x_2 \oplus (x_1x_2 \vee x_2x_3 \vee x_3x_1)$ ; 11)  $f = x_1x_2 \oplus x_3(x_1 \vee x_2)$ ;
- 12)  $f = x_1x_2x_3 \oplus x_1x_2 \oplus x_2x_3 \oplus x_3x_1$ ;
- 13)  $f = x_1x_2x_3 \oplus x_1x_2\overline{x}_3 \oplus x_2x_3 \oplus x_1x_3$ ;
- 14)  $f = (x_1 \rightarrow x_2) \oplus (x_2 \rightarrow x_3) \oplus (x_3 \rightarrow x_1) \oplus x_3$ ;
- 15)  $f = (x_1 \rightarrow x_2) \oplus (x_2 \rightarrow x_3) \oplus (x_2 \rightarrow x_1)$ .

б)

- 1)  $\tilde{\alpha}_f = (1010)$ ; 2)  $\tilde{\alpha}_f = (1001)$ ; 3)  $\tilde{\alpha}_f = (10010110)$ ;
- 4)  $\tilde{\alpha}_f = (01100110)$ ; 5)  $\tilde{\alpha}_f = (01110001)$ ; 6)  $\tilde{\alpha}_f = (01001101)$ ;
- 7)  $\tilde{\alpha}_f = (1100\ 1001\ 0110\ 1100)$ ; 8)  $\tilde{\alpha}_f = (1110\ 0111\ 0001\ 1000)$ ;
- 9)  $\tilde{\alpha}_f = (1000\ 0011\ 1000\ 1100)$ ; 10)  $\tilde{\alpha}_f = (1001\ 1011\ 1011\ 1001)$ ;
- 11)  $\tilde{\alpha}_f = (1100\ 0011\ 1010\ 0101)$ ; 12)  $\tilde{\alpha}_f = (1100\ 0011\ 0011\ 1100)$ ;
- 13)  $\tilde{\alpha}_f = (1001\ 0110\ 1001\ 0110)$ ; 14)  $\tilde{\alpha}_f = (1101\ 0100\ 1011\ 0010)$ ;
- 15)  $\tilde{\alpha}_f = (1010\ 0101\ 0101\ 1010)$ .

**1.7.10. Упражнение** Выяснить, является ли функция  $f$  линейной, представив её в виде полинома Жегалкина.

а)

- 1)  $f = x \rightarrow y$ ; 2)  $f = \overline{x \rightarrow y} \oplus \overline{xy}$ ; 3)  $f = x\overline{y}(x \sim y)$ ;
- 4)  $f = xy \vee \overline{x}\overline{y} \vee z$ ; 5)  $f = (xy \vee \overline{x}\overline{y})z \vee \overline{z}(x\overline{y} \vee \overline{x}y)$ ;
- 6)  $f = ((x \rightarrow y)(y \rightarrow x)) \sim z$ ; 7)  $f = xy\overline{z} \vee x\overline{y}$ ;
- 8)  $f = xyz \oplus xy\overline{z} \oplus \overline{x}y$ ; 9)  $f = m(x, y, z) \oplus \overline{x}\overline{y}\overline{z} \oplus xyz$ ;
- 10)  $f = (x \vee yz) \oplus xyz$ ; 11)  $f = (x \vee yz) \oplus \overline{x}yz$ ;
- 12)  $f = (xyz \vee x\overline{y}\overline{z}) \oplus x(y \oplus z)$ ; 13)  $f = xyz \oplus x(\overline{y}\overline{z}) \oplus x(y \vee z)$ ;
- 14)  $f = (xyz \oplus z\overline{x}\overline{y}) \vee (x\overline{y}z \oplus \overline{x}yz)$ ;
- 15)  $f = (\overline{x}\overline{y}\overline{z} \sim xy\overline{z}) \sim (x\overline{y}z \sim \overline{x}yz)$ .

б)

- 1)  $\tilde{\alpha}_f = (1001)$ ; 2)  $\tilde{\alpha}_f = (1101)$ ; 3)  $\tilde{\alpha}_f = (1001\ 0110)$ ;
- 4)  $\tilde{\alpha}_f = (1100\ 0011)$ ; 5)  $\tilde{\alpha}_f = (1010\ 0101)$ ; 6)  $\tilde{\alpha}_f = (1010\ 0110)$ ;
- 7)  $\tilde{\alpha}_f = (1100\ 1001\ 0110\ 1001)$ ; 8)  $\tilde{\alpha}_f = (0110\ 1001)$ ;
- 9)  $\tilde{\alpha}_f = (1001\ 0110\ 0110\ 1001)$ ; 10)  $\tilde{\alpha}_f = (0110\ 1001\ 0110\ 1001)$ ;
- 11)  $\tilde{\alpha}_f = (1010\ 0101\ 1001\ 1100)$ ; 12)  $\tilde{\alpha}_f = (1010\ 0101\ 0101\ 1010)$ ;
- 13)  $\tilde{\alpha}_f = (1010\ 0110\ 0110\ 0101)$ ; 14)  $\tilde{\alpha}_f = (0011\ 1100\ 1100\ 0011)$ ;
- 15)  $\tilde{\alpha}_f = (1001\ 1001\ 0110\ 0110)$ .

**1.7.11. Упражнение** Проверить, является ли функция  $f$  монотонной.

а)

- 1)  $\tilde{\alpha}_f = (0110)$ ; 2)  $\tilde{\alpha}_f = (0011\ 0111)$ ; 3)  $\tilde{\alpha}_f = (0101\ 0111)$ ;
- 4)  $\tilde{\alpha}_f = (0110\ 0110)$ ; 5)  $\tilde{\alpha}_f = (0001\ 0111)$ ; 6)  $\tilde{\alpha}_f = (0101\ 0011)$ ;
- 7)  $\tilde{\alpha}_f = (0010\ 0011\ 0111\ 1111)$ ; 8)  $\tilde{\alpha}_f = (0001\ 0101\ 0111\ 0111)$ .

б)

- 1)  $f = (x_1 \oplus x_2) \& (x_1 \sim x_2)$ ; 2)  $f = x_1 \rightarrow (x_2 \rightarrow x_1)$ ;
- 3)  $f = x_1 \rightarrow (x_1 \rightarrow x_2)$ ;
- 4)  $f = x_1\overline{x}_2\overline{x}_3 \vee x_1\overline{x}_2x_3 \vee x_1x_2\overline{x}_3 \vee x_1x_2x_3 \vee \overline{x}_1x_2x_3$ ;
- 5)  $f = x_1\overline{x}_2\overline{x}_3 \vee \overline{x}_1x_2x_3 \vee x_1x_2\overline{x}_3 \vee x_1x_2x_3 \vee \overline{x}_1\overline{x}_2x_3$ ;
- 6)  $f = (x_1 \oplus x_2)x_1x_2$ ; 7)  $f = x_1x_2 \oplus x_1x_3 \oplus x_3x_1$ ;
- 8)  $f = x_1x_2 \oplus x_2x_3 \oplus x_3x_1 \oplus x_1$ .

в)

- 1)  $f = x_1 x_2 x_3 \vee \bar{x}_1 x_2$ ; 2)  $f = x_1 \oplus x_2 \oplus x_3$ ; 3)  $f = x_1 x_2 \oplus x_3$ ;
- 4)  $f = x_1 \vee x_2 \bar{x}_3$ ; 5)  $f = x_1 x_3 \oplus x_2 x_4$ ;
- 6)  $f = (x_1 x_2 x_4 \rightarrow x_2 x_3) \oplus x_4$ .

**1.7.12. Упражнение** Выяснить, является ли система функций полной по теореме Поста.

а)

- 1)  $A = \{xy, x \vee y, x \oplus y, xy \vee yz \vee zx\}$ ;
- 2)  $A = \{xy, x \vee y, x \oplus y \oplus z \oplus 1\}$ ;
- 3)  $A = \{1, \bar{x}, x(y \sim z) \oplus \bar{x}(y \oplus z), x \sim y\}$ ;
- 4)  $A = \{0, \bar{x}, x(y \oplus z) \oplus yz\}$ ;
- 5)  $A = \{\bar{x}, x(y \sim z) \sim (y \vee z), x \oplus y \oplus z\}$ ;
- 6)  $A = \{\bar{x}, x(y \sim z) \sim yz, x \oplus y \oplus z\}$ ;
- 7)  $A = \{xy(x \oplus y), xy \oplus x \oplus y, 1, xy \oplus yz \oplus zx\}$ ;
- 8)  $A = \{xy(x \oplus z), 1\}$ ; 9)  $A = \{x \rightarrow y, \bar{x} \rightarrow \bar{y}x, x \oplus y \oplus z, 1\}$ ;
- 10)  $A = \{x \rightarrow y, x \oplus y\}$ .

б)

- 1)  $A = \{f_1 = (0110), f_2 = (1100\ 0011), f_3 = (1001\ 0110)\}$ ;
- 2)  $A = \{f_1 = (0111), f_2 = (0101\ 1010), f_3 = (0111\ 1110)\}$ ;
- 3)  $A = \{f_1 = (0111), f_2 = (1001\ 0110)\}$ ;
- 4)  $A = \{f_1 = (0101), f_2 = (1110\ 1000), f_3 = (0110\ 1001)\}$ ;
- 5)  $A = \{f_1 = (1001), f_2 = (1110\ 1000)\}$ ;
- 6)  $A = \{f_1 = (11), f_2 = (0111), f_3 = (0011\ 0111)\}$ ;
- 7)  $A = \{f_1 = (10), f_2 = (0011\ 0111)\}$ ;
- 8)  $A = \{f_1 = (11), f_2 = (00), f_3 = (0011\ 0101)\}$ ;
- 9)  $A = \{f_1 = (1000\ 0001), f_2 = (0111), f_3 = (1011)\}$ ;
- 10)  $A = \{f_1 = (1000\ 0001), f_2 = (0110), f_3 = (1001)\}$ .

### 1.7.13. Упражнение

а) проверить, является ли система базисом в  $P_2$ .

- 1)  $A = \{x \rightarrow y, x \oplus y, x \vee y\}$ ; 2)  $A = \{x \oplus y \oplus z, x \vee y, 0, 1\}$ ;
- 3)  $A = \{x \oplus y \oplus yz, x \oplus y \oplus 1\}$ ; 4)  $A = \{xy \vee z, xy \oplus z, xy \sim z\}$ ;
- 5)  $A = \{x \oplus y \oplus z, x \oplus y \oplus z \oplus 1, xy \oplus yz \oplus zx, \bar{x}\}$ ;
- 6)  $A = \{x \oplus y \oplus z, xy \oplus zx \oplus zy, 0, 1\}$ ; 7)  $A = \{x \oplus y, x \sim yz\}$ ;
- 8)  $A = \{xy \oplus yz \oplus zt, 0, 1, x \vee y\}$ .

б) из полной системы выделить все возможные базисы.

- 1)  $A = \{1, \bar{x}, xy(x \oplus y), x \oplus y \oplus xy \oplus yz \oplus zx\}$ ;
- 2)  $A = \{0, x \oplus y, x \rightarrow y, xy \sim xz\}$ ;
- 3)  $A = \{0, 1, x \oplus y \oplus z, xy \oplus zx \oplus yz, xy \oplus z, x \vee y\}$ ;
- 4)  $A = \{xy, x \vee y, xy \vee z, x \oplus y, x \rightarrow y\}$ ;

- 5)  $A = \{xy \oplus z, x \oplus y \oplus 1, x\bar{y}, \bar{x}\};$   
 6)  $A = \{xy \vee \bar{z}, \bar{x}, x \rightarrow y, 0, x \oplus zy\};$   
 7)  $A = \{xy, xy \vee z, x \oplus y, x \rightarrow y, \bar{x}\};$   
 8)  $A = \{x \oplus y, x \sim y, x \oplus y \oplus z, xy, x \rightarrow y\}.$

## 2. Логика предикатов

### 2.1. Язык прикладной логики предикатов

#### 2.1.1. Элементы языка прикладной логики предикатов.

♣ Рассмотрим предикат

$$x^2 < y. \quad (1)$$

Он не содержит логических связок, поэтому его формальная запись в языке логики высказываний состоит из одной буквы, например,  $P$ .

♦ В языке логики предикатов (точнее, *чистой* логики предикатов) должны быть выявлены все переменные, входящие в предикат, и какой-нибудь буквой обозначено *отношение* между ними, выражаемое этим предикатом:  $P \models A(x, y)$ .

♣ В данном случае буквой  $A$  обозначено следующее *свойство* объектов  $x$  и  $y$  (или *отношение* между ними): квадрат первого меньше второго (предполагается, что  $x$  и  $y$  – вещественные числа).

♦ Часто мы будем пользоваться более богатым языком *прикладной* логики предикатов, который отличается от обычного математического языка только более жесткими *синтаксическими* требованиями. Именно, в нем должны быть четко выделены следующие элементы.

– *Константы* – имена индивидуальных предметов. ♣ В (1) это 2.

– *Переменные* – имена неопределенных предметов, конкретные значения которых выбираются в единой для всех переменных *предметной области*  $D$ .

♣ В (1) переменными являются буквы  $x, y$  с предметной областью  $D = \mathbf{R}$ .

– *Функциональные знаки*, с помощью которых из *простых выражений* (констант и переменных) образуются *сложные*. ♣ В (1) единственная функция возведения в квадрат  $x^2$  изображена, как обычно, взаимным расположением аргумента  $x$  и параметра 2. Для табличного анализа умозаключений в прикладной логике предикатов удобно для каждой функции использовать явный функциональный знак. Например, выражение  $x^2$  можно записать в виде  $x \uparrow 2$ . В логике выражения чаще называются *термами* от английского “term” – член. Мы будем употреблять более традиционный для математики термин “выражение”.

– *Знаки отношений (свойств)*. ♣ В (1) единственным знаком отношения является “ $<$ ”. Отношения и функции могут зависеть от любого числа *предметных* (т.е. принимающих значения в  $D$ ) переменных. Единственным формальным отличием функции от отношения является то, что значения функции лежат в  $D$ ,



а значения отношения – в двухэлементном множестве булевских констант  $\mathbf{B} = \{u, l\}$ . Отношение от  $n$  переменных, примененное к  $n$  выражениям, образует *простой предикат*. Сложные предикаты строятся из простых с помощью логических операций.

– Логические связки  $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ .

– Кванторы  $\forall, \exists$ , которые подробно описываются ниже.

– Скобки, определяющие порядок образования сложных выражений и предикатов.

### 2.1.2. Кванторы. Свободные и связанные переменные.

♦ Из простого предиката (1) можно получить следующие более сложные предложения.

Существует  $x$ , для которого справедливо (1) –  $\exists(x)[x^2 < y]$ . (2)

Для любого  $y$  выполнено (1) –  $\forall(y)[x^2 < y]$ . (3)

Существует такое  $y$ , что для любого  $x$  выполнено (1) –  $\exists(y)\forall(x)[(1)]$ . (4)

Для любого  $x$  существует такое  $y$ , что выполнено (1) –  $\forall(x)\exists(y)[(1)]$ . (5)

♣ Знаки  $\forall$  и  $\exists$  происходят от английских слов All (все) и Exist (существовать) и называются *кванторами общности* и *существования*, соответственно. Термин “квантор” образован от латинского “quantum” – сколько. Кванторы указывают, для какого количества (для всех или хотя бы для одного) значений переменной справедливо данное утверждение.

♦ Истинность предложения (2), как нетрудно видеть, зависит только от выбора значения переменной  $y$ : при  $y \leq 0$  оно ложно, а при остальных значениях истинно. Поэтому говорят, что применение квантора по какой-нибудь переменной превращает эту переменную в *связанную*, от конкретных значений которой истинность утверждения уже не зависит. В (2) имеются два *вхождения* переменной  $x$ , которые связаны квантором существования, и одна *свободная* переменная  $y$ . Аналогично, в (3) два вхождения переменной  $y$  связаны квантором общности, а единственное вхождение переменной  $x$  свободно; утверждение ложно при всех значениях  $x$ . В (4) и (5) все переменные связаны; высказывание (4) ложно, а (5) истинно. Последнее обстоятельство следует подчеркнуть особо: *перестановка разноименных кванторов может существенно изменить предложение*.

### 2.1.3. Основные свойства кванторов.

• Формальное описание кванторов и действий с ними дают следующие четыре правила.

*Правила общности*

$$[\forall(x)A(x)] = u \models A(c) = u \quad (\forall u),$$

$(\forall l),$

$$[\exists(x)A(x)] = l \models A(c) = l \quad (\exists l),$$

*Правила существования*

$$[\forall(x)A(x)] = l \approx A(n) = l$$

$$[\exists(x)A(x)] = u \approx A(n) = u \quad (\exists u).$$

В правилах общности присутствует *произвольная* константа  $c$ , а в правилах существования утверждается только *существование* константы  $n$ , для которой справедлива правая часть.

♣Правило  $(\forall i)$  аналогично известному свойству конъюнкции: если конъюнкция двух или нескольких предикатов истинна, то истинны все ее операнды. Для квантора в роли операндов выступают высказывания, получающиеся из  $A(x)$  при всевозможных значениях  $x$ ; их может быть бесконечно много. Правило  $(\exists l)$  есть обобщение свойства дизъюнкции: если дизъюнкция ложна, то ложны все ее операнды.

♦ В правилах существования мы использовали нетрадиционный знак  $|\approx$ , которому мы придаем следующий смысл: если выполнено то, что написано слева от него, то можно ввести в рассмотрение *новую* (т.е. не участвовавшую ранее в данном рассуждении) константу  $n$ , для которой верно написанное справа от этого знака. ♣Например, если доказано, что уравнение  $f(x)=0$  имеет хотя бы одно решение, т.е.  $\exists(x)[f(x)=0]$ , то можно обозначить новой для данного рассуждения буквой  $n$  одно из его решений (без уточнения того, какое это именно решение) и в дальнейшем пользоваться истинным утверждением  $f(n)=0$ . Аналогично, если известно, что утверждение  $\forall(x)[f(x)=0]$  ложно, то можно ввести новую константу  $n$ , для которой  $f(n) \neq 0$ .

#### 2.1.4. Ограниченные кванторы.

♣Как уже отмечалось, в логике предикатов действует соглашение о том, что все предметные переменные имеют одну и ту же область изменения  $D$ . В математических теориях часто рассматриваются объекты различной природы: числа, множества, функции и т.п. Все они составляют единую предметную область  $D$ , а если некоторый квантор должен относиться только к части этой области, то на переменную, по которой он применяется, накладывают *ограничение*. Пример:

$$\forall(\varepsilon : \varepsilon > 0) \exists(n : n \in \mathbf{N}) \left[ \frac{1}{n} < \varepsilon \right]. \quad (6)$$

♦ Ограниченные кванторы не являются новыми логическими операциями; они сводятся к обычным кванторам с помощью следующих определений:

$$\begin{aligned} \forall(x : A(x)) B(x) &\overset{\text{опр}}{\leftrightarrow} \forall(x) [A(x) \rightarrow B(x)] , \\ \exists(x : A(x)) B(x) &\overset{\text{опр}}{\leftrightarrow} \exists(x) [A(x) \wedge B(x)] . \end{aligned}$$

♣Например, утверждение (6) в обычных кванторах принимает вид

$$\forall(\varepsilon) [\varepsilon > 0 \rightarrow \exists(n) [n \in \mathbf{N} \wedge \frac{1}{n} < \varepsilon]].$$

**2.1.5. Упражнение.** Записать данные формулы на обычном языке и определить, истинны ли они в теории.

1.  $\exists(x : x \in \mathbf{R}) \forall(n : n \in \mathbf{N}) [n > x]$ .

2.  $\forall(a : a \in \mathbf{R}) \exists(x : x \in \mathbf{R}) [ax + 1 = 0]$ .

3.  $\forall(a : a \in \mathbf{R} \wedge \neg a = 0)[\exists(x : x \in \mathbf{R})[ax + 1 > 0] \wedge \exists(x : x \in \mathbf{R})[ax + 1 < 0]]$ .
4.  $\exists(a : a \in \mathbf{R})\forall(x : x \in \mathbf{R})[ax + 1 > 0]$ .
5.  $\forall(a \in \mathbf{R})[\exists(x \in \mathbf{R})[ax + 1 > 0] \rightarrow \exists(y \in \mathbf{R})[ay + 1 < 0]]$ .
6.  $\exists(c \in \mathbf{R})[\neg \forall(x \in \mathbf{R})[x^2 + x + c > 0]]$ .
7.  $\forall(a \in \mathbf{R} : a \geq 0)\exists(x \in \mathbf{R})[ax^2 + x + 1 > 0]$ .
8.  $\forall(a, b, c \in \mathbf{R})[b^2 < 4ac \rightarrow \exists(x_1, x_2)[ax_1^2 + bx_1 + c = 0 \wedge ax_2^2 + bx_2 + c = 0 \wedge x_1 \neq x_2]]$ .
9.  $\forall(a \in \mathbf{R})\exists(x \in \mathbf{R})\forall(c \in \mathbf{R})[ax^2 + x + c^2 > 0]$ .
10.  $\exists(a \in \mathbf{R})\forall(c \in \mathbf{R})\exists(x \in \mathbf{R})[ax^2 + x + c > 0]$ .

### 2.1.6. Пример формализации в языке прикладной логики предикатов.

♣ Дополнения к процессу формализации, рассмотренному в 1.2.4 и 1.2.6, которые вносят такие формы предложений, как “Для любого... выполнено...” и “Существует..., для которого выполнено...” рассмотрим на следующем примере.

♣ Для любых вещественных  $a, b, c$  верно, что если  $ac < 0$ , то  $ax^2 + bx + c < 0$  при некотором вещественном  $x$ .

Очевидно, утверждение “ $ax^2 + bx + c < 0$  при некотором вещественном  $x$ ” можно без изменения смысла и логической формы преобразовать в “Существует вещественное  $x$ , для которого  $ax^2 + bx + c < 0$ ”. Теперь перевод на язык прикладной логики предикатов дает формулу

$$\forall(a : a \in \mathbf{R})\forall(b : b \in \mathbf{R})\forall(c : c \in \mathbf{R})[ac < 0 \rightarrow \exists(x : x \in \mathbf{R})[ax^2 + bx + c < 0]]. \quad (7)$$

Группу следующих друг за другом *одноименных* кванторов часто записывают в виде одного квантора по нескольким переменным. Кроме того, если это не может вызвать недоразумений, в круглых скобках рядом с квантором не указывают отдельно имя переменной, а пишут сразу предикат, ограничивающий ее значения:

$$\forall(a \in \mathbf{R}, b \in \mathbf{R}, c \in \mathbf{R})[ac < 0 \rightarrow \exists(x \in \mathbf{R})[ax^2 + bx + c < 0]]. \quad (8)$$

**2.1.7. Упражнение.** Формализовать данный предикат в языке прикладной логики предикатов. Определить, является ли он истинным.

1. Неравенство  $x^2 \geq 0$  справедливо для любого действительного  $x$ .
2. Найдется хотя бы одно действительное число  $x$ , для которого  $-x^2 + x + 1 < 0$ , и хотя бы одно действительное  $x$ , для которого  $-x^2 + x + 1 > 0$ .
3. Существует вещественное  $M$ , такое, что  $(n+1)/n \leq M$  для любого целого  $n \neq 0$ .
4. Не существует натурального  $N$ , которое больше любого вещественного  $x$ .
5. Для любых двух вещественных чисел  $x$  и  $y$ , удовлетворяющих неравенству  $x < y$ , найдется рациональное  $q$ , такое, что  $x < q < y$ .
6. Для любого отрицательного  $a$  имеется действительное значение  $x$ , для которого  $ax^2 + x + 1 < 0$ .

7. Для любых  $a > 0, M > 0$  существуют как положительное, так и отрицательное значения  $x$ , при которых  $ax^2 + x + 1 > M$ .
8. Для любого положительного  $\varepsilon$  существует натуральное  $N$ , такое, что  $\frac{1}{n} < \varepsilon$  при  $n \geq N$ .
9. Существуют целые числа, которые не делятся ни на какие натуральные числа, кроме 1 и модуля самого себя.
10. Для любых вещественных чисел  $x$  и  $y$  выполнено одно и только одно из соотношений  $x < y, x = y, x > y$ .

## 2.2. Следствие в прикладной логике предикатов

В этом параграфе мы распространим направленную табличную процедуру проверки логического следствия на формулы прикладной логики предикатов.

### 2.2.1. Применение правил общности.

♣ В приводимом ниже примере первые три шага обычны: посылкам присвоено значение “и”, заключению – “л”. На шаге 4 связанной переменной  $x$  присвоено значение  $a$ , а на пятом шаге применено правило общности ( $\forall u$ ) – истинностное значение перенесено с квантора на предикат. Шестой шаг следует из второго. На седьмом шаге получилось противоречие с шагом 3, поскольку во всей области действия квантора общности по  $x$  этой переменной присвоено значение  $a$ . Значения, присваиваемые связанным переменным, можно произвольно выбирать из ♦ *предметной области данного набора формул*, т.е. множества всех участвующих в них констант и свободных переменных, дополненного бесконечным множеством *стандартных констант*  $\{c_0, c_1, c_2, \dots\}$ .

$$\forall (x) [x < 0 \rightarrow x + 1 < 1], a < 0 \stackrel{?}{=} a + 1 < 1$$

|     |     |     |     |               |     |               |
|-----|-----|-----|-----|---------------|-----|---------------|
| $u$ | $a$ | $u$ | $u$ | $u$           | $u$ | $\frac{l}{3}$ |
| 1   | 4   | 6   | 5   | $\frac{u}{7}$ | 2   | $\frac{l}{3}$ |

Отметим новые по сравнению с логикой высказываний элементы табличного доказательства.

- ♦ 1. Связанной переменной можно присвоить любое значение из предметной области данного набора формул одновременно во всей области действия квантора.
- ♦ 2. Если при этом получается ситуация общности (т.е. выполнено условие одного из правил общности), то можно перенести истинностное значение с квантора на предикат.

### 2.2.2. Обозначения сложных выражений. Ограниченные кванторы.

♣ В рассматриваемом ниже примере на четвертом шаге введено обозначение  $c_0$  для сложного выражения  $\sin y$ . Такие обозначения выбираются из бесконечного списка стандартных констант  $c_0, c_1, c_2, \dots$  с тем условием, что для *нового выражения* вводимая константа должна быть *новой*, т.е. не входить в данные фор-

мулы и в предыдущую часть данного табличного доказательства. На шаге 6 к ограниченному квантору общности применено правило общности ( $\forall u$ ). Над скобкой помещен знак импликации, которая входит в определение ограниченного квантора общности; именно на него переносится на шестом шаге истинностное значение с квантора  $\forall$ .

$$\forall (x: x \in \mathbf{R}) \rightarrow [x \uparrow 2 \geq 0], \sin y \in \mathbf{R} \stackrel{?}{=} (\sin y) \uparrow 2 \geq 0$$

|     |       |     |     |     |       |     |      |       |               |
|-----|-------|-----|-----|-----|-------|-----|------|-------|---------------|
| $u$ | $c_0$ | $u$ | $u$ | $u$ | $c_0$ | $u$ | $da$ | $c_0$ | $\frac{l}{3}$ |
| 1   | 5     | 7   | 6   | 8   | 4     | 2   |      | 9     | 3             |

К списку новых элементов табличных доказательств для логики предикатов присоединим следующие два.

♦ 3. Сложным выражениям можно приписывать обозначения из числа новых стандартных констант.

♦ 4. Ограниченные кванторы сводятся к неограниченным путем добавления над скобкой знака импликации в случае квантора общности и знака конъюнкции для квантора существования.

### 2.2.3. Пример с подстроками.

♣ В следующем примере после шага 10 строка продолжается по вертикали с переходом на шаге 11 к новой подстроке, в которой переменной  $x$  присваивается еще одно значение  $y$ .

$$\forall (x < 0) \rightarrow [x + 1 < 1], a < 0, y < 0 \models a + 1 < 1 \wedge y + 1 < 1$$

|     |     |     |     |     |     |     |     |     |                |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|----------------|
| $u$ | $a$ | $u$ | $u$ | $u$ | $u$ | $u$ | $u$ | $l$ | $\frac{l}{10}$ |
| 1   | 5   | 7   | 6   | 8   | 2   | 3   |     | 9   | 4              |
|     |     | $y$ | $u$ | $u$ |     |     |     |     |                |
|     |     | 11  | 13  | 12  |     |     |     |     | 14             |

К списку новых элементов мы присоединим следующий.

♦ 5. Если по ходу табличного доказательства требуется связанной переменной присвоить последовательно несколько различных значений, то это делается в различных подстроках одной строки.

### 2.2.4. Применение правил существования.

♣ В следующем доказательстве на шаге 4 связанной переменной присвоено новое (не встречавшееся ранее в этой таблице) постоянное значение, поэтому в силу правила существования ( $\forall l$ ) значение “ $l$ ” перенесено с квантора на предикат (шаг 5).

$$\neg \exists (x \in \mathbf{R}) \wedge [\sin x > 1] \models \forall (x \in \mathbf{R}) \rightarrow [\neg \sin x > 1]$$

|     |     |       |     |     |                |      |     |       |     |     |     |               |
|-----|-----|-------|-----|-----|----------------|------|-----|-------|-----|-----|-----|---------------|
| $u$ | $l$ | $c_0$ | $u$ | $l$ | $\frac{l}{12}$ | $da$ | $l$ | $c_0$ | $u$ | $l$ | $l$ | $\frac{u}{8}$ |
| 1   | 3   | 9     | 11  | 10  | 12             |      | 2   | 4     | 6   | 5   | 7   | 8             |

♣ Отметим, что непосредственно после шага 3 была также возможность в левой части доказываемого утверждения воспользоваться правилом общности ( $\exists l$ ). Однако рациональнее, как это сделано, сначала применить правило существования в правой части, а затем – правило общности в левой. Иначе, как показано ниже, доказательство усложняется, так как на шаге 6 необходимо ввести новую константу, а затем её использовать на шаге 11.

$$\neg \exists (x \in \mathbf{R}) \wedge [\sin x > 1] \models \forall (x \in \mathbf{R}) \rightarrow [\neg \sin x > 1]$$

|     |     |       |  |     |  |      |     |       |     |     |     |  |                 |
|-----|-----|-------|--|-----|--|------|-----|-------|-----|-----|-----|--|-----------------|
| $u$ | $l$ | $c_0$ |  | $l$ |  | $да$ | $l$ | $c_1$ | $u$ | $l$ | $l$ |  | $u$             |
| 1   | 3   | 4     |  | 5   |  |      | 2   | 6     | 8   | 7   | 9   |  | $\overline{10}$ |

  

|       |     |     |  |                |
|-------|-----|-----|--|----------------|
| $c_1$ | $u$ | $l$ |  | $\overline{l}$ |
| 11    | 13  | 12  |  | 14             |

♦ 6. Если на некотором этапе табличной процедуры возможно применение правила общности и правила существования, то целесообразно начать с правила существования.

### 2.2.5. Обратное применение правил общности.

$$\exists (x) [x > 0 \wedge x < 1] \stackrel{?}{=} \exists (x) [x > 0] \wedge \exists (x) [x < 1]$$

|     |       |  |     |     |     |  |      |     |       |     |                |     |       |     |
|-----|-------|--|-----|-----|-----|--|------|-----|-------|-----|----------------|-----|-------|-----|
| $u$ | $c_0$ |  | $u$ | $u$ | $u$ |  | $да$ | $u$ | $c_0$ | $u$ | $\overline{l}$ | $u$ | $c_0$ | $u$ |
| 1   | 3     |  | 5   | 4   | 6   |  |      | 9   | 7     | 8   | 2              | 12  | 10    | 11  |

♣ После шага 2 можно было разветвить таблицу, так как конъюнкции присвоено значение «л». Но в данном случае имеется более прямой путь. На шагах 3, 4 применяется правило существования – вводится *новая* константа  $c_0$ . На шаге 7 сразу производится присваивание  $x = c_0$  с целью воспользоваться далее (шаг 8) результатом шага 5. Значение «и» на шаге 9 получено из 7 и 8 «обратным применением правила общности ( $\exists l$ )», поскольку значение «л» приводило бы к противоречию с этим правилом и шагом 8. Проведя аналогичные действия на шагах 10-12, мы получили противоречие между 12, 2 и 9. Отметим эту методику как ещё один новый элемент табличной процедуры.

♦ 7. Иногда удобно применять правила общности в следующем виде:

$$A(c) = u \models [\exists(x) A(x)] = u, \quad A(c) = l \models [\forall(x) A(x)] = l.$$

### 2.2.6. Равенство как логический предикат.

♦ Равенство  $x = y$  будем понимать как *тождество*, т. е. выражение того факта, что  $x$  и  $y$  – это имена одного и того же объекта. ♣ В математике равенство иногда понимается и в другом смысле; например, равенство двух векторов – это возможность добиться их полного совпадения путём параллельного переноса. Для табличной процедуры принятое понимание равенства выражается добавлением двух правил построения таблиц.

♦ 8. Если в таблице есть фрагмент вида  $\begin{smallmatrix} u = v \\ c \text{ и } c_1 \end{smallmatrix}$ , то всюду в дальнейшем в этой таблице можно выражению  $u$  присваивать значение  $c_1$ , а выражению  $v$  – значение  $c$ .

♦ 9. Фрагмент таблицы вида  $\begin{smallmatrix} u = v \\ c \text{ л } c \end{smallmatrix}$  можно отметить как противоречие,

или, что то же, фрагмент  $\begin{smallmatrix} u = v \\ c \text{ } c \end{smallmatrix}$  можно дополнить значением «и» под знаком равенства.

♣ В следующих двух примерах показано применение этих правил для доказательства утверждений, содержащих предикат равенства. Первый пример уста-

навливают *транзитивность* равенства, а второй – *взаимозаменяемость равных объектов*.

$$\models \forall (x, y, z) [x = y \wedge y = z \rightarrow x = z]$$

да л  $c_0$   $c_1$   $c_2$   $c_0$  и  $c_1$  и  $c_1$  и  $c_2$  л  $c_1$  л  $c_1$

1 2 3 4 8 6 9 5 10 7 11

$$\models \forall (x, y) [P(x) \wedge x = y \rightarrow P(y)]$$

да л  $c_0$   $c_1$  и  $c_0$  и  $c_0$  и  $c_1$  л  $c_1$  л  $c_0$

1 2 3 7 5 8 4 6 9

В первом примере на шагах 10 и 11 использовано правило 8, а противоречие отмечено по правилу 9. Во втором примере использовано только первое правило: оно позволило на шаге 9 присвоить переменной  $y$  значение  $c_0$ . В последнем примере предполагается, что предикат  $P(x)$  не содержит буквы  $y$ , иначе последовательная подстановка  $y$  вместо  $x$ , а затем  $c_0$  вместо  $y$  может дать результат, отличный от  $P(c_0)$ .

**2.2.7. Квантор существования и единственности.** ♦ Предикат равенства позволяет ввести часто используемый в математике *квантор существования и единственности*:

$$\exists!(x)P(x) \stackrel{\text{опр}}{=} \exists(x)P(x) \wedge \forall(x, y)[P(x) \wedge P(y) \rightarrow x = y].$$

♣ Например, он используется в следующем высказывании:

$$\forall(a \in \mathbf{R}, b \in \mathbf{R}) \exists!(x \in \mathbf{R})[a + x = b].$$

**2.2.8. Упражнение.** Доказать справедливость следующих логических соотношений.

1.  $\neg \exists(n \in \mathbf{N})[n + 1 < 1], (-1) + 1 < 1 \models \neg(-1 \in \mathbf{N})$ .
2.  $\forall(x \in \mathbf{R})[x^2 \geq 0], i^2 = -1, \neg(-1 \geq 0) \models \neg(i \in \mathbf{R})$ .
3.  $\forall(x \in \mathbf{R})[2x^2 + 1 > 0] \models \exists(n) \forall(x \in \mathbf{R})[nx^2 + 1 > 0]$ .
4.  $\forall(x: |x| \leq 1)[x \leq 1 \wedge -1 \leq x] \models \forall(x)[|x| \leq 1 \rightarrow x \leq 1] \wedge \forall(x)[\neg(-1 \leq x) \rightarrow \neg(|x| \leq 1)]$ .
5.  $\exists(d \in \mathbf{Z})[15: d \wedge (d: 2 \vee d: 3)] \models \exists(d: d: 2)[d \in \mathbf{Z} \wedge 15: d] \vee \exists(d: d \in \mathbf{Z} \wedge 15: d)[d: 3]$ .
6.  $\models \forall(x_1, x_2: x_1 < x_2)[f(x_1) < f(x_2)] \wedge e < \pi \rightarrow f(e) < f(\pi)$ .
7.  $\models \exists(q \in \mathbf{Q})[e < q \wedge q < \pi] \rightarrow \exists(q \in \mathbf{Q})[e < q] \wedge \exists(q < \pi)[q \in \mathbf{Q}]$ .
8.  $\models \forall(n)[n: 4 \rightarrow n: 2] \rightarrow \neg \exists(n: n: 4)[\neg n: 2]$ .
9.  $\forall(x \in (0, \pi))[\sin x > 0], u \in (0, \pi), \neg(\sin u > 0) \models$ .
10.  $\sin e > 0, e \in (0, \pi), \neg \exists(x: \sin x > 0)[x \in (0, \pi)] \models$ .

**2.2.9. Упражнение.** Формализовать и проверить.

1. Для любого  $x \in X$  справедливо неравенство  $x < n$ . Не существует такого  $m$ , чтобы для любого  $y \in Y$  выполнялось неравенство  $y < m$ . Следовательно, не любой элемент  $y \in Y$  принадлежит  $X$ .

2. Для любого  $n$  найдется  $x \in X$ , для которого не выполнено неравенство  $x < n$ . Неравенство  $y < t$  справедливо для каждого  $y \in Y$ . Следовательно, хотя бы один элемент множества  $X$  не принадлежит  $Y$ .

3. Для любого положительного  $\varepsilon$  существует натуральное  $n$ , такое, что  $n\varepsilon > 1$ . Не существует натурального  $n$ , для которого  $na > 1$ . Следовательно, неверно, что  $a$  положительно.

4. Существует натуральное  $n$ , такое, что  $x < n$  для любого  $x \in X$ . Для любого натурального  $m$  существует  $y \in Y$ , для которого не справедливо неравенство  $y < m$ . Следовательно, существует элемент  $y \in Y$ , который не принадлежит  $X$ .

### 2.3. Основные теоремы логики предикатов

Перечень наиболее употребительных соотношений логики предикатов мы представим в виде двух теорем.

#### 2.3.1. Теорема о кванторах, отрицании, конъюнкции и дизъюнкции.

• Пусть  $A, B, C$ , - произвольные предикаты,  $x$  и  $y$  - переменные,  $x_0$  - константа. Будем обозначать через  $A|_{x=y}$  результат замены в  $A$  всех свободных вхождений  $x$  на  $y$ . Утверждается, что справедливы следующие соотношения.

1) Правила переименования связанной переменной: если  $y$  не входит в  $A$  и  $B$  ни в связанном, ни в свободном виде, то

$$\forall(x:A)B \models \forall(y:A|_{x=y})B|_{x=y}, \quad (\forall xy)$$

$$\exists(x:A)B \models \exists(y:A|_{x=y})B|_{x=y}. \quad (\exists xy)$$

2) Правила удаления и введения кванторов:

$$\forall(x:A)B, A|_{x=x_0} \models B|_{x=x_0}, \quad (\forall - y\partial)$$

$$A|_{x=x_0}, B|_{x=x_0} \models \exists(x:A)B. \quad (\exists - \forall\partial)$$

3) Правила протаскивания кванторов через отрицание:

$$\neg\forall(x:A)B \models \exists(x:A)[\neg B], \quad (\neg\forall)$$

$$\neg\exists(x:A)B \models \forall(x:A)[\neg B]. \quad (\neg\exists)$$

4) Правила протаскивания кванторов через конъюнкцию:

$$\forall(x:A)[B \wedge C] \models \forall(x:A)B \wedge \forall(x:A)C, \quad (\forall \wedge)$$

$$\exists(x:A)[B \wedge C] \models \exists(x:A)B \wedge \exists(x:A)C; \quad (\exists \wedge \models)$$

если  $B$  или  $C$  не зависит от  $x$ , то

$$\exists(x:A)[B \wedge C] \models \exists(x:A)B \wedge \exists(x:A)C. \quad (\exists \wedge \models)$$

5) Правила протаскивания кванторов через дизъюнкцию:

$$\exists(x:A)[B \vee C] \models \exists(x:A)B \vee \exists(x:A)C, \quad (\exists \vee)$$

$$\forall(x:A)[B \vee C] \models \forall(x:A)B \vee \forall(x:A)C; \quad (\forall \vee \models)$$

если  $B$  или  $C$  не зависит от  $x$ , то



$$\forall(x:A)[B \vee C] \models \forall(x:A)B \vee \forall(x:A)C. \quad (\forall \vee \models)$$

♣ Условие, наложенное на  $y$  в  $(\forall xy)$  и  $(\exists xy)$ , существенно. Например, нарушение этого условия приводит к тому, что из верного для любого  $y$  предиката  $\exists(x:x \in \mathbf{Q})[x > y]$  получается ложное высказывание  $\exists(y:y \in \mathbf{Q})[y > y]$  и из истинного высказывания  $\forall(x:x \in \mathbf{R}) \exists(y:y \in \mathbf{R})[x > y]$  – ложное утверждение  $\forall(y:y \in \mathbf{R}) \exists(y:y \in \mathbf{R})[y > y]$ . ♣ Правила  $(\neg \forall)$ ,  $(\neg \exists)$  обобщают законы де Моргана. Они часто применяются в доказательствах от противного для переформулировки “отрицательных” утверждений в “позитивной” форме. Например, если мы предположили, что  $\neg \exists(M) \forall(n: n \in \mathbf{N})[a_n \leq M]$  (т.е. последовательность  $a$  не является ограниченной сверху), то мы можем переписать это предположение в эквивалентной *позитивной* форме:  $\forall(M) \exists(n: n \in \mathbf{N})[a_n > M]$  (здесь использована еще эквивалентность  $\neg(a_n \leq M) \Leftrightarrow a_n > M$ ). ♣ Все утверждения теоремы можно доказать с помощью табличной процедуры. Докажем, например,  $(\forall xy)$ ,  $(\exists \wedge \models)$  и  $(\exists \wedge \models)$ .

$$\begin{array}{l} \forall(x:A) \rightarrow B \models \forall(y:A|_{x=y}) \rightarrow B|_{x=y} \\ \heartsuit (\forall xy): \quad \begin{array}{cccccccc} u & c_1 & u & u & u & да & л & c_1 & u & л & л \\ 1 & 7 & 9 & 8 & 10 & 2 & 3 & 5 & 4 & 6 \end{array} \end{array}$$

Ограничение на переменную  $y$  использовано на шаге 9, так как без него результат последовательной подстановки  $A|_{x=y}|_{y=c_1}$  может не совпадать с результатом непосредственной подстановки  $A|_{x=c_1}$ . Например,  $(x < y)|_{x=y}|_{y=c_1}$  есть  $c_1 < c_1$ , а  $(x < y)|_{x=c_1}$  –  $c_1 < y$ . Это ограничение использовано и при выявлении противоречия между 6 и 10.

$$\begin{array}{l} \exists(x:A) \wedge [B \wedge C] \stackrel{?}{\models} \exists(x:A) \wedge B \wedge \exists(x:A) \wedge C \\ \heartsuit (\exists \wedge \models): \quad \begin{array}{cccccccc} u & c_0 & u & u & u & u & да & u & c_0 & u & u & л & u & c_0 & u & u & u \\ 1 & 3 & 5 & 4 & 7 & 6 & 8 & 13 & 9 & 10 & 12 & 11 & 2 & 18 & 14 & 15 & 17 & 16 \end{array} \end{array}$$

Тот факт, что левая часть не следует логически из правой, докажем с помощью смыслового контрпримера:  $A$  – “ $x \in \mathbf{N}$ ”,  $B$  – “ $x$  четно”,  $C$  – “ $x$  нечетно”. Очевидно, в такой интерпретации правая часть истинна, а левая ложна.

♥ В доказательстве  $(\exists \wedge \models)$  будем, для определенности, считать, что от  $x$  не зависит  $B$ . Ввиду  $(\exists \wedge \models)$  достаточно доказать только

$$\begin{array}{l} \exists(x:A) \wedge [B \wedge C] \stackrel{?}{\models} \exists(x:A) \wedge B \wedge \exists(x:A) \wedge C \\ (\exists \wedge \models): \quad \begin{array}{cccccccc} л & c_1 & u & л & u & л & у & да & u & c_0 & u & u & u & u & c_1 & u & u & u \\ 2 & 13 & 15 & 14 & 18 & 16 & 17 & 3 & 5 & 7 & 6 & 8 & 1 & 4 & 9 & 11 & 10 & 12 \end{array} \end{array}$$

Поскольку  $B|_{x=c_0} = u$  (шаг 8) и  $B$  не зависит от  $x$ , то и  $B|_{x=c_1} = u$  (шаг 18).

### 2.3.2. Теорема о кванторах и импликации.

• 1) Правила *пронесения* кванторов через импликацию:

$$\exists(x:A)[B \rightarrow C] \models \forall(x:A)B \rightarrow \exists(x:A)C ; \quad (\exists \rightarrow)$$

$$\forall(x:A)[B \rightarrow C] \stackrel{|\neq}{=} \exists(x:A)B \rightarrow \forall(x:A)C ; \quad (\forall \rightarrow \Rightarrow |)$$

если  $B$  или  $C$  не зависит от  $x$ , то

$$\forall(x:A)[B \rightarrow C] \models \exists(x:A)B \rightarrow \forall(x:A)C . \quad (\forall \rightarrow \models |)$$

• 2) Правила *пронесения* кванторов через кванторы: если  $A$  не содержит буквы  $y$ ,  $B$  – буквы  $x$ , а  $C$  может зависеть от  $x$  и  $y$ , то

$$\forall(x:A)\forall(y:B)C \models \forall(y:B)\forall(x:A)C ; \quad (\forall\forall)$$

$$\exists(x:A)\exists(y:B)C \models \exists(y:B)\exists(x:A)C ; \quad (\exists\exists)$$

$$\exists(x:A)\forall(y:B)C \stackrel{|\neq}{=} \forall(y:B)\exists(x:A)C . \quad (\exists\forall)$$

♥ Докажем  $(\forall \rightarrow \Rightarrow |)$  и  $(\forall \rightarrow \models |)$  с помощью *цепочки преобразований*.

$$\begin{aligned} \forall(x:A)[B \rightarrow C] \models \forall(x:A)[\neg B \vee C] &\stackrel{|\neq}{=} (| \models) \forall(x:A)[\neg B] \vee \forall(x:A)C \models \\ &\models \neg \exists(x:A)B \vee \forall(x:A)C \models \exists(x:A)B \rightarrow \forall(x:A)C . \end{aligned}$$

В преобразованиях последовательно использованы доказанные ранее утверждения: выражение  $\rightarrow$  через  $\neg$  и  $\vee$ , правило  $(\forall\vee \models |)$ , а если  $B$  или  $C$  не зависит от  $x$ , то  $(\forall\vee \models |)$ , правило  $(\neg\exists)$  и, наконец, вновь выражение  $\rightarrow$  через  $\neg$  и  $\vee$ , на этот раз в обратную сторону.

♣ В доказательствах цепочками преобразований применяется следующее свойство логической эквивалентности: • *если какую-нибудь часть формулы заменить на логически эквивалентную, то получится формула, логически эквивалентная данной.*

♥ Это верно, потому что в любой интерпретации логически эквивалентные формулы имеют одинаковые истинностные значения.

♥ Для доказательства утверждения " $\neq$ " в  $(\exists\forall)$  рассмотрим следующую интерпретацию:  $A$  – « $x \in \mathbf{R}$ »,  $B$  – « $y \in \mathbf{R}$ »,  $C$  – « $x < y$ ». В этой интерпретации, как нетрудно видеть, правая часть  $(\exists\forall)$  истинна, а левая ложна.

♥ Доказательство утверждения " $\models$ " в  $(\exists\forall)$  проведём с помощью табличной процедуры.

$$\begin{array}{cccccccccccccccc} \exists(x:A) \wedge \forall(y:B) \rightarrow C & \models & \forall(y:B) \rightarrow \exists(x:A) \wedge C \\ \text{и } c_0 & \text{и } \text{и } \text{и } c_1 & \text{и } \text{и } \underline{\text{и}} & \text{да} & \text{л} & c_1 & \text{и } \text{л} & \text{л} & c_0 & \text{и } \text{л} & \underline{\text{л}} \\ 1 & 3 & 5 & 4 & 6 & 15 & 17 & 16 & 18 & 2 & 7 & 9 & 8 & 10 & 11 & 13 & 12 & 14 \end{array}$$

**2.3.3. Упражнение.** Доказать остальные утверждения теорем 2.3.1 и 2.3.2.

## Литература

1. Лавров И.А., Максимова Л.Л. Задачи по теории множеств, математической логике и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. – М.: Физматлит, 2001. – 255 с.
2. Лексаченко В.А. Логика. Множества. Вероятность / В.А. Лексаченко. – М.: Вузовская книга, 2001. – 128 с.
3. Лихтарников Л.М., Сукачева Т.Г. Математическая логика: Курс лекций: Задачник – практикум и решения: Учеб. пособие / Л.М. Лихтарников, Т.Г. Сукачева. – СПб.: Лань, 1999. – 285 с.
4. Гладкий А.В. Математическая логика: Учеб. пособие / А.В. Гладкий. – М., 1998. – 479 с.
5. Петрова Л.П., Садовский Б.Н. Логика высказываний / Л.П. Петрова, Б.Н. Садовский. – Воронеж: ВГУ, 1989. – 24 с.
6. Петрова Л.П., Садовский Б.Н. Логика предикатов / Л.П. Петрова, Б.Н. Садовский. – Воронеж: ВГУ, 1989. – 18 с.
7. Ершов Ю.Л., Палютин Е.А. Математическая логика / Ю.Л. Ершов, Е.А.Палютин. – М.: Наука, 1979. – 320 с.
8. Мендельсон Э. Введение в математическую логику / Э. Мендельсон. – М.: Наука, 1976 – 320 с.
9. Шенфилд Дж. Математическая логика / Дж. Шенфилд. – М.: Наука, 1975. – 528 с.
10. Клини С. Математическая логика / С. Клини. – М.: Мир, 1973. – 480 с.
11. Столл Р.Р. Множества. Логика. Аксиоматические теории / Р.Р. Столл. – М.: Просвещение, 1968. – 230 с.
12. Новиков П.С. Элементы математической логики / П.С. Новиков. – М.: ГИФМЛ, 1959. – 400 с.