МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Факультет информационных технологий

Д. Е. Пальчунов

МАТЕМАТИЧЕСКАЯ ЛОГИКА И ТЕОРИЯ АЛГОРИТМОВ

ЧАСТЬ ПЕРВАЯ

Учебное пособие

Новосибирск
2016

УДК 510
ББК 22.12
П 146

Рецензент:
канд. физ.-мат. наук В. Н. Власов

Пальчунов, Д. Е.
П 146 Математическая логика и теория алгоритмов : учеб. пособие / Д. Е. Пальчунов ; Новосиб. гос. ун-т. – Новосибирск, 2016. – Ч. 1. – 96 с.

ISBN 978-5-4437-0547-7

В пособии излагаются основы теории множеств, математической логики и теории алгоритмов. Оно написано на основе лекционной и практической работы автора со студентами ФИТ НГУ. Цель пособия – ознакомить читателя с основными понятиями и начальными результатами по теории множеств, логике высказываний, логике предикатов, теории моделей, теории булевых алгебр, машинам Тьюринга и рекурсивным функциям.

Предназначено для студентов факультетов информационных технологий, математических, естественнонаучных и философских факультетов университетов, а также для всех самостоятельно изучающих математическую логику, теорию моделей и теорию алгоритмов.

УДК 510
ББК 22.12

ISBN 978-5-4437-0547-7

ОГЛАВЛЕНИЕ

1. МНОЖЕСТВА, ОПЕРАЦИИ НАД МНОЖЕСТВАМИ

1.1. Основные определения

Строгого определения множества нет, так как это понятие, из которого выводятся многие понятия математики, в то время как оно само не выводится из других понятий и не определяется ими. Понятие множества столь же первично, как понятие точки или числа. Синонимами слова «множества» можно считать такие слова, как «совокупность», «набор», «коллекция», «семейство».

Не всякая совокупность является множеством. В дальнейшем мы познакомимся с более общим, чем множество, понятием совокупности – классом. Каждое множество является классом, но не каждый класс является множеством.

Каждое множество является совокупностью своих элементов.

Определение 1.1. $x \in A$ *обозначает принадлежность элемента* x *множеству* A*; в таком случае говорят, что элемент* x *принадлежит множеству* A *или, другими словами, что* x *является элементом множества* A**.**

Определение 1.2. *Множество* A *является* ***подмножеством*** *множества* B (*обозначается* $\mathrm{A} \subseteq \mathrm{B}$)*, если все элементы множества* A *являются элементами множества* B*, т. е.* $A \subseteq B$ *тогда и только тогда, когда для всякого элемента* x *если* $x \in A$ *, то* $x \in B$*. Кратко, с помощью математических символов, это можно записать так*:

$$A \subseteq B \Leftrightarrow \forall x\,(x \in A \Rightarrow x \in B).$$

Отношение $\mathrm{A} \subseteq \mathrm{B}$ также можно изобразить с помощью диаграммы (рис. 1).

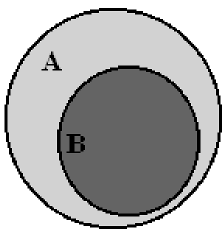

Рис. 1. Отношение A⊆B

Определение 1.3 (Принцип равнообъёмности). *Множества A и B называются* ***равными*** *(обозначается $A = B$), если они содержат одни и те же элементы, т. е. для всякого элемента x имеем $x \in A$ тогда и только тогда, когда выполнено $x \in B$.* Кратко это можно записать так:

$$A = B \;\Leftrightarrow\; \forall x\, (x \in A \;\Leftrightarrow\; x \in B).$$

Замечание 1.4. *Два множества равны тогда и только тогда, когда каждое из них является подмножеством другого, т. е.*

$$A = B \;\Leftrightarrow\; A \subseteq B \text{ и } B \subseteq A.$$

Доказательство. По определению, равенство двух множеств $A = B$ выполнено тогда и только тогда, когда эти множества имеют одни и те же элементы. Это означает, что для всякого элемента x выполнено $x \in A$ тогда и только тогда, когда выполнено $x \in B$. Последнее равносильно тому, что для всякого элемента x если $x \in A$, то $x \in B$, а если $x \in B$, то $x \in A$. Это утверждение, в свою очередь, равносильно тому, что, во-первых, для всякого элемента x если $x \in A$, то $x \in B$ и, во-вторых, для всякого элемента x если $x \in B$, то $x \in A$. По определению, это означает, что $A \subseteq B$ и $B \subseteq A$.

Таким образом, мы доказали, что для любых двух множеств A и B утверждение $A = B$ выполнено тогда и только тогда, когда $A \subseteq B$ и $B \subseteq A$. Кратко это доказательство можно записать так:

$$A = B \;\Leftrightarrow\; \forall x\, (x \in A \;\Leftrightarrow\; x \in B) \;\Leftrightarrow\; \begin{cases} \forall x\, (x \in A \;\Rightarrow\; x \in B) \;\Leftrightarrow\; A \subseteq B \\ \forall x\, (x \in B \;\Rightarrow\; x \in A) \;\Leftrightarrow\; B \subseteq A. \end{cases}$$

Замечание 1.4 доказано.

Позже мы познакомимся с общим понятием *двухместного отношения* и будем подробно изучать одно из наиболее важных двухместных отношений – *отношение частичного порядка*. Сейчас мы отметим, что отношение включения множеств является примером частичного порядка.

Предложение 1.5. *Отношение включения $\subseteq$ является* ***отношением частичного порядка****, т. е. обладает следующими свойствами:*

1) $\forall A\, (A \subseteq A)$ *(рефлексивность)*;
2) $\forall A, B\, \big((A \subseteq B \text{ и } B \subseteq A) \Rightarrow A = B\big)$ *(антисимметричность)*;
3) $\forall A, B, C\, \big((A \subseteq B \text{ и } B \subseteq C) \Rightarrow A \subseteq C\big)$ *(транзитивность)*.

Доказательство

1. По определению отношения включения, утверждение $A \subseteq A$ равносильно тому, что для всякого элемента x выполнено $(x \in A \Rightarrow x \in A)$. С другой стороны, утверждение $(x \in A \Rightarrow x \in A)$, очевидно, всегда истинно. Поэтому верно и утверждение $A \subseteq A$.

2. Очевидно из замечания 1.4.

3. Пусть $A \subseteq B$ и $B \subseteq C$. Допустим, что $A \nsubseteq C$. Тогда существует такой элемент x, что $x \in A$ и $x \notin C$. Поскольку $A \subseteq B$ и $x \in A$, выполнено $x \in B$. С другой стороны, $B \subseteq C$, поэтому $x \in C$. Мы пришли к противоречию, предположив, что $A \nsubseteq C$. Следовательно, выполнено $A \subseteq C$.

Предложение 1.5 доказано.

1.2. Операции над множествами

Определение 1.6. *Операции над множествами (рис. 2).*

1. *Объединение множеств:* $A \cup B = \{x \mid x \in A$ или $x \in B\}$.
2. *Пересечение множеств:* $A \cap B = \{x \mid x \in A$ и $x \in B\}$.
3. *Разность множеств:* $A \setminus B = \{x \mid x \in A$ и $x \notin B\}$.
4. *Симметрическая разность:* $A \dotdiv B = (A \setminus B) \cup (B \setminus A) = \{x \mid x \in A \setminus B$ или $x \in B \setminus A\}$.
5. *Дополнение множества:* $\bar{A} = U \setminus A = \{x \mid x \in U \setminus A\}$.

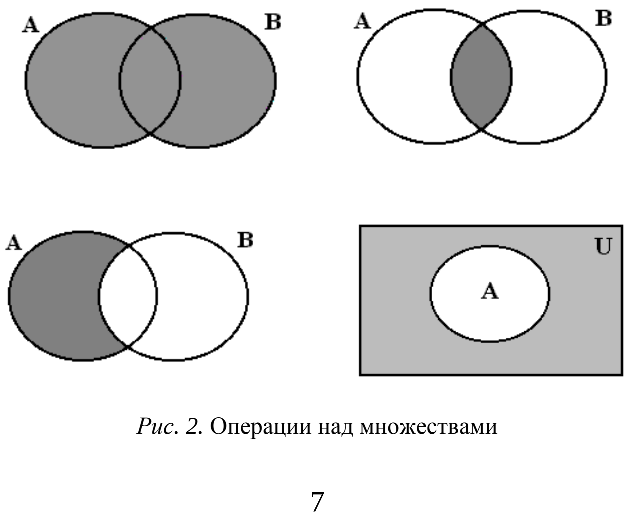

Рис. 2. Операции над множествами

Определение 1.7. ***Пустое*** *множество* $\varnothing$ *– это множество, не содержащее элементов, т. е. множество, которое не имеет ни одного элемента.*

Замечание 1.8. *Пустое множество единственно.*

Доказательство. Пусть есть два пустых множества $\varnothing_1$ и $\varnothing_2$. Так как они различны, то $\varnothing_1 \neq \varnothing_2$. По определению равенства множеств тогда найдётся элемент x такой, что $x \in \varnothing_1$ и $x \notin \varnothing_2$ либо, наоборот, $x \notin \varnothing_1$ и $x \in \varnothing_2$. Но так как множества $\varnothing_1$ и $\varnothing_2$ не имеют элементов, то такого x не может быть. Мы пришли к противоречию. Следовательно, пустое множество $\varnothing$ единственно.

Замечание 1.8 доказано.

Замечание 1.9. *Пустое множество является подмножеством любого множества.*

Доказательство. Действительно, рассмотрим некоторое множество A. По определению, включение $\varnothing \subseteq A$ означает следующее: если какой-то элемент x принадлежит пустому множеству $\varnothing$, то этот элемент принадлежит множеству $\varnothing \subseteq A$. Однако, поскольку в пустом множестве нет никаких элементов, это утверждение выполнено автоматически.

Замечание 1.9 доказано.

Излагая основы теории множеств, мы сейчас не рассматриваем строгий набор аксиом, которым должны удовлетворять множества и операции над ними. Такой подход иногда называют «*наивной теорией множеств*», в противоположность строгой «*аксиоматической теории множеств*». Как будет показано позже, использование наивной теории множеств, без накладывания дополнительных ограничений, приводит к парадоксам и противоречиям. С другой стороны, для нужд большей части математики и приложений (в частности для приложений в информационных технологиях) наивной теории множеств вполне достаточно.

Один из способов избежать парадоксов и противоречий – введение специального объемлющего множества, которое должно содержать все элементы. В таком случае все остальные множества, которые в данный момент рассматриваются, будут подмножествами этого множества. Таким образом, это объемлющее множество будет наибольшим по включению. Это множество называется *универсальным множеством* или кратко – *универсумом*.

Определение 1.10. ***Универсум*** *(универсальное множество),* U, – *это множество, содержащее все элементы*.

1.3. Теоретико-множественные тождества

Для того чтобы было легко и удобно пользоваться операциями над множествами, необходимо знать свойства, которыми обладают эти операции. Эти свойства называются теоретико-множественными тождествами.

Предложение 1.11. Имеют место следующие тождества:

1. $A \cup B = B \cup A$ (коммутативность);
2. $A \cap B = B \cap A$ (коммутативность);
3. $A \cup (B \cup C) = (A \cup B) \cup C$ (ассоциативность);
4. $A \cap (B \cap C) = (A \cap B) \cap C$ (ассоциативность);
5. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (дистрибутивность);
6. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (дистрибутивность);
7. $A \cup A = A$ (идемпотентность);
8. $A \cap A = A$ (идемпотентность);
9. $\overline{A \cup B} = \overline{A} \cap \overline{B}$ (закон де’Моргана);
10. $\overline{A \cap B} = \overline{A} \cup \overline{B}$ (закон де’Моргана);
11. $\overline{\overline{A}} = A$;
12. $A \cup \overline{A} = U$;
13. $A \cap \overline{A} = \emptyset$;
14. $A \cup U = U$;
15. $A \cup \emptyset = A$;
16. $A \cap U = A$;
17. $A \cap \emptyset = \emptyset$.

Доказательство

1. $\boldsymbol{A \cup B = B \cup A}$**.**

Рассмотрим утверждение $x \in A \cup B$. По определению, это равносильно тому, что $x \in A$ или $x \in B$. Это то же самое, что $x \in B$ или $x \in A$, что, в свою очередь, равносильно утверждению $x \in B \cup A$.

Мы, таким образом, показали, что утверждение $x \in A \cup B$ равносильно утверждению $x \in B \cup A$. В силу принципа равнообъёмности (определение 1.3) это означает, что рассматриваемые множества равны, т. е. $A \cup B = B \cup A$.

2. $\boldsymbol{A \cap B = B \cap A}$**.**

Рассмотрим утверждение $x \in A \cap B$. По определению, это равносильно тому, что $x \in A$ и $x \in B$. Это то же самое, что $x \in B$ и $x \in A$, что, в свою очередь, равносильно утверждению $x \in B \cap A$.

Мы, таким образом, показали, что утверждение $x \in A \cap B$ равносильно утверждению $x \in B \cap A$. В силу принципа равнообъёмности (определение 1.3) это означает, что рассматриваемые множества равны, т. е. что $A \cap B = B \cap A$.

3. $\boldsymbol{A \cup (B \cup C) = (A \cup B) \cup C}$**.**

Рассмотрим утверждение $x \in A \cup (B \cup C)$. По определению, это равносильно тому, что $x \in A$ или $x \in (B \cup C)$. Это, по определению, равносильно тому, что $x \in A$ или ($x \in B$ или $x \in C$).

Это то же самое, что ($x \in A$ или $x \in B$) или $x \in C$, что, в свою очередь, равносильно утверждению $x \in (A \cup B)$ или $x \in C$. Последнее, по определению, равносильно утверждению $x \in (A \cup B) \cup C$. Мы, таким образом, показали, что утверждение $x \in A \cup (B \cup C)$ равносильно утверждению $x \in (A \cup B) \cup C$. В силу принципа равнообъёмности это означает, что рассматриваемые множества равны, т. е. что $A \cup (B \cup C) = (A \cup B) \cup C$.

4. $\boldsymbol{A \cap (B \cap C) = (A \cap B) \cap C}$**.**

Рассмотрим утверждение $x \in A \cap (B \cap C)$. По определению, это равносильно тому, что $x \in A$ и $x \in (B \cap C)$. Это, по определению, равносильно тому, что $x \in A$ и ($x \in B$ и $x \in C$). Это то же самое, что ($x \in A$ и $x \in B$) и $x \in C$, что, в свою очередь, равносильно утверждению $x \in (A \cap B)$ и $x \in C$.

Последнее, по определению, равносильно утверждению $x \in (A \cap B) \cap C$. Мы, таким образом, показали, что утверждение $x \in A \cap (B \cap C)$ равносильно утверждению $x \in (A \cap B) \cap C$. В силу принципа равнообъёмности это означает, что рассматриваемые множества равны, т. е. что $A \cap (B \cap C) = (A \cap B) \cap C$.

5. $\boldsymbol{A \cup (B \cap C) = (A \cup B) \cap (A \cup C)}$**.**

Рассмотрим утверждение $x \in A \cup (B \cap C)$. По определению, это равносильно тому, что $x \in A$ или $x \in (B \cap C)$. Это, по определению, равносильно тому, что $x \in A$ или ($x \in B$ и $x \in C$). Однако, в отличие от предыдущих случаев, здесь не совсем понятно, что делать дальше – дальнейшие преобразования не являются такими же очевидными, как это было раньше.

Поэтому попробуем произвести преобразования с другого конца.

Рассмотрим теперь утверждение $x \in (A \cup B) \cap (A \cup C)$. По определению, это равносильно тому, что

$$x \in (A \cup B) \text{ и } x \in (A \cup C).$$

Это, по определению, равносильно тому, что

$$(x \in A \text{ или } x \in B) \text{ и } (x \in A \text{ или } x \in C).$$

Опять непонятно, как дальше преобразовывать это выражение. Нам необходимо ответить на вопрос: верно ли, что утверждение

«$x \in A$ или ($x \in B$ и $x \in C$)»

и утверждение

«($x \in A$ или $x \in B$) и ($x \in A$ или $x \in C$)»

являются эквивалентными? Кому-то будет непонятно, как отвечать на этот вопрос; кому-то положительный ответ на этот вопрос может быть очевидным.

Однако отметим следующее обстоятельство. Как правило, если кто-то говорит, что для него некоторое утверждение является очевидным, но при этом не может сразу внятно пояснить, почему это утверждение является верным, то в половине случаев это утверждение является неверным. Поэтому нам необходимо иметь не «внутреннюю убеждённость» в верности таких утверждений, а строгие формальные методы проверки их истинности. Такие методы мы изложим в следующем параграфе.

По существу, нам необходим алгоритм проверки (или «вычисления»), являются ли два данных высказывания равносильными. При этом рассматриваемые высказывания состоят из одинаковых «кирпичиков» – простейших, атомарных высказываний, которые соединены связками «и», «или», «не», «если…, то…». Требуемый алгоритм будет основан на построении так называемых «таблиц истинности», при помощи которых мы сможем определить, равносильны два данных высказывания или нет.

Таким образом, доказательство пунктов 5–17 остаётся в качестве упражнения на применение таблиц истинности, которые мы рассмотрим в следующем параграфе.

2. ЛОГИКА ВЫСКАЗЫВАНИЙ

2.1. Логические связки и таблицы истинности

Логика высказываний является своеобразной «арифметикой меры истинности», так же как обычная арифметика является «арифметикой меры количества».

Точно так же, как в арифметике, в логике высказываний есть переменные и операции над переменными. Только в арифметике мы имеем дело с мерой количества, а в логике высказываний – с мерой истинности. В логике высказываний значениями переменных являются не количества – натуральные или вещественные числа, а значения истинности: «истина» и «ложь». Каждая переменная обозначает некоторое неизвестное нам высказывание, предложение, про которое может быть известно только, является оно истинным или ложным. Такие переменные называются *пропозициональными переменными* – от латинского слова *propositio*, означающего «предложение, фраза».

Определение 2.1. ***Пропозициональными переменными*** *(A, B, C ...) будем называть переменные, принимающие свои значения из множества* ***{и, л}*** *(где* ***и*** *– истина,* ***л*** *– ложь).*

Как было отмечено выше, для того чтобы из «кирпичиков» – пропозициональных переменных – строить сложные высказывания, нам необходимы операции над мерами истинности; эти операции называются логическими связками.

Определение 2.2 (Логические связки и таблицы истинности). *Мы будем рассматривать четыре операции над пропозициональными переменными – четыре* ***логические связки***.

1. ***Дизъюнкция***. *Означает связку «и», обозначается* $\vee$.
2. ***Конъюнкция***. *Означает связку «или», обозначается* &.
3. ***Импликация***. *Означает связку «если ..., то ...», обозначается* $\rightarrow$.
4. ***Отрицание***. *Означает связку «не», обозначается* $\neg$.

Иногда для удобства рассматривают ещё одну логическую связку.

5. ***Эквиваленция***. *Означает связку «равносильно», обозначается* $\leftrightarrow$.

Когда мы рассматриваем арифметические операции над натуральными числами – сложение и умножение, – эти операции определяются таблицами своих значений: таблицами сложения и умножения. Точно так же и логические связки определяются таблицами своих значений; эти таблицы называются таблицами истинности. Только в отличие от арифметических операций здесь всё гораздо проще, поскольку пропозициональные переменные принимают всего два значения: «*истина*» и «*ложь*», тогда как в арифметике переменные принимают значения в бесконечном множестве натуральных чисел.

Значения логических связок приведены в следующих таблицах, называемых ***таблицами истинности***.

A	B	$A \vee B$
и	***и***	***и***
и	***л***	***и***
л	***и***	***и***
л	***л***	***л***

A	B	$A \,\&\, B$
и	***и***	***и***
и	***л***	***л***
л	***и***	***л***
л	***л***	***л***

A	B	$A \to B$
и	***и***	***и***
и	***л***	***л***
л	***и***	***и***
л	***л***	***и***

A	B	$A \leftrightarrow B$
и	***и***	***и***
и	***л***	***л***
л	***и***	***л***
л	***л***	***и***

A	$\neg A$
и	***л***
л	***и***

2.2. Формулы логики высказываний

Определение 2.3 (Формулы логики высказываний).

1. *Простейшие формулы: все пропозициональные переменные* $A, B, C, \ldots$ *являются формулами*.

2. *Построение новых формул из уже имеющихся: если* φ *и* ψ *являются формулами, то* $(\varphi \vee \psi)$, $(\varphi \,\&\, \psi)$, $(\varphi \to \psi)$, $(\neg\varphi)$ *также являются формулами*.

3. *Других формул нет*.

Данное определение является *индуктивным*: по существу, оно описывает процесс построения всех формул логики высказываний, начиная от простейших – пропозициональных переменных, до самых сложных. Такой способ определения математических объектов удобен ещё и тем, что мы можем доказывать разнообразные утверждения о формулах логики высказываний *индукцией по построению* этих формул.

Далее мы встретимся со многими другими индуктивными определениями математических объектов.

Обращаем внимание, что в определение формул логики высказываний логическая связка эквиваленция не входит. Это означает, что она не может присутствовать в записи формул.

Определение 2.4. *Часть формулы, которая сама является формулой, называется* ***подформулой*** *данной формулы.*

Определение 2.5. *Формула, принимающая значение «истина» при любых значениях входящих в нее пропозициональных переменных, называется* ***тождественно истинной (такая формула также называется теоремой или тавтологией)***.

Определение 2.6. *Формула, принимающая значение «ложь» при любых значениях входящих в нее пропозициональных переменных, называется* ***тождественно ложной.***

Определение 2.7. *Формула, не являющаяся тождественно ложной, называется* ***выполнимой***.

Определение 2.8. *Формула, не являющаяся тождественно истинной, называется* ***опровержимой***.

Замечание 2.9.

1. *Если формула φ тождественно истинна, то формула φ является выполнимой.*

2. Если формула φ тождественно ложна, то формула φ является опровержимой.

Доказательство: упражнение.

Замечание 2.10.

1. *Формула φ является тождественно истинной тогда и только тогда, когда формула $\neg\varphi$ является тождественно ложной.*

2. Формула φ является выполнимой тогда и только тогда, когда формула $\neg\varphi$ является опровержимой.

Доказательство: упражнение.

Предложение 2.11 (Тождественно истинные формулы логики высказываний).

Следующие формулы являются тождественно истинными:

1. $\big(A \to (B \to A)\big)$;
2. $\Big((A \to B) \to \big((A \to (B \to C)) \to (A \to C)\big)\Big)$;
3. $\big((A \& B) \to A\big)$;
4. $\big((A \& B) \to B\big)$;
5. $\big(B \to (A \vee B)\big)$;
6. $\big(A \to (A \vee B)\big)$;
7. $\Big((A \to B) \to \big((A \to \mathrm{C}) \to (A \to (B \& \mathrm{C}))\big)\Big)$;
8. $\Big((A \to \mathrm{C}) \to \big((B \to \mathrm{C}) \to ((A \vee B) \to \mathrm{C})\big)\Big)$;
9. $\big((A \to \neg B) \to (B \to \neg A)\big)$;
10. $(\neg\neg A \to A)$;
11. $(A \to \neg\neg A)$;
12. $\big((A \to B) \vee (B \to A)\big)$;
13. $\big((A \to B) \vee (A \to \neg B)\big)$;
14. $(A \vee \neg A)$ (*закон исключения третьего*);
15. $\neg(A \& \neg A)$ (*закон невозможности противоречия*).

Доказательство: упражнение. Доказать при помощи построения таблиц истинности.

2.3. Основные тождества логики высказываний

Определение 2.12. *Двуместное отношение ~ (тильда) называется* ***отношением эквивалентности*** *(на множестве A), если для любых элементов $a, b, c \in A$ выполняются свойства:*

1) $a \sim a$ (рефлексивность);
2) $a \sim b \;\Rightarrow\; b \sim a$ (симметричность);
3) $(a \sim b$ и $b \sim c) \;\Rightarrow\; a \sim c$ (транзитивность).

Определение 2.13. *Формулы φ и ψ называются* ***эквивалентными*** *(обозначается $(\varphi \sim \psi)$), если они принимают одинаковые значения истинности при одинаковых значениях пропозициональных переменных.*

Пример. Формулы $(\neg (A \,\&\, \neg B))$ и $(\neg A \vee B)$ являются эквивалентными:

$$(\neg (A \,\&\, \neg B)) \sim (\neg A \vee B).$$

Заметим, что смысл математического термина не определяется этимологией слова, обозначающего этот термин. Например, нечётная функция – это не функция, которая не является чётной. Поэтому, если мы говорим «формулы называются эквивалентными», это совсем не означает, что определяемое отношение между формулами действительно является отношением эквивалентности. Такое свойство определяемого отношения, если оно имеет место, необходимо отдельно доказывать.

Предложение 2.14. *«Отношение эквивалентности формул» $\sim$ действительно является отношением эквивалентности, т. е. для любых формул φ, ψ и ξ это отношение обладает следующими свойствами:*

1) $(\varphi \sim \varphi)$ *(рефлексивность)*;
2) $((\varphi \sim \psi) \Rightarrow (\psi \sim \varphi))$ *(симметричность)*;
3) $\big((\varphi \sim \psi \,\&\, \psi \sim \xi) \Rightarrow \varphi \sim \xi\big)$ *(транзитивность)*.

Доказательство: упражнение.

Рассмотрим основные эквивалентности логики высказываний. Эти эквивалентности, называемые тождествами логики высказываний, полезны при доказательстве многих утверждений о формулах логики высказываний. Кроме того, тождества логики высказываний нам пригодятся для доказательства тождеств теории множеств.

Предложение 2.15 (Тождества логики высказываний). *Имеют место* с*ледующие эквивалентности*:

1. $(A \vee B) \sim (B \vee A)$ *(коммутативность)*;
2. $(A \,\&\, B) \sim (B \,\&\, A)$ *(коммутативность)*;
3. $\big(A \vee (B \vee C)\big) \sim \big((A \vee B) \vee C\big)$ *(ассоциативность)*;
4. $\big(A \,\&\, (B \,\&\, C)\big) \sim \big((A \,\&\, B) \,\&\, C\big)$ *(ассоциативность)*;
5. $\big(A \vee (B \,\&\, C)\big) \sim \big((A \vee B) \,\&\, (A \vee C)\big)$ *(дистрибутивность)*;
6. $\big(A \,\&\, (B \vee C)\big) \sim \big((A \,\&\, B) \vee (A \,\&\, C)\big)$ *(дистрибутивность)*;
7. $(A \vee A) \sim A$ *(идемпотентность)*;
8. $(A \,\&\, A) \sim A$ *(идемпотентность)*;
9. $\neg(A \vee B) \sim (\neg A \,\&\, \neg B)$ *(закон де'Моргана)*;
10. $\neg(A \,\&\, B) \sim (\neg A \vee \neg B)$ *(закон де'Моргана)*;

11. $\neg\neg A \sim A$ *(снятие двойного отрицания)*;
12. $(A \to B) \sim (\neg A \vee B)$;
13. $(A \to \neg B) \sim (B \to \neg A)$;
14. $\big(A \,\&\, (A \vee B)\big) \sim A$;
15. $\big(A \vee (A \,\&\, B)\big) \sim A$;
16. $\big(A \vee (B \,\&\, \neg B \,\&\, C)\big) \sim A$;
17. $\big(A \,\&\, (B \vee \neg B \vee C)\big) \sim A$;
18. $(A \leftrightarrow B) \sim \big((A \to B) \,\&\, (B \to A)\big) \sim \big((\neg A \vee B) \,\&\, (\neg B \vee A)\big)$.

Доказательство: упражнение – при помощи построения таблиц истинности. Строим таблицы истинности для формул, стоящих в левой и правой части рассматриваемой эквивалентности. Проверяем, что у этих формул значения истинности совпадают.

Отметим, что, если в тождествах логики высказываний заменить входящие в них пропозициональные переменные на произвольные формулы, эти тождества останутся верными. Полученные эквивалентности логики высказываний также называются *законами логики*. В частности, свойство рефлексивности отношения эквивалентности формул $(\varphi \sim \varphi)$ называется законом тождества.

Следствие 2.16 (Законы логики высказываний). *Имеют место следующие эквивалентности*:
1. $(\varphi \vee \psi) \sim (\psi \vee \varphi)$ *(коммутативность)*;
2. $(\varphi \,\&\, \psi) \sim (\psi \,\&\, \varphi)$ *(коммутативность)*;
3. $\big(\varphi \vee (\psi \vee \xi)\big) \sim \big((\varphi \vee \psi) \vee \xi\big)$ *(ассоциативность)*;
4. $\big(\varphi \,\&\, (\psi \,\&\, \xi)\big) \sim \big((\varphi \,\&\, \psi) \,\&\, \xi\big)$ *(ассоциативность)*;
5. $(\varphi \vee (\psi \,\&\, \xi)) \sim \big((\varphi \vee \psi) \,\&\, (\varphi \vee \xi)\big)$ *(дистрибутивность)*;
6. $\big(\varphi \,\&\, (\psi \vee \xi)\big) \sim \big((\varphi \,\&\, \psi) \vee (\varphi \,\&\, \xi)\big)$ *(дистрибутивность)*;
7. $(\varphi \vee \varphi) \sim \varphi$ *(идемпотентность)*;
8. $(\varphi \,\&\, \varphi) \sim \varphi$ *(идемпотентность)*;
9. $\neg(\varphi \vee \psi) \sim (\neg \varphi \,\&\, \neg\psi)$ *(закон де’Моргана)*;
10. $\neg(\varphi \,\&\, \psi) \sim (\neg \varphi \vee \neg\psi)$ *(закон де’Моргана)*;
11. $(\neg\neg \varphi) \sim \varphi$ *(снятие двойного отрицания)*;
12. $(\varphi \to \psi) \sim (\neg \varphi \vee \psi)$;
13. $(\varphi \to \neg \psi) \sim (\psi \to \neg\varphi)$;
14. $\big(\varphi \,\&\, (\varphi \vee \psi)\big) \sim \varphi$;
15. $\big(\varphi \vee (\varphi \,\&\, \psi)\big) \sim \varphi$;

16. $(\varphi \vee (\psi \,\&\, \neg\psi \,\&\, \xi)) \sim \varphi$;

17. $(\varphi \,\&\, (\psi \vee \neg\psi \vee \xi)) \sim \varphi$;

18. $(\varphi \leftrightarrow \psi) \sim ((\varphi \to \psi) \,\&\, (\psi \to \varphi)) \sim ((\neg\varphi \vee \psi) \,\&\, (\neg\psi \vee \varphi))$.

Доказательство. Рассмотрим какое-либо из тождеств, приведённых выше. Пусть $\varphi,\ \psi$ и ξ – произвольные формулы логики высказываний. Построим таблицы истинности для формул, стоящих в левой и правой части рассматриваемой эквивалентности. Заметим, что какие бы значения истинности ни были у подформул $\varphi,\ \psi$ и ξ этих формул, в силу Предложения 2.15 значения истинности у формул, стоящих в левой и правой части данного тождества, совпадают. Поэтому эти формулы являются эквивалентными.

Следствие 2.16 доказано.

Предложение 2.17. *Пусть для формул* φ_1 , φ_2 , ψ_1 , *и* ψ_2 *выполнено:* $\varphi_1 \sim \psi_1$ *и* $\varphi_2 \sim \psi_2$. *Тогда имеют место следующие эквивалентности:*

а) $(\varphi_1 \vee \varphi_2) \sim (\psi_1 \vee \psi_2)$;

б) $(\varphi_1 \,\&\, \varphi_2) \sim (\psi_1 \,\&\, \psi_2)$;

в) $(\varphi_1 \to \varphi_2) \sim (\psi_1 \to \psi_2)$;

г) $\neg\varphi_1 \sim \neg\psi_1$.

Доказательство

а) Рассмотрим таблицы истинностей для формул

$$(\varphi_1 \vee \varphi_2) \text{ и } (\psi_1 \vee \psi_2).$$

В силу того, что $\varphi_1 \sim \psi_1$ и $\varphi_2 \sim \psi_2$, значения истинности формулы φ_1 совпадают со значениями истинности формулы ψ_1, а значения истинности формулы φ_2 – со значениями истинности формулы ψ_2. Поэтому, после применения логической связки $\vee$, значения истинности формул $(\varphi_1 \vee \varphi_2)$ и $(\psi_1 \vee \psi_2)$ также будут совпадать, поэтому эти формулы являются эквивалентными, т. е.

$$(\varphi_1 \vee \varphi_2) \sim (\psi_1 \vee \psi_2).$$

б) Рассмотрим таблицы истинностей для формул

$$(\varphi_1 \,\&\, \varphi_2) \text{ и } (\psi_1 \,\&\, \psi_2).$$

В силу того, что $\varphi_1 \sim \psi_1$ и $\varphi_2 \sim \psi_2$, значения истинности формулы φ_1 совпадают со значениями истинности формулы ψ_1, а значения истинности формулы φ_2 – со значениями истинности формулы ψ_2. Поэтому, после применения логической связки &, значения истинности формул $(\varphi_1 \,\&\, \varphi_2)$ и $(\psi_1 \& \psi_2)$ также будут совпадать, поэтому эти формулы являются эквивалентными, т. е.

$$(\varphi_1 \,\&\, \varphi_2) \sim (\psi_1 \& \psi_2).$$

в) Рассмотрим таблицы истинностей для формул

$$(\varphi_1 \;\rightarrow\; \varphi_2) \text{ и } (\psi_1 \rightarrow\; \psi_2).$$

В силу того, что $\varphi_1 \sim \psi_1$ и $\varphi_2 \sim \psi_2$, значения истинности формулы φ_1 совпадают со значениями истинности формулы ψ_1, а значения истинности формулы φ_2 – со значениями истинности формулы ψ_2. Поэтому, после применения логической связки $\rightarrow$, значения истинности формул $(\varphi_1 \rightarrow\; \varphi_2)$ и $(\psi_1 \rightarrow\; \psi_2)$ также будут совпадать, поэтому эти формулы являются эквивалентными, т. е. $(\varphi_1 \rightarrow \varphi_2) \sim (\psi_1 \rightarrow\; \psi_2)$.

г) Упражнение.

Предложение 2.17 доказано.

Далее мы будем использовать следующее.

Обозначение 2.18. *Пусть φ и ξ – произвольные формулы логики высказываний, а ψ – некоторая подформула формулы φ, причём зафиксировано определённое вхождение этой подформулы ψ в формулу φ (если подформула ψ несколько раз входит в формулу φ).*

Через $(\varphi)_\xi^\psi$ обозначим формулу, полученную в результате заменены в формуле φ данного вхождения подформулы ψ на формулу ξ .

Пример 2.19. Пусть $\varphi = \big((A \rightarrow B) \vee \neg C\big)$, $\psi = (A \rightarrow B)$ и $\xi = \big(D \vee (A \,\&\, \neg B)\big)$. Тогда $(\varphi)_\xi^\psi = \Big(\big(D \vee (A \,\&\, \neg B)\big) \vee \neg C\Big)$.

Длиной формулы будем называть количество символов, входящих в эту формулу.

Предложение 2.20. *Пусть φ и ξ – произвольные формулы логики высказываний, а ψ – некоторая подформула формулы φ, причём зафиксировано определённое вхождение этой подформулы ψ в формулу φ, и пусть $\psi \sim \xi$. Тогда $\varphi \sim (\varphi)_\xi^\psi$.*

Доказательство. Пусть длина формулы ψ равна l. Доказательство будем проводить индукцией по длине n формулы φ. Очевидно, что, поскольку формула ψ является подформулой формулы φ, выполнено $l \leq n$. Поэтому доказательство начинаем со случая $n = l$.

1. Пусть $n = l$, тогда выполнено $\varphi = \psi$, поэтому $(\varphi)_\xi^\psi = \xi$, следовательно $\varphi = \psi \sim \xi = (\varphi)_\xi^\psi$, т. е. $\varphi \sim (\varphi)_\xi^\psi$.

2. Допустим, при любом $k < n$ утверждение Предложения 2.20 для формул длины k является верным. Докажем данное утверждение для формулы φ длины n.

Заметим, что в силу Определения 2.3 формул логики высказываний имеет место один из следующих случаев строения формулы φ: $\varphi = (\varphi_1 \vee \varphi_2)$, либо $\varphi = (\varphi_1 \,\&\, \varphi_2)$, либо $\varphi = (\varphi_1 \to \varphi_2)$, либо $\varphi = \neg\varphi_1$. Очевидно, что во всех этих случаях длина формул φ_1 и φ_2 меньше, чем n, поэтому, по индукционному предположению, для формул φ_1 и φ_2 выполнено утверждение Предложения. Мы зафиксировали ровно одно вхождение подформулы ψ в формулу φ, для которого мы производим замену. Это вхождение содержится либо в формуле φ_1, либо в формуле φ_2. Предположим, что зафиксированное вхождение подформулы ψ в формулу φ содержится в формуле φ_1; случай, когда вхождение подформулы ψ в формулу φ содержится в формуле φ_2 , рассматривается аналогично. Тогда, в зависимости от строения формулы φ, выполнено

$$\text{либо } (\varphi)_\xi^\psi = \left((\varphi_1)_\xi^\psi \vee \varphi_2\right),$$

$$\text{либо } (\varphi)_\xi^\psi = \left((\varphi_1)_\xi^\psi \,\&\, \varphi_2\right),$$

$$\text{либо } (\varphi)_\xi^\psi = \left((\varphi_1)_\xi^\psi \to \varphi_2\right),$$

$$\text{либо } (\varphi)_\xi^\psi = (\neg\varphi_1)_\xi^\psi$$

соответственно. По индукционному предположению, поскольку длина формулы φ_1 меньше, чем n, выполнено $\varphi_1 \sim (\varphi_1)_\xi^\psi$. По Предложению 2.14 имеем $\varphi_2 \sim \varphi_2$. Поэтому, в силу Предложения 2.17, в зависимости от строения формулы φ, выполнено

$$\text{либо } \varphi = (\varphi_1 \vee \varphi_2) \sim \left((\varphi_1)_\xi^\psi \vee \varphi_2\right) = (\varphi)_\xi^\psi ,$$

$$\text{либо } \varphi = (\varphi_1 \,\&\, \varphi_2) \sim \left((\varphi_1)_\xi^\psi \,\&\, \varphi_2\right) = (\varphi)_\xi^\psi,$$

$$\text{либо } \varphi = (\varphi_1 \to \varphi_2) \sim \left((\varphi_1)_\xi^\psi \to \varphi_2\right) = (\varphi)_\xi^\psi,$$

$$\text{либо } \varphi = \neg\varphi_1 \sim (\neg\varphi_1)_\xi^\psi = (\varphi)_\xi^\psi$$

соответственно. Стало быть, во всех случаях мы имеем $\varphi \sim (\varphi)_{\xi}^{\psi}$.

Предложение 2.20 доказано.

Обозначение 2.21. Пусть φ и ξ – произвольные формулы логики высказываний, а ψ – некоторая подформула формулы φ. Через $[\varphi]_{\xi}^{\psi}$ обозначим формулу, полученную в результате замены в формуле φ всех вхождений подформулы ψ на формулу ξ.

Теорема 2.22 (о замене). *Пусть φ и ξ – произвольные формулы логики высказываний, а ψ – некоторая подформула формулы φ и пусть $\psi \sim \xi$. Тогда $\varphi \sim [\varphi]_{\xi}^{\psi}$.*

Доказательство. Пусть подформула ψ имеет n вхождений в формулу φ. Сделаем n раз в формуле φ замену очередного вхождения подформулы ψ на формулу ξ и применим n раз Предложение 2.20. В силу транзитивности отношения эквивалентности формул (Предложение 2.14) формула $[\varphi]_{\xi}^{\psi}$, полученная в результате проведённых n замен, будет эквивалентна исходной формуле, т. е. будет выполнено $\varphi \sim [\varphi]_{\xi}^{\psi}$.

Теорема 2.22 доказана.

Следствие 2.23. *Для любой формулы φ существует формула $\psi \sim \varphi$, такая что ψ не содержит символов импликации.*

Доказательство. Пусть формула φ содержит n символов импликации. Обозначим $\psi_0 = \varphi$. Проделаем цепочку преобразований следующим образом: если формула ψ_k содержит символ импликации $\rightarrow$, выберем самое левое вхождение подформулы формулы ψ_k, имеющей вид $(\varphi_1 \rightarrow \varphi_2)$, и проделаем замену:

$$\psi_{k+1} = (\psi_k)_{(\neg\varphi_1 \vee \varphi_2)}^{(\varphi_1 \rightarrow \varphi_2)}.$$

Формула ψ_{k+1} будет содержать на один символ импликации меньше, чем формула ψ_k; поэтому, как легко видеть, формула ψ_{k+1} будет содержать $n-k-1$ символ импликации. Кроме того, в силу Предложения 2.20 выполнено $\psi_k \sim \psi_{k+1}$. Сделав n замен, мы получим формулу $\psi = \psi_n$, не содержащую символов импликации. Таким образом, выполнено

$$\varphi = \psi_0 \sim \ldots \sim \psi_k \sim \psi_{k+1} \sim \ldots \sim \psi_n = \psi.$$

В силу транзитивности отношения эквивалентности формул (Предложение 2.14) имеем $\psi \sim \varphi$, при этом формула ψ не содержит символов импликации.

Следствие 2.23 доказано.

2.4. Нормальные формы

Определение 2.24. *Формула φ называется формулой с* ***тесными отрицаниями****, если она не содержит символов импликаций, а отрицания в формуле φ стоят только перед пропозициональными переменными.*

Определение 2.25. ***Элементарной конъюнкцией*** *называется конъюнкция пропозициональных переменных и отрицаний пропозициональных переменных.*

Определение 2.26. ***Элементарной дизъюнкцией*** *называется дизъюнкция пропозициональных переменных и отрицаний пропозициональных переменных.*

Определение 2.27. ***Дизъюнктивной нормальной формой*** *(ДНФ) называется дизъюнкция элементарных конъюнкций.*

Определение 2.28. ***Конъюнктивной нормальной формой*** *(КНФ) называется конъюнкция элементарных дизъюнкций.*

Теорема 2.29. *Для любой формулы φ существует формула ψ, находящаяся в дизъюнктивной нормальной форме (ДНФ) такая, что $\varphi \sim \psi$.*

Доказательство. *Алгоритм приведения формулы к дизъюнктивной нормальной форме при помощи эквивалентных преобразований.*

Проделаем четыре шага преобразований.

1. При помощи тождества

$$(\varphi_1 \to \varphi_2) \sim (\neg\varphi_1 \vee \varphi_2)$$

избавляемся от импликации (см. Следствие 2.23).

2. При помощи тождеств

$$\neg(\varphi_1 \vee \varphi_2) \sim (\neg\varphi_1 \& \neg\varphi_2) \text{ и } \neg(\varphi_1 \& \varphi_2) \sim (\neg\varphi_1 \vee \neg\varphi_2),$$

а также тождества $(\neg\neg\varphi) \sim \varphi$ (снятие двойного отрицания) вносим отрицание внутрь подформул вплоть до пропозициональных переменных.

После первых двух шагов мы получили формулу с тесными отрицаниями.

3. При помощи тождества

$$(\varphi \,\&\, (\psi \vee \xi)) \sim \big((\varphi \& \psi) \vee (\varphi \& \xi)\big)$$

выносим дизъюнкцию $\vee$ наружу.

4. Имея в виду тождества

$$(\varphi \vee (\psi \vee \xi)) \sim ((\varphi \vee \psi) \vee \xi) \text{ и } (\varphi \,\&\, (\psi \,\&\, \xi)) \sim ((\varphi \,\&\, \psi) \,\&\, \xi),$$

удаляем скобки внутри последовательностей конъюнкций и последовательностей дизъюнкций.

В силу Предложения 2.20 мы выполнили последовательность эквивалентных преобразований:

$$\varphi = \psi_0 \sim \dots \sim \psi_k \sim \psi_{k+1} \sim \dots \sim \psi_n = \psi.$$

В результате выполнения этой последовательности преобразований мы получили формулу ψ, находящуюся в дизъюнктивной нормальной форме (ДНФ); при этом, в силу симметричности и транзитивности отношения эквивалентности формул (Предложение 2.14), имеем $\varphi \sim \psi$.

Теорема 2.29 доказана.

Теорема 2.30. *Для любой формулы φ существует формула ψ, находящаяся в конъюнктивной нормальной форме (КНФ) такая, что $\varphi \sim \psi$.*

Доказательство. *Алгоритм приведения формулы к конъюнктивной нормальной форме при помощи эквивалентных преобразований.*

Проделаем четыре шага преобразований.

1. При помощи тождества

$$(\varphi_1 \to \varphi_2) \sim (\neg \varphi_1 \vee \varphi_2)$$

избавляемся от импликации (см. Следствие 2.23).

2. При помощи тождеств

$$\neg(\varphi_1 \vee \varphi_2) \sim (\neg \varphi_1 \,\&\, \neg \varphi_2) \text{ и } \neg(\varphi_1 \& \varphi_2) \sim (\neg \varphi_1 \vee \neg \varphi_2),$$

а также тождества $(\neg\neg \varphi) \sim \varphi$ (снятие двойного отрицания) вносим отрицание внутрь подформул вплоть до пропозициональных переменных. После первых двух шагов мы получили формулу с тесными отрицаниями.

3. При помощи тождества

$$(\varphi \vee (\psi \,\&\, \xi)) \sim ((\varphi \vee \psi) \,\&\, (\varphi \vee \xi))$$

выносим конъюнкцию & наружу.

4. Имея в виду тождества

$(\varphi \vee (\psi \vee \xi)) \sim ((\varphi \vee \psi) \vee \xi)$ и $(\varphi \,\&\, (\psi \,\&\, \xi)) \sim ((\varphi \,\&\, \psi) \,\&\, \xi)$, удаляем скобки внутри последовательностей конъюнкций и последовательностей дизъюнкций.

В силу Предложения 2.20, мы выполнили последовательность эквивалентных преобразований:

$$\varphi = \psi_0 \sim \dots \sim \psi_k \sim \psi_{k+1} \sim \dots \sim \psi_n = \psi.$$

В результате выполнения этой последовательности преобразований мы получили формулу ψ, находящуюся в конъюнктивной нормальной форме (КНФ); при этом, в силу симметричности и транзитивности отношения эквивалентности формул (Предложение 2.14), имеем $\varphi \sim \psi$.

Теорема 2.30 доказана.

Определение 2.31. ***Совершенной дизъюнктивной нормальной формой*** *(СДНФ) называют ДНФ, в которой любая пропозициональная переменная, содержащаяся в этой формуле, входит в каждую её элементарную конъюнкцию ровно один раз (с отрицанием или без него).*

Определение 2.32. ***Совершенной конъюнктивной нормальной формой*** *(СКНФ) называют КНФ, в которой любая пропозициональная переменная, содержащаяся в этой формуле, входит в каждую её элементарную дизъюнкцию ровно один раз (с отрицанием или без него).*

Теорема 2.33. *Для любой выполнимой формулы существует эквивалентная ей совершенная дизъюнктивная нормальная форма (СДНФ).*

Доказательство. *Алгоритм приведения формулы к совершенной дизъюнктивной нормальной форме при помощи таблиц истинности.*

1. Строим таблицу истинности для данной формулы.
2. Вычеркиваем из таблицы все строки, в которых формула принимает ложные значения.
3. По каждой невычеркнутой строке строим элементарную конъюнкцию, в которой каждая истинная пропозициональная переменная берется без отрицания, а каждая ложная пропозициональная переменная – с отрицанием.

4. Строим дизъюнкцию всех полученных в п. 3 элементарных конъюнкций.

Теорема 2.33 доказана.

Пример. Пусть для формулы φ от трех переменных A_1, A_2, A_3 построена следующая таблица истинности.

A_1	A_2	A_3	$\varphi(A_1, A_2, A_3)$
и	***и***	***и***	***и***
и	***и***	***л***	***л***
и	***л***	***и***	***л***
и	***л***	***л***	***и***
л	***и***	***и***	***л***
л	***и***	***л***	***л***
л	***л***	***и***	***л***
л	***л***	***л***	***и***

Вычеркнув из этой таблицы строки, в которых формула φ принимает ложные значения, получим следующую таблицу.

A_1	A_2	A_3	$\varphi(A_1, A_2, A_3)$
и	***и***	***и***	***и***
и	***л***	***л***	***и***
л	***л***	***л***	***и***

Построим по полученной таблице СДНФ:

$$\big((A_1 \,\&\, A_2 \,\&\, A_3) \vee (A_1 \,\&\, \neg A_2 \,\&\, \neg A_3) \vee (\neg A_1 \,\&\, \neg A_2 \,\&\, \neg A_3)\big).$$

Теорема 2.34. *Для любой опровержимой формулы существует эквивалентная ей совершенная конъюнктивная нормальная форма (СКНФ).*

Доказательство. Алгоритм приведения формулы к совершенной конъюнктивной нормальной форме при помощи таблиц истинности.

1. Строим таблицу истинности для данной формулы.
2. Вычеркиваем из таблицы все строки, в которых формула принимает истинные значения.
3. По каждой невычеркнутой строке строим элементарную дизъюнкцию, в которой каждая ложная пропозициональная переменная берется без отрицания, а каждая истинная пропозициональная переменная – с отрицанием.
4. Строим конъюнкцию всех полученных в п. 3 элементарных дизъюнкций.

Теорема 2.34 доказана.

Пример. Пусть для формулы φ от трех переменных A_1, A_2, A_3 построена следующая таблица истинности.

A_1	A_2	A_3	$\varphi(A_1, A_2, A_3)$
и	***и***	***и***	***и***
и	***и***	***л***	***л***
и	***л***	***и***	***и***
и	***л***	***л***	***и***
л	***и***	***и***	***л***
л	***и***	***л***	***и***
л	***л***	***и***	***л***
л	***л***	***л***	***и***

Вычеркнув из этой таблицы строки, в которых формула φ принимает ложные значения, получим следующую таблицу.

A_1	A_2	A_3	$\varphi(A_1, A_2, A_3)$
и	***и***	***л***	***л***
л	***и***	***и***	***л***
л	***л***	***и***	***л***

Построим по полученной таблице СКНФ:
$\big((\neg A_1 \vee \neg A_2 \vee A_3) \,\&\, (A_1 \vee \neg A_2 \vee \neg A_3) \,\&\, (A_1 \vee A_2 \vee \neg A_3)\big)$.

Определение 2.35. *Функция* $f : \{\text{и}, \text{л}\}^n \to \{\text{и}, \text{л}\}$ *называется* ***логической*** *функцией. Область определения функции* f *— множество* $\{\text{и}, \text{л}\}$*, область значения определения функции* f *— множество* $\{\text{и}, \text{л}\}$.

Предложение 2.36. *Для любой логической функции* f *существует формула* φ*, представляющая* f*, т. е. такая формула* φ*, что функция* f *и формула* φ *имеют одинаковые таблицы истинности (другими словами, они имеют одинаковые графики).*

Доказательство. Рассмотрим логическую функцию $f(x_1, x_2, \dots, x_n)$ от n переменных. Представим её график в виде таблицы истинности. Заметим, что по алгоритмам, приведённым в доказательстве Теорем 2.33 и 2.34, для любой таблицы истинности можно построить СДНФ или СКНФ: если в таблице истинности в столбце значений есть хотя бы одна «и», то можно построить СДНФ, а если в столбце значений есть хотя бы одна «л», то – СКНФ. Поэтому для логической функции f можно построить формулу, являющуюся СДНФ или СКНФ, которая будет принимать те же значения истинности, что и функция f.

Предложение 2.36 доказано.

2.5. Связь с теорией множеств

В предыдущем параграфе мы столкнулись с трудностями при доказательстве тождеств теории множеств. Следствие 2.16 даёт нам возможность доказывать эти тождества. Например, доказательство теоретико-множественного тождества 5, с которым у нас возникли проблемы, легко проводится при помощи тождества 5 логики высказываний из Следствия 2.16. Точно так же, как легко видеть, при помощи законов логики высказываний из Следствия 2.16 мы можем доказать оставшиеся теоретико-множественные тождества.

С другой стороны, видно, что многие тождества теории множеств, сформулированные в Предложении 2.15, очень похожи на тождества логики высказываний. Например:

а) $(A \cup (B \cup C)) = ((A \cup B) \cup C))$ и $(A \vee (B \vee C) \sim (A \vee B) \vee C)$;

б) $(A \cap (B \cup C)) = ((A \cap B) \cup (A \cap C))$ и $\big(A \,\&\, (B \vee C)\big) \sim \big((A \,\&\, B) \vee (A \,\&\, C)\big)$;

в) $(\overline{A \cup B}) = (\overline{A} \cap \overline{B})$ и $\neg(A \vee B) \sim (\neg A \,\&\, \neg B)$;

г) $\overline{\overline{A}} = A$ и $\neg\neg A \sim A$.

Легко видеть, что разница между этими выражениями состоит в следующем: во-первых, переменные A, B, C, обозначающие множества, заменяются на те же самые символы A, B, C, но обозначающие пропозициональные переменные; во-вторых, символы теоретико-множественных операций $\cup$, $\cap$ и $\overline{}$ заменяются на логические связки $\vee$, $\&$ и $\neg$ соответственно. Символ равенства множеств $=$ заменяется на символ эквивалентности формул $\sim$.

Цель оставшейся части этого параграфа – строго математически сформулировать это наблюдение и доказать его верность. Для этого запишем указанные выше преобразования на формальном математическом языке. Сначала нам нужно формально определить теоретико-множественные выражения, над которыми производятся такие преобразования.

Определение 2.37 (Термы теории множеств).

1. *Простейшие термы. Пусть* A, B, C *– переменные, обозначающие множества, тогда* A, B, C *являются термами.*

2. *Построение новых термов из уже имеющихся: пусть* t_1 *и* t_2 *являются термами, тогда выражения* $(t_1 \cup t_2)$, $(t_1 \cap t_2)$ *и* $\overline{t_1}$ *также являются термами.*

3. *Других термов нет.*

Определение 2.37 является индуктивным, как и приведённое выше Определение 2.3 формул логики высказываний: оно полностью описывает процесс построения термов.

Заметим, что если зафиксированы конкретные множества $A_1, \dots, A_n$, то значением терма $t = t(A_1, \dots, A_n)$ является множество (полученное из множеств $A_1, \dots, A_n$ последовательным применением теоретико-множественных операций, так как это указано в записи терма t).

Здесь важно отметить, что теоретико-множественные термы являются аналогом алгебраических выражений, таких как, например,

$$(x + y),\ (x - y) \text{ или } (x + y)(x - y),$$

построенных из символов переменных (принимающих числовые значения), символов арифметических операций и служебных символов – скобок. Для того чтобы лучше это понять, полезно выполнить следующее упражнение.

Упражнение 2.38. По аналогии с Определением 2.37 термов теории множеств записать индуктивное определение алгебраических выражений.

Теперь дадим формальное определение преобразования, которое по теоретико-множественному терму строит соответствующую ему формулу логики высказываний.

Определение 2.39. *Обозначим через T множество всех термов теории множеств, а через F – множество всех формул логики высказываний. Отображение $\rho\colon T \to F$ определим следующим образом.*

1. Преобразование простейших термов:

$$\rho(A) = A,\ \rho(B) = B,\ \ \rho(C) = C \quad \text{и т. д.}$$

для всех переменных, обозначающих множества.

2. Преобразование составных термов: пусть t_1 и t_2 являются термами, тогда

а) $\rho(t_1 \cup t_2) = \big(\rho\,(t_1) \vee \rho(t_2)\big)$;

б) $\rho(t_1 \cap t_2) = (\rho\,(t_1)\ \&\ \rho(t_2))$;

в) $\rho\big(\,\overline{t_1}\,\big) = \neg\,\rho(t_1)$.

Пример 2.40. $\rho(\,(A \cup B) \cap (A \cup C)) = ((A \vee B)\ \&\ (A \vee C))$.

Таким образом, мы ввели все необходимые определения и обозначения. Теперь мы можем сформулировать на математическом языке и доказать сделанное нами выше наблюдение о преобразовании теоретико-множественных тождеств в эквивалентности логики высказываний.

Теорема 2.41. *Рассмотрим два произвольных терма* $t_1, t_2 \in T$. *Имеет место теоретико-множественное тождество* $t_1 = t_2$ *тогда и только тогда, когда в логике высказываний верна эквивалентность* $\rho(t_1) \sim \rho(t_2)$.

Доказательство. Введём следующие обозначения. Для теоретико-множественного терма t запись $t(A_1, \ldots, A_n)$ означает, что среди $A_1, \ldots, A_n$ перечислены все переменные, входящие в данный терм t; при этом вполне может оказаться, что некоторые из этих переменных на самом деле в терм t не входят. Такое допущение, как это будет видно в дальнейшем, является достаточно удобным.

Рассмотрим терм $t = t(A_1, \ldots, A_n)$, пусть x – произвольный элемент (который может входить в некоторые из множеств $A_1, \ldots, A_n$, а может и не входить ни в одно из этих множеств). Тогда запись

$$[\rho(t)]^{A_i}_{(x \in A_i)}$$

обозначает утверждение (не являющееся формулой логики высказываний), полученное из формулы $\rho(t)$ заменой всех вхождений пропозициональной переменной A_i на выражение $(x \in A_i)$. Аналогичным образом определяется

$$[\rho(t)]^{A_i, \quad A_j}_{(x \in A_i), \ (x \in A_j)}$$

и т. д. Запись

$$[\rho(t)]^{A_1, \quad \ldots, \quad A_n}_{(x \in A_1), \ldots, \ (x \in A_n)}$$

обозначает утверждение, полученное из формулы $\rho(t)$ заменой всех вхождений пропозициональной переменной A_1 на выражение $(x \in A_1)$, … , всех вхождений пропозициональной переменной A_i на выражение $(x \in A_i)$, … , всех вхождений пропозициональной переменной A_n на выражение $(x \in A_n)$.

Напомним, что если зафиксированы конкретные множества $A_1, \ldots, A_n$, то значением терма $t = t(A_1, \ldots, A_n)$ является множество (полученное из множеств $A_1, \ldots, A_n$ последовательным применением теоретико-множественных операций, так как это указано в записи терма t). Поэтому в этом случае для любого элемента x либо выполнено $t(A_1, \ldots, A_n)$, либо выполнено $x \notin t(A_1, \ldots, A_n)$.

Лемма 2.42. *Рассмотрим терм* $t = t(A_1, \ldots, A_n)$. *Пусть зафиксированы множества* $A_1, \ldots, A_n$ *и некоторый элемент* x. *Выполнено*

$x \in t(A_1, \dots, A_n)$ *тогда и только тогда, когда утверждение* $[\rho(t)]^{A_1, \ \dots, \ A_n}_{(x \in A_1), \ \dots, \ (x \in A_n)}$ *является истинным.*

Доказательство будем проводить индукцией по построению терма t.

1. Простейшие термы.

Пусть $t = A$. Очевидно, что тогда утверждение $x \in t$ равносильно утверждению $x \in A$. Кроме того, как легко видеть,

$$[\rho(t)]^{A}_{(x \in A)} = (x \in A).$$

Следовательно, в этом случае выполнено $x \in t$ тогда и только тогда, когда утверждение $[\rho(t)]^{A}_{(x \in A)}$ является истинным.

2. Термы, полученные в результате применения теоретико-множественных операций.

Рассмотрим термы t, t_1 и t_2, без ограничения общности будем считать, что

$$t = t(A_1, \dots, A_n) \ , \ t_1 = t_1(A_1, \dots, A_n) \ \text{ и } \ t_1 = t_1(A_1, \dots, A_n).$$

Пусть терм t получен в результате применения теоретико-множественных операций из термов t_1 и t_2. Пусть зафиксированы множества $A_1, \dots, A_n$. Рассмотрим элемент x, нам нужно показать, что $x \in t(A_1, \dots, A_n)$ тогда и только тогда, когда утверждение

$$[\rho(t)]^{A_1, \ \dots, \ A_n}_{(x \in A_1), \ \dots, \ (x \in A_n)}$$

является истинным.

По индукционному предположению для термов t_1 и t_2 мы имеем $x \in t_1(A_1, \dots, A_n)$ тогда и только тогда, когда утверждение

$$[\rho(t_1)]^{A_1, \ \dots, \ A_n}_{(x \in A_1), \ \dots, \ (x \in A_n)}$$

является истинным, и $x \in t_2(A_1, \dots, A_n)$ тогда и только тогда, когда утверждение

$$[\rho(t_2)]^{A_1, \ \dots, \ A_n}_{(x \in A_1), \ \dots, \ (x \in A_n)}$$

является истинным.

Нам нужно рассмотреть три случая.

а) Пусть $t = t_1 \cup t_2$.

Тогда мы имеем: $x \in t$ равносильно тому, что ($x \in t_1$ или $x \in t_2$), по индукционному предположению это равносильно тому, что

$$[\rho(t_1)]^{A_1, \ \dots, \ A_n}_{(x \in A_1), \ \dots, \ (x \in A_n)}$$

является истинным или

$$[\rho(t_2)]^{A_1, \ \dots, \ A_n}_{(x \in A_1), \ \dots, \ (x \in A_n)}$$

является истинным, что, в свою очередь, равносильно истинности утверждения

$$\left([\rho(t_1)]^{A_1,\ \ \dots,\ \ A_n}_{(x\in A_1),\ \dots,\ (x\in A_n)} \vee [\rho(t_2)]^{A_1,\ \ \dots,\ \ A_n}_{(x\in A_1),\ \dots,\ (x\in A_n)}\right),$$

которое, как легко видеть, синтаксически совпадает с утверждением

$$[\rho(t_1) \vee \rho(t_2)]^{A_1,\ \ \dots,\ \ A_n}_{(x\in A_1),\ \dots,\ (x\in A_n)}$$

(поскольку сделать замену в дизъюнкции – это всё равно, что сначала сделать замену в каждом дизъюнктивном члене, а потом взять дизъюнкцию полученных выражений); последнее утверждение, по определению отображения ρ, совпадает с утверждением

$$[\rho(t_1 \cup t_2)]^{A_1,\ \ \dots,\ \ A_n}_{(x\in A_1),\ \dots,\ (x\in A_n)},$$

которое равно

$$[\rho(t)]^{A_1,\ \ \dots,\ \ A_n}_{(x\in A_1),\ \dots,\ (x\in A_n)},$$

так как, по условию, терм $t = t_1 \cup t_2$.

Поэтому в рассматриваемом случае утверждение

$$x \in t(A_1, \dots, A_n)$$

выполнено тогда и только тогда, когда утверждение

$$[\rho(t)]^{A_1,\ \ \dots,\ \ A_n}_{(x\in A_1),\ \dots,\ (x\in A_n)}$$

является истинным.

б) Пусть $t = t_1 \cap t_2$.

В этом случае мы имеем: $x \in t$ равносильно тому, что $x \in t_1$ и $x \in t_2$, по индукционному предположению это равносильно тому, что

$$[\rho(t_1)]^{A_1,\ \ \dots,\ \ A_n}_{(x\in A_1),\ \dots,\ (x\in A_n)}$$

является истинным и

$$[\rho(t_2)]^{A_1,\ \ \dots,\ \ A_n}_{(x\in A_1),\ \dots,\ (x\in A_n)}$$

является истинным, что, в свою очередь, равносильно истинности утверждения

$$\left([\rho(t_1)]^{A_1,\ \ \dots,\ \ A_n}_{(x\in A_1),\ \dots,\ (x\in A_n)} \ \&\ [\rho(t_2)]^{A_1,\ \ \dots,\ \ A_n}_{(x\in A_1),\ \dots,\ (x\in A_n)}\right),$$

которое синтаксически совпадает с утверждением

$$[\rho(t_1)\ \&\ \rho(t_2)]^{A_1,\ \ \dots,\ \ A_n}_{(x\in A_1),\ \dots,\ (x\in A_n)}$$

(поскольку сделать замену в конъюнкции – это всё равно, что сначала сделать замену в каждом конъюнктивном члене, а потом взять конъюнкцию полученных выражений); последнее утверждение, по определению отображения ρ, совпадает с утверждением

$$[\rho(t_1 \cap t_2)]^{A_1, \ \dots, \ A_n}_{(x \in A_1), \ \dots, \ (x \in A_n)},$$

которое равно

$$[\rho(t)]^{A_1, \ \dots, \ A_n}_{(x \in A_1), \ \dots, \ (x \in A_n)},$$

так как, по условию, терм $t = t_1 \cap t_2$.

Поэтому и в данном случае утверждение $x \in t(A_1, \dots, A_n)$ выполнено тогда и только тогда, когда утверждение

$$[\rho(t)]^{A_1, \ \dots, \ A_n}_{(x \in A_1), \ \dots, \ (x \in A_n)}$$

является истинным.

в) Случай $t = \overline{t_1}$ – упражнение.

Лемма 2.42 доказана.

Замечание 2.43. *Рассмотрим терм* $t = t(A_1, \dots, A_n)$. *Пусть зафиксированы множества* $A_1, \dots, A_n$ *и некоторый элемент* x. *Определим значения истинности пропозициональных переменных* $A_1, \dots, A_n$ *следующим образом: для каждого* $i \leq n$ *если* $x \in A_i$ *, то положим* $A_i = \text{и}$ *, а если* $x \notin A_i$ *, то положим* $A_i = \text{л}$. *В этом случае утверждение*

$$[\rho(t)]^{A_1, \ \dots, \ A_n}_{(x \in A_1), \ \dots, \ (x \in A_n)}$$

является истинным тогда и только тогда, когда формула логики высказываний $\rho(t)$ *является истинной при указанных значениях истинности пропозициональных переменных* $A_1, \dots, A_n$.

Доказательство. Заметим, что для того чтобы определить, является ли утверждение

$$[\rho(t)]^{A_1, \ \dots, \ A_n}_{(x \in A_1), \ \dots, \ (x \in A_n)}$$

истинным, мы должны в этом утверждении вместо выражений $x \in A_i$ подставить значения истинности этих выражений: если $x \in A_i$, то подставить истину, а если $x \notin A_i$, то – ложь. В результате такой подстановки мы получим в точности формулу логики высказываний $\rho(t)$, в которой подставлены значениях истины всех пропозициональных переменных $A_1, \dots, A_n$. Поэтому утверждение

$$[\rho(t)]^{A_1, \ \dots, \ A_n}_{(x \in A_1), \ \dots, \ (x \in A_n)}$$

истинно только тогда, когда формула логики высказываний $\rho(t)$ принимает значение истины при данных значениях пропозициональных переменных $A_1, \dots, A_n$.

Замечание 2.43 доказано.

Лемма 2.44. *Рассмотрим произвольные термы* $t_1, t_2 \in T$. *Если имеет место эквивалентность формул логики высказываний* $\rho(t_1) \sim \rho(t_2)$, *то для любых множеств* $A_1, \dots, A_n$ *верно равенство* $t_1(A_1, \dots, A_n) = t_2(A_1, \dots, A_n)$.

Доказательство. Предположим, что не для любых множеств $A_1, \dots, A_n$ верно равенство

$$t_1(A_1, \dots, A_n) = t_2(A_1, \dots, A_n).$$

Тогда существуют такие множества $A_1, \dots, A_n$, что

$$t_1(A_1, \dots, A_n) \neq t_2(A_1, \dots, A_n).$$

Значит, найдётся такой элемент x, что $x \in t_1$ и $x \notin t_2$ либо, наоборот, $x \notin t_1$ и $x \in t_2$. Без ограничения общности будем считать, что $x \in t_1$ и $x \notin t_2$. Следовательно, по лемме 2.42 получим, что утверждение

$$[\rho(t_1)]^{A_1, \quad \dots, \quad A_n}_{(x \in A_1), \quad \dots, \quad (x \in A_n)}$$

истинно, а утверждение

$$[\rho(t_2)]^{A_1, \quad \dots, \quad A_n}_{(x \in A_1), \quad \dots, \quad (x \in A_n)}$$

ложно. Определим значения пропозициональных переменных $A_1, \dots, A_n$ следующим образом: для каждого $i \leq n$ если $x \in A_i$, то положим $A_i = \text{и}$, а если $x \notin A_i$, то – $A_i = \text{л}$. При указанных значениях пропозициональных переменных $A_1, \dots, A_n$, по Замечанию 2.43, поскольку утверждение

$$[\rho(t_1)]^{A_1, \quad \dots, \quad A_n}_{(x \in A_1), \quad \dots, \quad (x \in A_n)}$$

является истинным, то формула логики высказываний $\rho(t_1)$ истинна, а поскольку утверждение

$$[\rho(t_2)]^{A_1, \quad \dots, \quad A_n}_{(x \in A_1), \quad \dots, \quad (x \in A_n)}$$

является ложным, то формула логики высказываний $\rho(t_2)$ ложна.

Стало быть, согласно определению 2.13, получаем, что формулы логики высказываний $\rho(t_1)$ и $\rho(t_2)$ не являются эквивалентными: $\rho(t_1) \nsim \rho(t_2)$ – противоречие с условием Леммы 2.44. Мы пришли к противоречию, предположив, что не для любых множеств $A_1, \dots, A_n$ верно равенство $t_1(A_1, \dots, A_n) = t_2(A_1, \dots, A_n)$.

Следовательно, для любых множеств $A_1, \dots, A_n$ имеет место тождество $t_1(A_1, \dots, A_n) = t_2(A_1, \dots, A_n)$.

Лемма 2.44 доказана.

Лемма 2.45. *Рассмотрим произвольные термы* $t_1, t_2 \in T$. *Если для любых множеств* $A_1, \dots, A_n$ *верно равенство*

$$t_1(A_1, \dots, A_n) = t_2(A_1, \dots, A_n),$$

то имеет место эквивалентность формул логики высказываний

$$\rho(t_1) \sim \rho(t_2).$$

Доказательство. Предположим, что для термов $t_1, t_2 \in T$ эквивалентность формул логики высказываний $\rho(t_1) \sim \rho(t_2)$ не является верной, т. е. $\rho(t_1) \nsim \rho(t_2)$. Тогда найдётся такой набор значений истинности пропозициональных переменных $A_1, \dots, A_n \in \{\text{и}, \text{л}\}$, что при этих значениях истинности переменных формула логики высказываний $\rho(t_1)$ является истинной, а формула логики высказываний $\rho(t_2)$ – ложной или, наоборот, формула $\rho(t_1)$ является ложной, а формула $\rho(t_2)$ – истинной. Без ограничения общности будем считать, что при данных значениях истинности пропозициональных переменных $A_1, \dots, A_n$ формула $\rho(t_1)$ является истинной, а формула $\rho(t_2)$ – ложной.

Рассмотрим натуральные числа 2 и 3. Определим множества $A_1, \dots, A_n$ следующим образом:

$$A_i = \begin{cases} \{2\}, & \text{если пропозициональная переменная } A_i = \text{и}; \\ \{3\}, & \text{если пропозициональная переменная } A_i = \text{л}. \end{cases}$$

Заметим, что при таком определении множеств $A_1, \dots, A_n$ для каждого $i \le n$ выполнено $2 \in A_i$ (где A_i – множество) тогда и только тогда, когда пропозициональная переменная $A_i = \text{и}$.

Используя Замечание 2.43, поскольку при данных значениях истинности пропозициональных переменных $A_1, \dots, A_n$ формула $\rho(t_1)$ является истинной, а формула $\rho(t_2)$ – ложной, получаем, что утверждение

$$[\rho(t_1)]^{A_1, \quad \dots, \quad A_n}_{(2 \in A_1), \quad \dots, \quad (2 \in A_n)}$$

является истинным, а утверждение

$$[\rho(t_2)]^{A_1, \quad \dots, \quad A_n}_{(2 \in A_1), \quad \dots, \quad (2 \in A_n)}$$

– ложным.

Следовательно, по лемме 2.42 выполнено $2 \in t_1$ и $2 \notin t_2$. Стало быть, при таких множествах $A_1, \dots, A_n$ термы t_1 и t_2 не равны: $t_1 \neq t_2$ – противоречие с условием Леммы 2.45.

Мы пришли к противоречию, предположив, что эквивалентность формул логики высказываний $\rho(t_1) \sim \rho(t_2)$ не является верной.

Следовательно, формулы $\rho(t_1)$ и $\rho(t_2)$ эквивалентны: $\rho(t_1) \sim \rho(t_2)$.

Лемма 2.45 доказана.

Из Лемм 2.44 и 2.45 вытекает доказательство Теоремы 2.41.

Теорема 2.41 доказана.

На этом мы заканчиваем изучение семантики логики высказываний. Мы вернёмся к синтаксису логики высказываний позже, при изучении *исчисления высказываний*.

Изложение первых двух параграфов мы намеренно проводили очень подробно, чтобы в деталях продемонстрировать основные приёмы и методы работы с формулами. Здесь мы имели дело со *значениями истинности*, существенно отличающимися от *числовых значений*, с которыми работают многие другие разделы математики.

Далее, в следующих параграфах, изложение материала будет значительно менее подробным, многие детали будут опускаться или оставляться в виде упражнений.

3. ЛОГИКА ПРЕДИКАТОВ

3.1. Понятие алгебраической системы, сигнатуры алгебраической системы

Определение 3.1. ***Декартовым произведением*** *множеств A и B называется множество $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$.*

Декартовым произведением *множеств $A_1, \dots, A_n$ называется множество $A_1 \times \dots \times A_n = \{(a_1, \dots, a_n) \mid a_1 \in A, \dots, a_n \in A_n\}$.*

Под множеством A^n будем понимать декартово произведение

$$\underbrace{A \times \dots \times A}_{n\ \text{раз}}.$$

Определение 3.2. *Рассмотрим множество A. Множество $P \subseteq A^n$ назовём* ***n-местным отношением****, определённым на множестве A.*

Определение 3.3. *Рассмотрим множество A. Отображение $f: A^n \to A$ назовём* ***n-местной функцией****, определённой на множестве A.*

Заметим, что каждой n-местной функции $f: A^n \to A$ можно сопоставить $(n+1)$-местный предикат G_f :

$$G_f = \{(a_1, \dots, a_{n+1}) \mid a_i \in A, i = 1, \dots, n+1 \text{ и } f(a_1, \dots, a_n) = a_{n+1}\}.$$

Предикат G_f называется ***графиком*** *функции f.*

Определение 3.4. ***Алгебраическая система*** *$\mathfrak{A}$ состоит из основного множества A и заданных на нём предикатов $P_1, \dots, P_n$, функций $f_1, \dots, f_k$ и констант $c_1, \dots, c_l$.*

Кортеж

$$\sigma = < P_1^{s_1}, \dots, P_n^{s_n}, \quad f_1^{r_1}, \dots, f_k^{r_k}, \quad c_1, \dots, c_l >$$

предикатных символов $P_1^{s_1}, \dots, P_n^{s_n}$, функциональных символов $f_1^{r_1}, \dots, f_k^{r_k}$ и константных символов $c_1, \dots, c_l$ называется ***сигнатурой*** *алгебраической системы $\mathfrak{A}$ и обозначается $\sigma = \sigma(\mathfrak{A})$. При этом запись $P_i^{s_i}$ означает, что P_i является s_i-местным предикатом алгебраической системы $\mathfrak{A}$, а запись $f_i^{r_i}$ означает, что f_i является r_i-местной функцией алгебраической системы $\mathfrak{A}$.*

Основное множество A также называется ***универсумом*** *алгебраической системы $\mathfrak{A}$ и обозначается $A = |\mathfrak{A}|$.*

Алгебраическая система обозначается

$$\mathfrak{A} = \langle A;\ P_1, \dots, P_n,\ f_1, \dots, f_k,\ c_1, \dots, c_l \rangle, \text{ или}$$
$$\mathfrak{A} =\ \langle A; \sigma \rangle, \text{ или }\ \mathfrak{A} = \langle |\mathfrak{A}|;\ \sigma \rangle.$$

Предикат P_i, определённый на алгебраической системе $\mathfrak{A}$, обозначается $P_i^{\mathfrak{A}}$, а функция f_i, определённая на алгебраической системе $\mathfrak{A}$, обозначается $f_i^{\mathfrak{A}}$. Т. е. для данной алгебраической системы $\mathfrak{A}$ имеем $P_i^{\mathfrak{A}} = P_i$ и $f_i^{\mathfrak{A}} = f_i$. Это обозначение нужно для того, чтобы различать предикаты и функции с одним и тем же именем (символом, входящим в сигнатуру), но определённые на разных алгебраических системах.

Определение 3.5. *Алгебраическая система, сигнатура которой содержит только символы функций и констант, называется* ***алгеброй***.

Алгебраическая система, сигнатура которой содержит только символы предикатов, называется ***моделью***.

3.2. Термы и формулы логики предикатов. Свободные и связанные переменные

Определение 3.6. *Пусть дана сигнатура*

$$\sigma =< P_1^{s_1}, \dots, P_n^{s_n}, f_1^{r_1}, \dots, f_k^{r_k},\ c_1, \dots, c_l >.$$

Определим понятие ***терма*** *сигнатуры* σ.

1. *Термами являются*:

а) переменные $x_1, x_2,\ x_3, \dots$;

б) константы: $c_1, \dots, c_l \in \sigma$.

2. *Если* $t_1, \dots, t_r$ *– термы и функциональный символ* $f^r \in \sigma$, *то* $f(t_1, \dots, t_r)$ *– терм.*

3. *Других термов нет.*

Заметим, что как переменные $x_1, x_2, \dots$, так и термы принимают свои значения на множестве A. Переменные $x_1, x_2, \dots$ называются *предметными переменными*, в отличие от *пропозициональных переменных* $A, B, C, \dots$, значениями которых являются истина и ложь.

Определение 3.7. *Пусть дана сигнатура*

$$\sigma =< P_1^{s_1}, \dots, P_n^{s_n}, f_1^{r_1}, \dots, f_k^{r_k}, c_1, \dots, c_l >.$$

Определим понятие ***формулы*** *сигнатуры* σ.

1. *Если* t_1 *и* t_2 *— термы, то* $t_1 = t_2$ *— формула.*

2. *Если* $t_1, \ldots, t_s$ *— термы и предикатный символ* $P^s \in \sigma$, *то* $P(t_1, \ldots, t_s)$ *— формула.*

3. *Если* φ *и* ψ *– формулы, то* $(\varphi \vee \psi)$, $(\varphi \,\&\, \psi)$, $(\varphi \to \psi)$, $\neg\varphi$, $\exists x\varphi(x)$ *и* $\forall x\varphi(x)$ *— формулы.*

4. *Других формул нет.*

Часть формулы, которая сама является формулой, называется ***подформулой*** данной формулы. Если $\forall x\, \psi$ или $\exists x\, \psi$ – подформула формулы φ, то говорят, что ψ является ***областью действия квантора*** $\forall x$ или $\exists x$ соответственно.

Вхождением переменной в формулу называется вхождение этой переменной в какой-либо терм этой формулы. Вхождение называется ***связанным***, если переменная находится в области действия квантора по этой переменной. Иначе вхождение называется ***свободным***. Переменная, имеющая хотя бы одно свободное вхождение в формулу, называется ***свободной***. Иначе она называется ***связанной***. Формула без свободных переменных называется ***предложением***.

Введём следующие обозначения:

$\boldsymbol{FV(\varphi)}$ — множество свободных переменных формулы φ;

$\boldsymbol{FV(t)}$ — множество переменных терма t;

$\boldsymbol{K(\sigma)}$ – класс алгебраических систем сигнатуры σ;

$\boldsymbol{T(\sigma)}$ – множество всех термов сигнатуры σ;

$\boldsymbol{F(\sigma)}$ – множество всех формул сигнатуры σ;

$\boldsymbol{S(\sigma)}$ – множество всех предложений сигнатуры σ.

Замечание 3.8. *Если* $\sigma_1 \subseteq \sigma_2$, *то*

1. $T(\sigma_1) \subseteq T(\sigma_2)$;
2. $F(\sigma_1) \subseteq F(\sigma_2)$;
3. $S(\sigma_1) \subseteq S(\sigma_2)$.

Доказательство. (1) $x_i \in T(\sigma_1) \Rightarrow x_i \in T(\sigma_2)$; $c \in T(\sigma_1) \Rightarrow c \in T(\sigma_2)$;

$$f(t_1, \ldots, t_n) \in T(\sigma_1) \Rightarrow \left\{\begin{matrix} t_1, \ldots, t_n \in T(\sigma_1) \Rightarrow t_1, \ldots, t_n \in T(\sigma_2) \\ f \in \sigma_1 \Rightarrow f \in \sigma_2 \end{matrix}\right\} \Rightarrow$$

$$\Rightarrow f(t_1, \ldots, t_n) \in T(\sigma_2).$$

(2) $\varphi = (t_1 = t_2) \in F(\sigma_1) \Rightarrow t_1, t_2 \in T(\sigma_1) \Rightarrow t_1, t_2 \in T(\sigma_2) \Rightarrow (t_1 = t_2) \in F(\sigma_2)$;

$\varphi = P(t_1, \dots, t_n) \in F(\sigma_1) \Rightarrow t_1, \dots, t_n \in T(\sigma_1), P \in \sigma_1 \Rightarrow$
$\Rightarrow t_1, \dots, t_n \in T(\sigma_2), P \in \sigma_2 \Rightarrow P(t_1, \dots, t_n) \in F(\sigma_2);$

$\varphi = (\varphi_1 \vee \varphi_2) \in F(\sigma_1) \Rightarrow \varphi_1, \varphi_2 \in F(\sigma_1) \Rightarrow \varphi_1, \varphi_2 \in F(\sigma_2) \Rightarrow$
$\Rightarrow (\varphi_1 \vee \varphi_2) \in F(\sigma_2).$

$\varphi = (\varphi_1 \& \varphi_2) \in F(\sigma_1) \Rightarrow \varphi_1, \varphi_2 \in F(\sigma_1) \Rightarrow \varphi_1, \varphi_2 \in F(\sigma_2) \Rightarrow$
$\Rightarrow (\varphi_1 \& \varphi_2) \in F(\sigma_2).$

$\varphi = (\varphi_1 \to \varphi_2) \in F(\sigma_1) \Rightarrow \varphi_1, \varphi_2 \in F(\sigma_1) \Rightarrow \varphi_1, \varphi_2 \in F(\sigma_2) \Rightarrow$
$\Rightarrow (\varphi_1 \to \varphi_2) \in F(\sigma_2).$

$\varphi = (\neg \varphi_1) \in F(\sigma_1) \Rightarrow \varphi_1 \in F(\sigma_1) \Rightarrow \varphi_1 \in F(\sigma_2) \Rightarrow (\neg \varphi_1) \in F(\sigma_2).$

$\varphi = (\forall x \varphi_1) \in F(\sigma_1) \Rightarrow \varphi_1 \in F(\sigma_1) \Rightarrow \varphi_1 \in F(\sigma_2) \Rightarrow (\forall x \varphi_1) \in F(\sigma_2).$

$\varphi = (\exists x \varphi_1) \in F(\sigma_1) \Rightarrow \varphi_1 \in F(\sigma_1) \Rightarrow \varphi_1 \in F(\sigma_2) \Rightarrow (\exists x \varphi_1) \in F(\sigma_2).$

(3) Упражнение.

Замечание 3.8 доказано.

Замечание 3.9. *Если $\sigma_1 \neq \sigma_2$, то $K(\sigma_1) \cap K(\sigma_2) = \emptyset$.*

Доказательство. Алгебраические системы $\mathfrak{A}_1 = \langle A_1; \sigma_1 \rangle \in K(\sigma_1)$ и $\mathfrak{A}_2 = \langle A_2; \sigma_2 \rangle \in K(\sigma_2)$ не могут быть равными, поскольку у них различны вторые компоненты – сигнатуры.

Замечание 3.9 доказано.

3.3. Значение терма на модели. Истинность формул на модели

Определение 3.10 (Значение терма на модели). *Пусть дана сигнатура σ, модель $\mathfrak{A} \in \boldsymbol{K(\sigma)}$ и множество переменных $\boldsymbol{X}$. Отображение $\boldsymbol{\gamma}: \boldsymbol{X} \to |\mathfrak{A}|$ называется* ***означиванием*** *переменных из множества $\boldsymbol{X}$ на модели $\mathfrak{A}$. Рассмотрим терм $\boldsymbol{t} \in \boldsymbol{T(\sigma)}$, пусть его переменные принадлежат множеству $\boldsymbol{X}$: $\boldsymbol{FV(t)} \subseteq \boldsymbol{X}$. Определим* ***значение терма $\boldsymbol{t}$ на модели $\mathfrak{A}$****, которое обозначается $\boldsymbol{t}^{\mathfrak{A}}[\boldsymbol{\gamma}]$.*

1. *Пусть $\boldsymbol{t} = \boldsymbol{x}$. Тогда $\boldsymbol{t}^{\mathfrak{A}}[\boldsymbol{\gamma}] = \boldsymbol{\gamma}(\boldsymbol{x})$.*

2. *Пусть $\boldsymbol{t} = \mathrm{c}$. Тогда $\boldsymbol{t}^{\mathfrak{A}}[\boldsymbol{\gamma}] = \mathrm{c}^{\mathfrak{A}}$.*
3. *Пусть $\boldsymbol{t} = \boldsymbol{f}(\boldsymbol{t_1}, \dots, \boldsymbol{t_n})$. Тогда $\boldsymbol{t}^{\mathfrak{A}}[\boldsymbol{\gamma}] = \boldsymbol{f}^{\mathfrak{A}}\left(\boldsymbol{t_1^{\mathfrak{A}}}[\boldsymbol{\gamma}], \dots, \boldsymbol{t_n^{\mathfrak{A}}}[\boldsymbol{\gamma}]\right)$.*

Пример. Пусть дана сигнатура $\sigma =< P^2, f_1^2, f_2^2, c_1, c_2 >$ и модель
$\mathfrak{N} =< N, \leq, +, *, 1, 0 >$

сигнатуры σ, т. е. $P = \leq$, $f_1 = +$, $f_2 = *$, $c_1^{\mathfrak{N}} = 1$ и $c_2^{\mathfrak{N}} = 0$.

Пусть $X = \{x_1, x_2\}$, определим означивание переменных $\gamma: X \to \mathbb{N}$ следующим образом: $\gamma(x_1) = 2$ и $\gamma(x_2) = 10$. Рассмотрим терм $t = f_1(x_1, x_2)$, тогда значение $t^{\mathfrak{N}}[\gamma]$ терма t на модели $\mathfrak{N}$ будет равно $t^{\mathfrak{N}}[\gamma] = 2 + 10$.

Определение 3.11 (Истинность формулы на модели). *Пусть дана сигнатура σ, модель $\mathfrak{A} \in K(\sigma)$, означивание $\gamma: X \to |\mathfrak{A}|$ и формула $\varphi \in F(\sigma)$, причём множество свободных переменных $FV(\varphi) \subseteq X$. Определим понятие* ***истинности формулы φ на модели $\mathfrak{A}$***. *То, что формула φ истинна на модели $\mathfrak{A}$, обозначается $\mathfrak{A} \vDash \varphi[\gamma]$.*

1. $\mathfrak{A} \vDash (t_1 = t_2)[\gamma]$ *тогда и только тогда, когда* $t_1^{\mathfrak{A}}[\gamma] = t_2^{\mathfrak{A}}[\gamma]$.
2. $\mathfrak{A} \vDash P(t_1, \dots, t_n)[\gamma]$ *тогда и только тогда, когда*
$$\mathfrak{A} \vDash P^{\mathfrak{A}}\left(t_1^{\mathfrak{A}}[\gamma], \dots, t_n^{\mathfrak{A}}[\gamma]\right).$$
3. $\mathfrak{A} \vDash (\varphi_1 \vee \varphi_2)[\gamma]$ *тогда и только тогда, когда*
$$\mathfrak{A} \vDash \varphi_1[\gamma] \text{ или } \mathfrak{A} \vDash \varphi_2[\gamma].$$
4. $\mathfrak{A} \vDash (\varphi_1 \,\&\, \varphi_2)[\gamma]$ *тогда и только тогда, когда*
$$\mathfrak{A} \vDash \varphi_1[\gamma] \text{ и } \mathfrak{A} \vDash \varphi_2[\gamma].$$
5. $\mathfrak{A} \vDash (\varphi_1 \to \varphi_2)$ *тогда и только тогда, когда*
$$\text{если } \mathfrak{A} \vDash \varphi_1[\gamma], \text{ то } \mathfrak{A} \vDash \varphi_2[\gamma].$$
6. $\mathfrak{A} \vDash \neg\varphi[\gamma]$ *тогда и только тогда, когда* $\mathfrak{A} \nvDash \varphi[\gamma]$.
7. $\mathfrak{A} \vDash \exists x\, \varphi[\gamma]$ *тогда и только тогда, когда найдётся элемент* $a \in |\mathfrak{A}|$, *для которого выполнено условие* $\mathfrak{A} \vDash \varphi[\gamma_1]$, *где*
$$\gamma_1: (X \cup \{x\}) \to |\mathfrak{A}| \text{ и } \gamma_1(y) = \begin{cases} a, & y = x; \\ \gamma(y), & y \neq x. \end{cases}$$
8. $\mathfrak{A} \vDash \forall x\, \varphi[\gamma]$ *тогда и только тогда, когда для любого элемента* $a \in |\mathfrak{A}|$ *выполнено* $\mathfrak{A} \vDash \varphi[\gamma_1]$, *где*
$$\gamma_1: (X \cup \{x\}) \to |\mathfrak{A}| \text{ и } \gamma_1(y) = \begin{cases} a, & y = x; \\ \gamma(y), & y \neq x. \end{cases}$$

Определение 3.12. *Формула называется* ***истинной*** *на данной модели, если она истинна при любом означивании. Формула называется* ***ложной*** *на данной модели, если она ложна при любом означивании. Формула называется* ***тождественно истинной****, если она истинна на любой модели при любом означивании. Формула называется* ***тождественно ложной****, если она ложна на любой модели* *при любом означивании. Формула называется **выполнимой**, если она не является тождественно ложной. Формула называется **опровержимой**, если она не является тождественно истинной.*

Замечание 3.13. *1. Формула φ – тождественно истинна тогда и только тогда, когда $\neg\varphi$ – тождественно ложна.*

2. Формула φ – выполнима тогда и только тогда, когда $\neg\varphi$ – опровержима.

Доказательство: упражнение.

3.4. Семантическая эквивалентность формул. Предваренная нормальная форма.

Определение 3.14. *Формулы φ и ψ называются **семантически эквивалентными** (или просто **эквивалентными**),* обозначается *$\varphi \sim \psi$, если для любой модели $\mathfrak{A} \in K(\sigma(\varphi) \cup \sigma(\psi))$ и любого означивания $\gamma\colon \big(FV(\varphi) \cup FV(\psi)\big) \to |\mathfrak{A}|$ выполнено:*

$$\mathfrak{A} \vDash \varphi[\gamma] \ \text{ тогда и только тогда, когда } \ \mathfrak{A} \vDash \psi[\gamma].$$

Замечание 3.15. *Отношение семантической эквивалентности формул является отношением эквивалентности.*

Доказательство: упражнение.

Предложение 3.16. *Имеют место следующие эквивалентности формул:*

1. $\neg(\forall x\, \varphi) \sim \exists x\, \neg\varphi$;
2. $\neg(\exists x\, \varphi) \sim \forall x\, \neg\varphi$;
3. $\forall x\, (\varphi \,\&\, \psi) \sim \big((\forall x\varphi) \& (\forall x\psi)\big)$;
4. $\exists\, x\, (\varphi \vee \psi) \sim \big((\exists x\varphi) \vee (\exists x\psi)\big)$;
5. $\forall x\, (\varphi \,\&\, \xi) \sim \big((\forall x\varphi) \& \,\xi\big)$, где $x \notin FV(\xi)$;
6. $\forall x\, (\varphi \vee \xi) \sim \big((\forall x\varphi) \vee \xi\big)$, где $x \notin FV(\xi)$;
7. $\exists\, x\, (\varphi \vee \xi) \sim \big((\exists x\varphi) \vee \xi\big)$, где $x \notin FV(\xi)$;
8. $\exists\, x\, (\varphi \,\&\xi) \sim \big((\exists x\varphi)\&\xi\big)$, где $x \notin FV(\xi)$;
9. $\forall x\varphi(x) \sim \forall y\varphi(y)$, где $x, y \notin FV(\varphi(z))$;
10. $\exists x\varphi(x) \sim \exists y\varphi(y)$, где $x, y \notin FV(\varphi(z))$.

Доказательство. Докажем пункт (3).

Выберем модель $\mathfrak{A} \in K\big(\sigma(\varphi) \cup \sigma(\psi)\big)$ и означивание

$$\gamma: \big(FV(\varphi) \cup FV(\psi)\big) \to |\mathfrak{A}|.$$

Тогда $\mathfrak{A} \vDash \forall x\, (\varphi \,\&\, \psi)[\gamma] \Leftrightarrow$

$\Leftrightarrow$ для любого элемента $a \in |\mathfrak{A}|$ выполнено $\mathfrak{A} \vDash (\varphi \,\&\, \psi)[\gamma_1]$ (где $\gamma_1: (X \cup \{x\}) \to |\mathfrak{A}|$ и $\gamma_1(y) = \begin{cases} a, & y = x; \\ \gamma(y), & y \neq x; \end{cases}$) $\Leftrightarrow$

$\Leftrightarrow$ для любого элемента $a \in |\mathfrak{A}|$ выполнено $\mathfrak{A} \vDash (\varphi[\gamma_1] \,\&\, \psi[\gamma_1]) \Leftrightarrow$

$\Leftrightarrow$ для любого элемента $a \in |\mathfrak{A}|$ выполнено ($\mathfrak{A} \vDash \varphi[\gamma_1]$ и $\mathfrak{A} \vDash \psi[\gamma_1]$) $\Leftrightarrow$

$\Leftrightarrow$ для любого элемента $a \in |\mathfrak{A}|$ выполнено $\mathfrak{A} \vDash \varphi[\gamma_1]$ и
для любого элемента $a \in |\mathfrak{A}|$ выполнено $\mathfrak{A} \vDash \psi[\gamma_1] \Leftrightarrow$

$\Leftrightarrow$ $\mathfrak{A} \vDash \forall x\, \varphi[\gamma]$ и $\mathfrak{A} \vDash \forall x\, \psi[\gamma]$ $\Leftrightarrow$ $\mathfrak{A} \vDash (\forall x \varphi \,\&\, \forall x \psi)[\gamma]$.

Пункты (1, 2) и (4–10) – упражнение.

Предложение 3.16 доказано.

Предложение 3.17. *Существуют формулы φ и ψ, для которых выполнено:*

а) $\forall x(\varphi \vee \psi) \nsim (\forall x \varphi \vee \forall x \psi)$;

б) $\exists x(\varphi \,\&\, \psi) \nsim (\exists x \varphi \,\&\, \exists x \psi)$.

Доказательство. Рассмотрим алгебраическую систему

$$\mathfrak{N} = \langle \mathbb{N}, \leq, 1 \rangle$$

и формулы

$$\varphi(x) = (x \leq 1) \text{ и } \psi(x) = \neg(x \leq 1).$$

Тогда

а) $\mathfrak{N} \vDash \forall x\big(x \leq 1 \vee \neg(x \leq 1)\big)$; кроме того,

$$\mathfrak{N} \nvDash \forall x(x \leq 1) \text{ и } \mathfrak{N} \nvDash \forall x\, \neg(x \leq 1).$$

Поэтому

$$\mathfrak{N} \nvDash \big(\forall x(x \leq 1) \vee \forall x\, \neg(x \leq 1)\big).$$

Следовательно,

$$\forall x(\varphi \vee \psi) \nsim (\forall x \varphi \vee \forall x \psi).$$

б) $\mathfrak{N} \nvDash \exists x\big(x \leq 1 \,\&\, \neg(x \leq 1)\big)$. При этом

$$\mathfrak{N} \vDash \exists x(x \leq 1) \text{ и } \mathfrak{N} \vDash \exists x \neg(x \leq 1).$$

Поэтому

$$\mathfrak{N} \vDash \big(\exists x(x \leq 1) \& \exists x \neg(x \leq 1)\big).$$

Следовательно,

$$\exists x(\varphi \,\&\, \psi) \nsim (\exists x \varphi \,\&\, \exists x \psi).$$

Предложение 3.17 доказано.

Предложение 3.18. *Существует формула* φ*, для которой выполнено*

$$\forall x \exists y\, \varphi(x, y) \nsim \exists y \forall x\, \varphi(x, y).$$

Доказательство. Рассмотрим алгебраическую систему

$$\mathfrak{N} = \langle \mathbb{N}, \leq \rangle$$

и формулу

$$\varphi(x, y) = (x \leq y).$$

Тогда

$$\mathfrak{N} \vDash \forall x \exists y (x \leq y) \text{ и } \mathfrak{N} \nvDash \exists y \forall x\, (x \leq y).$$

Следовательно,

$$\forall x \exists y\, \varphi(x, y) \nsim \exists y \forall x\, \varphi(x, y).$$

Предложение 3.18 доказано.

Определение 3.19. *Формула* φ *находится в* ***предваренной нормальной форме****, если она имеет вид*

$$\varphi = Q_1 x_1 Q_2 x_2 \dots Q_n x_n \psi(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n),$$

где $Q_i \in \{\forall, \exists\}$*, а* ψ *– бескванторная формула. Предваренную нормальную форму называют также* ***пренексной нормальной формой****.*

Предложение 3.20. *Для любой* φ *существует эквивалентная ей формула, находящаяся в предваренной нормальной форме.*

Доказательство. Алгоритм приведения формулы к предваренной нормальной форме.

1. Избавляемся от импликации, используя эквивалентность 12 из Следствия 2.16.

2. Вносим отрицание под кванторы. Используются эквивалентности 1 и 2 из Предложения 3.16, а также эквивалентности 9–11 из Следствия 2.16.

3. Переименовываем переменные, по которым действуют кванторы, так, чтобы были выполнены следующие условия: во-первых, чтобы разные кванторы действовали по разным переменным и, во-вторых, чтобы каждая переменная имела либо только свободные, либо только связанные вхождения.

Используются эквивалентности 9 и 10 из Предложения 3.16.

4. Выносим кванторы наружу. Используются эквивалентности 5–8 из Предложения 3.16.

В результате получается формула, находящаяся в предваренной нормальной форме. В силу Замечания 3.15, а именно в силу транзитивности отношения семантической эквивалентности, полученная формула будет эквивалентна исходной.

Предложение 3.20 доказано.

4. ОТНОШЕНИЯ И ФУНКЦИИ

4.1. Основные определения

Определение 4.1. *Множество* $G \subseteq A \times B$ *называется* ***соответствием*** *между множествами* A *и* B.

Определение 4.2. *Пусть* $G \subseteq A \times B,\ H \subseteq B \times C$.

Композицией *соответствий* G *и* H *называется множество*

$$G \circ H = \{ (a, c) \mid \exists b \in B \text{ такое, что } (a, b) \in G \text{ и } (b, c) \in H) \}.$$

Соответствием, ***обратным*** *к соответствию* G, *называется множество* $G^{-1} = \{(b, a) \mid (a, b) \in G\}$.

Множество $id_A = \{(a, a) \mid a \in A\}$ *называется* ***отношением тождества****, определённым на множестве* A.

Замечание 4.3. *Для любого множества* A *справедливы следующие утверждения:*

1) $(id_A)^{-1} = id_A$;

2) $(A^2)^{-1} = A^2$;

3) $id_A \circ (id_A)^{-1} = id_A$;

4) $A^2 \circ (A^2)^{-1} = A^2$.

Доказательство: упражнение.

Замечание 4.4.

1. $\emptyset^{-1} = \emptyset$.
2. $\emptyset \circ \emptyset^{-1} = \emptyset$.

Доказательство: упражнение.

Определение 4.5. *Пусть* $F \subseteq A \times B$. *Соответствие* F *называется* ***функцией*** *(графиком функции), если для любого элемента* $a \in A$ *существует единственный элемент* $b \in B$ *такой, что* $(a, b) \in F$, *т. е. выполнено следующее.*

1. *Для любого элемента* $a \in A$ *существует такой элемент* $b \in B$, *что* $(a, b) \in F$.
2. *Для любых элементов* $a \in A$ *и* $b_1, b_2 \in B$ *если* $(a, b_1), (a, b_2) \in F$, *то* $b_1 = b_2$.

Далее, если соответствие F является функцией, то вместо записи $F \subseteq A \times B$ мы будем писать $f: A \rightarrow B$, а вместо записи $(a, b) \in F$ будем писать $f(a) = b$.

Если $A = \mathrm{C}^n$, то функцию $f: \mathrm{C}^n \rightarrow B$ можно рассматривать как n-местную функцию, определённую на множестве A.

Определение 4.6. *Пусть* $\mathrm{C} \subseteq A \times B$. ***Проекциями*** *множества* C *на множества* A *и* B *называются множества*

$pr_A \mathrm{C} = \{a | (a, b) \in C\} \subseteq A$ и $pr_B \mathrm{C} = \{b | (a, b) \in C\} \subseteq B$.

Замечание 4.7. *Если* $F \subseteq A \times B$ *является функцией, то выполнено* $pr_A F = A$.

Доказательство: упражнение.

Определение 4.8. *Функция* F *называется* ***обратимой****, если соответствие* F^{-1} *также является функцией.*

Предложение 4.9. *Функция* $F \subseteq A \times B$ *является обратимой тогда и только тогда, когда для любого элемента* $b \in B$ *существует единственный элемент* $a \in A$ *такой, что* $(a, b) \in F$, *т. е. когда выполнены следующие условия.*

1. *Для любого элемента* $b \in B$ *существует такой элемент* $a \in A$, *что* $(a, b) \in F$ *(отображение «на», сюръективность).*

2. *Для любых элементов* $a_1, a_2 \in A$ *и* $b \in B$ *если* (a_1, b), $(a_2, b) \in F$, *то* $a_1 = a_2$ *(отображение разнозначно, инъективность).*

Доказательство. Функция F обратима тогда и только тогда, когда соответствие F^{-1} является функцией. Следовательно, для F^{-1} должны выполняться условия из Определения 4.5, т. е. условия (1) и (2) данного предложения.

Предложение 4.9 доказано.

Предложение 4.10. *Если функция* $F \subseteq A \times B$ *обратима, то*

$$F \circ F^{-1} = id_A \text{ и } F^{-1} \circ F = id_B.$$

Доказательство. По определению композиции соответствий (см. Определение 4.2), в силу Предложения 4.9 имеем:

$$F \circ F^{-1} \leftrightharpoons \{(a, a) | \exists b \in B\colon (a, b) \in F \text{ и } (b, a) \in F^{-1}\} = id_A;$$

$$F^{-1} \circ F \leftrightharpoons \{(b, b) | \exists a \in A\colon (b, a) \in F^{-1} \text{ и } (a, b) \in F\} = id_B.$$

Предложение 4.10 доказано.

Определение 4.11. *Функция F называется **взаимно-однозначным отображением (биекцией)**, если она является обратимой,* т. е. *разнозначной (инъективной) и «на» (сюръективной).*

4.2. Свойства бинарных отношений

Рассмотрим бинарное отношение $R \subseteq A^2$, определённое на множестве A. Будем записывать aRb, если $(a, b) \in R$.

Определение 4.12. *Перечислим основные свойства бинарных отношений.*

1. *Рефлексивность:* $\forall a \in A \ (aRa)$.
2. *Иррефлексивность:* $\forall a \in A \ \neg(aRa)$.
3. *Симметричность:* $\forall a, b \in A \ (aRb \Leftrightarrow bRa)$.
4. *Антисимметричность:* $\forall a, b \in A \left((aRb \,\&\, bRa) \Rightarrow (a = b)\right)$.
5. *Транизитивность:* $\forall a, b, c \in A \left((aRb \,\&\, bRc) \Rightarrow aRc\right)$.
6. *Линейность:* $\forall a, b \in A \ (aRb \vee bRa)$.

Определение 4.13. *Отношение R называется отношением:*

*1) **предпорядка**, если оно обладает свойствами 1 и 5;*

*2) **эквивалентности**, если оно обладает свойствами 1, 3 и 5;*

*3) **частичного порядка**, если оно обладает свойствами 1, 4 и 5;*

*4) **линейного порядка**, если оно обладает свойствами 1, 4, 5 и 6;*

*5) **строгого частичного порядка**, если оно обладает свойствами 2, 4 и 5.*

Замечание 4.14.

1. A^2 *– отношение эквивалентности.*

2. id_A *– отношение эквивалентности, частичного порядка.*

3. id_A *– отношение линейного порядка тогда и только тогда, когда* $\mathrm{A} = \emptyset$ *или* A *– одноэлементное.*

4. $\emptyset$ *– симметрично и антисимметрично.*

Доказательство: упражнение.

4.3. Отношение эквивалентности

Определение 4.15. *Бинарное отношение $R \subseteq A^2$ называется* ***отношением эквивалентности****, если оно рефлексивно, симметрично и транзитивно. Обычно обозначается знаком $\sim$, т. е. $a \sim b$.*

Если $\sim\, \subseteq A^2$ – отношение эквивалентности на множестве A, то множество

$$[a] = [a]_\sim = \{b \in A \mid a \sim b\}$$

называется ***классом эквивалентности,*** *или* ***смежным классом,*** *или* ***фактор-классом****.*

Множество всех классов эквивалентности множества A называется ***фактор-множеством***. Обозначается оно так:

$$A/_\sim = \{\, [a]_\sim \mid a \in A\}.$$

Предложение 4.16. *Пусть $\sim$ – отношение эквивалентности, определённое на множестве A. Тогда*

1) $\bigcup_{a\in A}[a] = A$*;*

2) $a \sim b \;\Rightarrow\; [a] = [b]$;

3) $a \nsim b \;\Rightarrow\; [a] \cap [b] = \emptyset$.

Доказательство

1. Для любого $a \in A$ имеем $[a] \subseteq A$. Тогда $\bigcup_{a\in A}[a] \subseteq$ A. С другой стороны, для любого элемента $c \in A$ имеем $c \sim a$. Следовательно, $c \in [c]$. Откуда получаем $c \in \bigcup_{a\in A}[a]$. А значит, $A \subseteq \bigcup_{a\in A}[a]$.

2. Пусть для $a, b \in A$ имеем $a \sim b$. Тогда если $c \in [a]$, то $c \sim a$. Следовательно, $c \sim b$. А значит, $c \in [b]$, т. е. [a] ⊆ [b].

Аналогично доказываем, что $[b] \subseteq [a]$.

3. Пусть $a \nsim b$. Допустим, что $[a] \cap [b] \neq \emptyset$. Тогда найдётся такой элемент $c \in A$, что $c \in [a] \cap [b]$. Тогда из $c \sim a$, $c \sim b$ следует $a \sim b$. Пришли к противоречию с условием.

Предложение 4.16 доказано.

Определение 4.17. *Пусть I – множество индексов такое, что для любого индекса $i \in I$ имеем $B_i \subseteq A$. Класс множеств $\{B_i\}_{i\in I}$ называется* ***разбиением*** *множества A, если выполнены следующие условия:*

1) $\bigcup_{i\in I}\{B_i\} = A$*;*

2) $\forall i, j\ \big((i \neq j) \Rightarrow (B_i \cap B_j = \emptyset)\big)$;

3) $\forall i \in I\ (B_i \neq \emptyset)$.

Предложение 4.18. *Пусть* $R \in A^2$, $\{B_i\}_{i \in I}$ *− разбиение множества A. Определим отношение*

$$R = \{(a, b) \mid \exists i \in I: (a, b) \in B_i\}.$$

Тогда

а) R *– отношение эквивалентности;*

б) $\{[a]_R \mid a \in A\} = \{B_i \mid i \in I\}$.

Доказательство: упражнение.

Предложение 4.19. *Каждая эквивалентность определяет множество фактор-классов, которое является разбиением множества, и каждое разбиение определяет отношение эквивалентности, для которого это разбиение будет множеством фактор-классов.*

Доказательство: упражнение.

4.4. Отношение порядка. Упорядоченные множества

Определение 4.20. $R \subseteq A^2$ *называется отношением* ***частичного порядка****, если оно рефлексивно, антисимметрично и транзитивно. Множество A с заданным на нем отношением частичного порядка будем называть* ***частично упорядоченным множеством*** *(ЧУМ).*

Определение 4.21. $R \subseteq A^2$ *называется отношением* ***линейного порядка****, если оно рефлексивно, антисимметрично, транзитивно и линейно. Множество A с заданным на нем отношением линейного порядка будем называть* ***линейно упорядоченным множеством*** *(ЛУМ).*

В дальнейшем отношение частичного / линейного порядка будем обозначать символом $\leq$.

Определение 4.22. *Пусть* $\langle A, \leq \rangle$ *– частично упорядоченное множество,* $a \in A$. *Тогда*

1) a *называется наименьшим элементом множества A, если*

$$\forall b \in A\ (a \leq b);$$

2) a *называется наибольшим элементом множества A, если*

$$\forall b \in A\ (b \leq a);$$

3) a *называется минимальным элементом множества A, если*

$$\forall b \in A\ \big((b \leq a) \Rightarrow (a = b)\big);$$

4) a называется максимальным элементом множества A, если

$$\forall b \in A\left((a \leq b) \Rightarrow a = b\right).$$

Замечание 4.23. *Наибольший элемент всегда является максимальным, а наименьший элемент – минимальным.*

Доказательство. Пусть $\langle A, \leq \rangle$ – частично упорядоченное множество. Пусть a – наибольший элемент. Тогда для любого $b \in A$ имеем $b \leq a$. Следовательно, в силу антисимметричности, если $a \leq b$, то $a = b$. Таким образом, получим, что a – максимальный элемент.

Аналогично доказывается для наименьшего.

Определение 4.24. *Отношение $R \subseteq A^2$ называется строгим частичным порядком, если оно иррефлексивно, антисимметрично и транзитивно.*

Предложение 4.25. *Пусть дана модель $\langle A, \leq \rangle$. Определим отношение $<$ следующим образом: положим $a < b$, если $a \leq b$ и $a \neq b$. В таком случае $\langle A, \leq \rangle$ – частично упорядоченное множество тогда и только тогда, когда $\langle A, < \rangle$ – строго частично упорядоченное множество.*

Доказательство: упражнение.

Предложение 4.26. *Пусть $\langle A, \leq \rangle$ – частично упорядоченное множество и A конечно. Тогда для любого $a \in A$ найдутся такие $b, c \in A$, что $b \leq a \leq c$ и b – минимальный, c – максимальный.*

Доказательство. Докажем существование c. Если a является максимальным, то $c = a$. Если a не максимальный, то найдётся $a_1 \in A$ такой, что $a \leq a_1$ и $a \neq a_1$, т. е. $a < a_1$. Если a_1 – максимальный, то $c = a_1$. Если a_1 не максимальный, то найдётся $a_2 \in A$ такой, что $a_1 < a_2$. И т. д., пока не найдётся элемент $a_n = c$, а он найдётся, так как A конечно.

Аналогично для минимального элемента b.

Предложение 4.26 доказано.

Предложение 4.27. *Пусть $\langle A, \leq \rangle$ – частично упорядоченное множество, $a \in A$. Тогда если a – наибольший элемент, то a – единственный максимальный элемент; если a – наименьший элемент, то a – единственный минимальный элемент.*

Доказательство. Пусть a – наибольший элемент, а b – максимальный. Следовательно, $b \leq a$ и, значит, $a = b$. Аналогично для наименьшего элемента.

Предложение 4.27 доказано.

Предложение 4.28. *Пусть* $\langle A, \leq \rangle$ *– конечное частично упорядоченное множество и* $a \in A$. *Тогда если* a *– единственный максимальный элемент, то* a *– наибольший элемент; если* a *– единственный минимальный элемент, то* a *– наименьший элемент.*

Доказательство. Пусть a – единственный максимальный элемент, покажем, что он является наибольшим. Рассмотрим произвольный элемент $b \in A$. В силу конечности множества A, найдётся максимальный элемент c такой, что $b \leq c$. Поскольку a – единственный максимальный элемент, имеем $a = c$, поэтому $b \leq a$. Следовательно, a – наибольший элемент.

Предложение 4.28 доказано.

Следствие 4.29.

1) *В конечном частично упорядоченном множестве элемент является наибольшим (наименьшим) тогда и только тогда, когда он является единственным максимальным (минимальным).*

2) *В конечном частично упорядоченном множестве* $\langle A, \leq \rangle$ *существует наибольший (наименьший) элемент только тогда, когда в* A *максимальный (соответственно, минимальный) элемент единственен.*

Доказательство: упражнение.

Замечание 4.30. $\langle \mathbb{N}, \leq \rangle, \langle \mathbb{Z}, \leq \rangle, \langle \mathbb{Q}, \leq \rangle, \langle \mathbb{R}, \leq \rangle$ *– линейно упорядоченные множества.*

Доказательство: упражнение.

Предложение 4.31. Пусть $\langle A, \leq \rangle$ *– линейно упорядоченное множество и* $a \in A$.

1. a *– наименьший элемент тогда и только тогда, когда* a *– минимальный.*

2. a *– наибольший элемент тогда и только тогда, когда* a *– максимальный.*

Доказательство. Если a – наименьший элемент, то a – минимальный в силу Замечания 4.23.

Допустим, что a – минимальный элемент. В силу линейности порядка для любого элемента $b \in A$ имеем $a \leq b$ или $b \leq a$.

Пусть неверно, что $a \leq b$, тогда выполнено $b \leq a$. Следовательно, так как a – минимальный, имеем $a = b$ и, значит, $a \leq b$. Получили противоречие, поэтому элемент a – наименьший.

Аналогично для максимального элемента.

Предложение 4.31 доказано.

Следствие 4.32. В конечном линейно упорядоченном множестве всегда существует наименьший и наибольший элемент.

Доказательство: упражнение.

4.5. Решётки

Определение 4.33. *Пусть $\langle A, \leq \rangle$ – частично упорядоченное множество, $M \subseteq A$ и $a \in A$.*

1. a – верхняя грань M (обозначается $M \leq a$), если

$$\forall b \in M\ (b \leq a).$$

2. a – нижняя грань M (обозначается $a \leq M$), если

$$\forall b \in M\ (a \leq b).$$

3. a – точная верхняя грань M ($a = sup_A\, M$), если a – наименьшая из всех верхних граней, т. е.

a. $M \leq a$;

b. $\forall c \in A\ (M \leq c \Rightarrow a \leq c)$.

4. a – точная нижняя грань M ($a = inf_A\, M$), если a – наибольшая из всех нижних граней, т. е.

a. $a \leq M$;

b. $\forall c \in A\ (c \leq M \Rightarrow c \leq a)$.

Предложение 4.34. *Пусть $\langle A, \leq \rangle$ – частично упорядоченное множество, $M \subseteq A$ и $a \in M$. Тогда*

1. если $M \leq a$, то $a = sup_A\, M$;

2. если $a \leq M$, то $a = inf_A\, M$;

3. $M \leq a$ тогда и только тогда, когда $a = sup_A\, M$, что выполнено тогда и только тогда, когда a – наибольший в M;

4. $a \leq M$ тогда и только тогда, когда $a = inf_A\, M$, что выполнено тогда и только тогда, когда a – наименьший в M.

Доказательство: упражнение.

Определение 4.35. *Пусть* $\langle A, \leq \rangle$ *– частично упорядоченное множество.* $\langle A, \leq \rangle$ *называется* ***решёточно упорядоченным множеством*** *(РУМ), если оно частично упорядоченно и для любых* $a, b \in A$ *существуют* $sup_A\{a, b\}$ *и* $inf_A\{a, b\}$.

Определение 4.36. *Введем обозначения:* $a \cup b = sup_A\{a, b\}$ *и* $a \cap b = inf_A\{a, b\}$. *Тогда система* $\langle A, \cup, \cap \rangle$ *называется* ***решёткой****, система* $\langle A, \cup \rangle$ *–* ***верхней полурешёткой****, а система* $\langle A, \cap \rangle$ *–* ***нижней полурешёткой***.

Определение 4.37. *Пусть* X *– множество. Тогда множество*

$$\rho(X) = \{Y |\; Y \subseteq X\}$$

называется множеством всех подмножеств множества X*, или* ***множеством-степенью*** *множества* X.

Предложение 4.38. *Множество* $\langle \rho(X), \subseteq \rangle$ *является решёточно упорядоченным множеством.*

Доказательство.

1. Рефлексивность. Для любого $A \subseteq X$ имеем $A \subseteq A$.
2. Антисимметричность. Если для множеств $A, B \subseteq X$ выполнено $A \subseteq B$ и $B \subseteq A$, то, по определению равенства множеств, получаем $A = B$.
3. Транзитивность. Если для множеств $A, B, C \subseteq X$ выполнено $A \subseteq B$ и $B \subseteq C$, то, по определению отношения включения, получаем $A \subseteq C$.
4. Для любых множеств $A, B \subseteq X$ выполнено:

$$\sup_A\{A, B\} = A \cup B,\ \inf_A\{A, B\} = A \cap B.$$

Доказательство: упражнение.

Предложение 4.38 доказано.

Предложение 4.39. *Если* $\langle A, \leq \rangle$ *– линейно упорядоченное множество, то* $< A, \leq >$ *– решёточно упорядоченное множество.*

Доказательство. Из свойства линейности вытекает, что для любых $a, b \in A$ имеет место $a \leq b$ или $b \leq a$. Тогда определим $\sup_A\{a, b\} = \max\{a, b\}$ и $\inf_A\{a, b\} = \min\{a, b\}$. Доказательство: упражнение.

Предложение 4.39 доказано.

5. БУЛЕВЫ АЛГЕБРЫ

5.1. Определение булевой алгебры. Примеры булевых алгебр. Свойства булевых алгебр

Определение 5.1. *Алгебраическая система* $\mathfrak{A} = \langle A; \cap, \cup, ^{-}, 0, 1\rangle$ *называется булевой алгеброй, если для любых* $a, b, c \in A$ *выполняются следующие условия:*

1) $a \cup b = b \cup a$;
2) $a \cap b = b \cap a$;
3) $a \cup (b \cup c) = (a \cup b) \cup c$;
4) $a \cap (b \cap c) = (a \cap b) \cap c$;
5) $a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$;
6) $a \cap (b \cup c) = (a \cup b) \cap (a \cup c)$;
7) $(\overline{a \cup b}) = \bar{a} \cap \bar{b}$;
8) $\left(\overline{a \cap b}\right) = \bar{a} \cup \bar{b}$;
9) $a \cup a = a$;
10) $a \cap a = a$;
11) $\bar{\bar{a}} = a$;
12) $a \cup \bar{a} = 1$;
13) $a \cap \bar{a} = 0$;
14) $a \cup 0 = a$;
15) $a \cap 0 = 0$;
16) $a \cup 1 = 1$;
17) $a \cap 1 = a$.

Предложение 5.2. $\langle \rho(X); \cap, \cup, ^{-}, \emptyset, X\rangle$ *– булева алгебра.*
Доказательство: упражнение.

Определение 5.3. *Введем следующие обозначения:*

$F_n = F(A_1, \dots, A_n)$ ={φ | φ *– формула логики высказываний от пропозициональных переменных* $A_1, \dots, A_n$};

$F = \bigcup_{n \in \mathbb{N}} F_n$ = {φ | φ *– формула логики высказываний от пропозициональных переменных* $A_1, \dots, A_n, \dots$ };

$[\varphi]_n = \{\psi \mid \psi \in F_n$ и $\varphi \sim \psi\}$;

$[\varphi] = \{\psi \mid \psi \in F$ и $\varphi \sim \psi\}$;

$F_n/_\sim = \{[\varphi]_n \mid \varphi \in F_n\}$ – *фактор-множество;*

$F/_\sim = \{[\varphi] \mid \varphi \in F\}$ – *фактор-множество.*

Замечание 5.4. *Для любых* $n, m \in \mathbb{N}$ *если* $n < m$, *то*

$$F_n \subset F_m \subset F.$$

Доказательство: упражнение.

Определение 5.5. *Пусть* $\varphi, \psi \in F_n$. *Тогда*

a. $[\varphi]_n \,\&\, [\psi]_n = [(\varphi \& \psi)]_n$;

b. $[\varphi]_n \vee [\psi]_n = [(\varphi \vee \psi)]_n$;

c. $[\varphi]_n \to [\psi]_n = [(\varphi \to \psi)]_n$;

d. $\neg[\varphi]_n = [\neg\varphi]_n$.

Пусть $\varphi, \psi \in F$. *Тогда*

a. $[\varphi] \,\&\, [\psi] = [(\varphi \& \psi)]$;

b. $[\varphi] \vee [\psi] = [(\varphi \vee \psi)]$;

c. $[\varphi] \to [\psi] = [(\varphi \to \psi)]$;

d. $\neg[\varphi] = [\neg\varphi]$.

Предложение 5.6. *Определение 5.5 корректно, т. е. не зависит от выбора представителей.*

Другими словами, если $\varphi \sim \varphi_1$ и $\psi \sim \psi_1$, *то выполняются следующие условия:*

a) $[(\varphi \& \psi)]_n = [(\varphi_1 \& \psi_1)]_n$;

b) $[(\varphi \vee \psi)]_n = [(\varphi_1 \vee \psi_1)]_n$;

c) $[(\varphi \to \psi)]_n = [(\varphi_1 \to \psi_1)]_n$;

d) $[\neg\varphi]_n = [\neg\varphi_1]_n$.

Доказательство: упражнение.

Предложение 5.7. *Следующие алгебраические системы являются булевыми алгебрами:*

1) $\langle F_n/_\sim, \&, \vee, \neg, \text{и}, \text{л}\rangle$;

2) $\langle F/_\sim, \&, \vee, \neg, \text{и}, \text{л}\rangle$.

Доказательство: упражнение.

Определение 5.8. *Пусть* $\mathfrak{A}$ *– булева алгебра и* $a, b \epsilon |\mathfrak{A}|$. *Определим отношение* $\leq$:

$$a \leq b \iff a \cap b = a.$$

Предложение 5.9. *Пусть* $\mathfrak{A} = \langle A; \cap, \cup, \bar{\ }, 0, 1\rangle$ *– булева алгебра. Тогда* $\langle A, \leq\rangle$ *– частично упорядоченное множество.*

Доказательство

a. Рефлексивность. Так как $a \cap a = a$, то $a \leq a$.

b. Антисимметричность. Если для элементов $a, b \in A$ выполняются условия $a \leq b$ и $b \leq a$, то $a \cap b = a$ и $a \cap b = b$. Следовательно, получим $a = a \cap b = b \cap a = b$.

c. Транзитивность. Если для элементов $a, b \in A$ выполняются условия $a \leq b$ и $b \leq$ c, то $a \cap b = a$ и $\text{c} \cap b = b$. Следовательно, получим

$$a \cap \text{c} = (a \cap b) \cap \text{c} = a \cap (b \cap \text{c}) = a \cap b = a,$$

т. е. $a \leq$ c.

Предложение 5.9 доказано.

Предложение 5.10. *Пусть* $\mathfrak{A} = \langle A; \cap, \cup, \bar{\ }, 0, 1\rangle$ *– булева алгебра. Тогда для любого элемента* $a \in |\mathfrak{A}|$ *имеем* $0 \leq a \leq 1$.

Доказательство. Так как $a \cap 0 = 0$, то $0 \leq a$. С другой стороны, в силу $a \cap 1 = a$ получим $a \leq 1$.

Предложение 5.10 доказано.

Предложение 5.11. *Пусть* $\mathfrak{A} = \langle A; \cap, \cup, \bar{\ }, 0, 1\rangle$ *– булева алгебра. Введем обозначения* $a \cup^* b = a \cap b$, $a \cap^* b = a \cup b$, $0^* = 1$, $1^* = 0$. *Тогда алгебраическая система* $\langle A; \cap^*, \cup^*, -, 0^*, 1^*\rangle$ *так же является булевой алгеброй.*

Доказательство: упражнение.

Предложение 5.12. *Пусть* $\mathfrak{A} = \langle A; \cap, \cup, \bar{\ }, 0, 1\rangle$ *– булева алгебра. Тогда для любых* $a, b \in |\mathfrak{A}|$ *имеет место*

$$a \leq b \iff a \cup b = b.$$

Доказательство. (⇒) Пусть $a \leq b$. Тогда, по Определению 5.8, имеем $a = a \cap b$. Следовательно, $\bar{a} = \bar{a} \cup \bar{b}$. Откуда получим

$$b = b \cup 0 = b \cup (a \cap \bar{a}) = (b \cup a) \cap (b \cup \bar{a}) =$$
$$(b \cup a) \cap \left(b \cup \bar{a} \cup \bar{b}\right) = (b \cup a) \cap \left(\left(b \cup \bar{b}\right) \cup \bar{a}\right) = a \cup b.$$

(⇐) Пусть $b = a \cup b$. Тогда имеем $\bar{b} = \bar{a} \cap \bar{b}$. Следовательно, получим

$$a = a \cap 1 = a \cap \left(b \cup \bar{b}\right) = (a \cap b) \cup \left(a \cap \bar{b}\right) =$$
$$(a \cap b) \cup \left(a \cap \bar{a} \cap \bar{b}\right) = a \cap b.$$

Таким образом, мы получили, что $a \leq b$.

Предложение 5.12 доказано.

Предложение 5.13. *Пусть* $\mathfrak{A} = \langle A; \cap, \cup, \bar{\ }, 0, 1\rangle$ *– булева алгебра. Тогда* $\langle |\mathfrak{A}|, \leq\rangle = \langle A, \leq\rangle$ *– решёточно упорядоченное множество.*

Доказательство. Достаточно доказать, что для любых $a, b \in |\mathfrak{A}|$ выполнено

$$\sup_{|\mathfrak{A}|}\{a, b\} = a \cup b \ \text{ и } \ \inf_{|\mathfrak{A}|}\{a, b\} = a \cap b.$$

1. Так как

$$a \cup (a \cup b) = (a \cup a) \cup b = a \cup b,$$

то $a \leq (a \cup b)$. С другой стороны, из

$$b \cup (a \cup b) = a \cup (b \cup b) = a \cup b$$

следует, что $b \leq (a \cup b)$. А значит, $\{a, b\} \leq (a \cup b)$.

2. Пусть $\{a, b\} \leq c$. Тогда $a \leq c$ и $b \leq c$. Следовательно,

$$a \cap c = a \ \text{ и } b \cap c = c.$$

Тогда

$$a \cup b = (a \cap c) \cup (b \cap c) = (a \cup b) \cap c,$$

т. е. $a \cup b \leq c$. Таким образом, получим

$$a \cup b = \sup_{|\mathfrak{A}|}\{a, b\}.$$

Аналогично доказывается, что

$$a \cap b = \inf_{|\mathfrak{A}|}\{a, b\}.$$

Предложение 5.13 доказано.

5.2. Атомные и безатомные булевы алгебры

Определение 5.14. ***Атомом*** *называется минимальный среди ненулевых элементов булевой алгебры. Т. е.* a *– атом, если* $a \neq 0$ *и для любого* $b \in A$ *из* $0 \leq b \leq a$ *следует (*$b = 0$ *либо* $b = a$*).*

Элемент b *булевой алгебры называется* ***безатомным****, если под ним нет атомов, т. е. если* $c \leq b$*, то* c *– не атом.*

Элемент c булевой алгебры называется ***атомным****, если под ним нет ненулевых безатомных элементов, т. е. если $b \leq c$ и b – безатомный, то $b = 0$.*

Булева алгебра называется ***атомной****, если в ней нет безатомных элементов, кроме нуля. Булева алгебра называется* ***безатомной****, если в ней нет атомов.*

Замечание 5.15. *Элемент 0 является атомным и безатомным одновременно.*

Доказательство: упражнение.

Определение 5.16. *Введем обозначения.*

1. $At(\mathfrak{A})$ *– множество атомов булевой алгебры*.
2. $At(\text{c}) = \{a \in A |\ a$ – атом и $a \leq c\}$.

Замечание 5.17. $At(\mathfrak{A}) = At(1^{\mathfrak{A}})$.

Доказательство: упражнение.

Замечание 5.18.

1. *Булева алгебра $\mathfrak{A}$ является атомной тогда и только тогда, когда $1^{\mathfrak{A}}$ – атомный элемент.*
2. *Булева алгебра $\mathfrak{A}$ является безатомной тогда и только тогда, когда $1^{\mathfrak{A}}$ – безатомный элемент.*

Доказательство: упражнение.

Определение 5.19. *Булева алгебра $\mathfrak{A}$ называется* ***вырожденной****, если* $0 = 1$.

Предложение 5.20. *Для любого множества алгебра всех его подмножеств является атомной. Если X – множество и*

$$B = \langle \rho(X), \cup, \cap, -, \emptyset, X \rangle$$

является булевой алгеброй всех его подмножеств, то

1) $At(B) = \{\{a\} |\ a \in X\}$;

2) B – атомная булева алгебра.

Доказательство. 1) ($\subseteq$) Пусть $A \in At(B)$. Тогда $A \neq \emptyset$. Следовательно, существует элемент $a \in A$. Тогда $\{a\} \neq \emptyset$ и $\{a\} \subseteq A$. Значит, $\{a\} = A$.

($\supseteq$) Рассмотрим $a \in A$. Очевидно, что $\{a\} \neq \emptyset$. Пусть $B \subseteq \{a\}$ и $B \neq \emptyset$. Следовательно, найдётся такой элемент $b \in B$, что $b \in \{a\}$. А значит, $b = a$. Следовательно, $\{a\} \subseteq B$, и тогда $B = \{a\}$. Таким образом, получили, что $\{a\}$ – атом.

2) Рассмотрим множество $A \subseteq X$, $A \neq \emptyset$. Тогда существует элемент $a \in A$. Следовательно, $\{a\} \subseteq A$ и $\{a\}$ – атом. Значит, $B = \langle \rho(X), \cup, \cap, -, \emptyset, X \rangle$ – атомная булевая алгебра.

Предложение 5.20 доказано.

Замечание 5.21. *Пусть $\langle A, \leq \rangle$ – частично упорядоченное множество и $B \subseteq A$. Тогда $\langle \mathrm{B}, \leq \rangle$ – частично упорядоченное множество.*

Доказательство. Пусть $a, b, \mathrm{c} \in B$. Следовательно, $a, b, \mathrm{c} \in A$. Тогда

1) $a \leq a$;

2) $(a \leq b,\ b \leq a) \Rightarrow b = a$;

3) $(a \leq b, b \leq \mathrm{c}) \Rightarrow a \leq \mathrm{c}$.

Замечание 5.21 доказано.

Предложение 5.22. *Любая конечная булева алгебра является атомной.*

Доказательство. Пусть $\mathfrak{A} = \langle A; \cap, \cup, {}^{-}, 0, 1 \rangle$ – булева алгебра и A – конечно. Рассмотрим множество $B = A \backslash \{0\}$. Очевидно, что B – конечно. Так как $\langle \mathrm{B}, \leq \rangle$ – ЧУМ, получим, что для любого $c \in B$, $c \neq 0$ найдётся такой элемент $a \in B$, что $a \leq c$ и a – минимальный в B. Следовательно, a является атомом алгебры $\mathfrak{A}$ и, значит $\mathfrak{A}$ – атомная булева алгебра.

Предложение 5.22 доказано.

Предложение 5.23. *Пусть $\mathfrak{A} = \langle A; \cap, \cup, {}^{-}, 0, 1 \rangle$ – булева алгебра и $a, b \in |\mathfrak{A}|$. Тогда*

$$a \cap b = 0 \iff a \leq \bar{b}.$$

Доказательство. ($\Rightarrow$) Пусть $a \cap b = 0$. Тогда

$$a = a \cap 1 = a \cap (b \cup \bar{b}) = (a \cap b) \cup (a \cap \bar{b}) = a \cap \bar{b}.$$

Следовательно, $a \leq \bar{b}$.

($\Leftarrow$) Упражнение.

Предложение 5.23 доказано.

Предложение 5.24. *Пусть $\mathfrak{A} = \langle A; \cap, \cup, {}^{-}, 0, 1 \rangle$ – булева алгебра, $a, b \in |\mathfrak{A}|$ и a – атом. Тогда*

$$a \leq b \iff a \nleq \bar{b}.$$

Доказательство: упражнение.

Замечание 5.25. *Пусть* $\mathfrak{A} = \langle A; \cap, \cup, \bar{}, 0, 1\rangle$ *– булева алгебра и* $a, b, c \in |\mathfrak{A}|$. *Тогда*

1) $c \leq a \cap b \Leftrightarrow c \leq a$ и $c \leq b$;

2) $c \geq a \cup b \Leftrightarrow c \geq a$ и $c \geq b$.

Доказательство. (1) ($\Rightarrow$) Пусть $c \leq a \cap b$. Так как $a \cap b \leq a$ и $a \cap b \leq b$, то получим $c \leq a$ и $c \leq b$.

($\Leftarrow$) Пусть $c \leq a$ и $c \leq b$. Тогда $c \leq \{a, b\}$. Следовательно, $c \leq \inf_{\mathfrak{A}}\{a, b\} = a \cap b$.

(2) Доказывается аналогично.

Замечание 5.25 доказано.

Замечание 5.26. *Пусть* $\mathfrak{A} = \langle A; \cap, \cup, \bar{}, 0, 1\rangle$ *– булева алгебра и* $a_1, \dots, a_n \in |\mathfrak{A}|$. *Тогда*

1) $a_1 \cup \dots \cup a_n = \sup_{\mathfrak{A}}\{a_1, \dots, a_n\}$;

2) $a_1 \cap \dots \cap a_n = \inf_{\mathfrak{A}}\{a_1, \dots, a_n\}$;

Доказательство. (1) Будем доказывать индукцией по числу элементов n.

Если $n = 1$, то

$$a_1 = \sup_{\mathfrak{A}}\{a_1\}.$$

Если $n = 2$, то

$$a_1 \cup a_2 = \sup_{\mathfrak{A}}\{a_1, a_2\}.$$

Пусть для n верно, докажем для $n + 1$.

$$(a_1 \cup \dots \cup a_n) \cup a_{n+1} = \sup_{\mathfrak{A}}\{a_1, \dots, a_n\} \cup a_{n+1} =$$
$$= \sup_{\mathfrak{A}}\left\{\sup_{\mathfrak{A}}\{a_1, \dots, a_n\}, a_{n+1}\right\} = \sup_{\mathfrak{A}}\{a_1, \dots, a_{n+1}\}.$$

(2) Доказывается аналогично.

Замечание 5.26 доказано.

Предложение 5.27. *Пусть* $\mathfrak{A} = \langle A; \cap, \cup, \bar{}, 0, 1\rangle$ *– конечная булева алгебра,* $a \in \mathfrak{A}$ *и* $At(a) = \{c_1, \dots, c_n\}$. *Тогда* $a = c_1 \cup \dots \cup c_n$, *т. е.*

$$a = \bigcup_{c \in At(a)} c.$$

Т. е. каждый элемент конечной булевой алгебры является объединением атомов, лежащих под ним.

Доказательство. Пусть $a \in |\mathfrak{A}|$. Введем обозначения:

$$C \leftrightharpoons At(a), \qquad b \leftrightharpoons \bigcup_{d \in C} d\,.$$

Покажем, что $a = b$.

1) Покажем, что $a \leq b$. Будем доказывать от противного. Предположим, что $a \nleq b$. Так как $b = \overline{\overline{b}}$, то $a \nleq \overline{\overline{b}}$. Следовательно, $a \cap \overline{b} \neq 0$. А это значит, что найдётся такой элемент $d \in At(\mathfrak{A})$, что $d \leq a \cap \overline{b}$. Тогда $d \leq a$. Следовательно, $d \in C$. Значит, $d \leq b$ и $d \leq \overline{b}$, поэтому $d \leq b \cap \overline{b} = 0$. Таким образом, мы получили, что $d = 0$, и тем самым пришли к противоречию.

2) Покажем, что $b \leq a$. Так как для любого $d \in C$ мы имеем $d \leq a$ и $b = \sup C$, то $b \leq a$.

Таким образом, мы получили, что $a = b$.

Предложение 5.27 доказано.

Определение 5.28 (изоморфизм булевых алгебр). *Рассмотрим булевы алгебры* $\mathfrak{A}$ *и* $\mathfrak{B}$. *Отображение* $h\colon |\mathfrak{A}| \to |\mathfrak{B}|$ *называется изоморфизмом* $h\colon \mathfrak{A} \to \mathfrak{B}$ *булевых алгебр* $\mathfrak{A}$ *и* $\mathfrak{B}$, *если*

1) отображение $h\colon |\mathfrak{A}| \to |\mathfrak{B}|$ *является взаимно-однозначным;*

2) отображение h *сохраняет операции и константы, т. е.*

a. $h\,(a_1 \cup a_2) = h(a_1) \cup h(a_2)$,
$h(a_1 \cap a_2) = h(a_1) \cap h(a_2)$,
$h(\overline{a}) = \overline{h(a)}$;

b. $h(0) = 0$ и $h(1) = 1$.

Булевы алгебры $\mathfrak{A}$ *и* $\mathfrak{B}$ *называются* ***изоморфными***, *если существует изоморфизм* $h\colon \mathfrak{A} \to \mathfrak{B}$ *булевых алгебр* $\mathfrak{A}$ *и* $\mathfrak{B}$. *Обозначается* $\mathfrak{A} \cong \mathfrak{B}$.

5.3. Теорема Стоуна для конечных булевых алгебр

Теорема 5.29 (Теорема Стоуна для конечных булевых алгебр). *Любая конечная булева алгебра изоморфна булевой алгебре всех подмножеств некоторого множества. Пусть* $\mathfrak{A} = \langle A; \cap, \cup, ^{-}, 0, 1\rangle$ *– конечная булева алгебра. Тогда*

$$\mathfrak{A} \cong \langle \rho\big(At(\mathfrak{A})\big), \cup, \cap, ^{-}, \emptyset, At(\mathfrak{A})\rangle.$$

Доказательство. Определим отображение

$$h\colon |\mathfrak{A}| \to \rho(At(\mathfrak{A}))$$

следующим образом: для любого $a \in |\mathfrak{A}|$ имеем $h(a) = At(a)$. Покажем, что h является изоморфизмом булевых алгебр

$$\mathfrak{A} \text{ и } \langle \rho\big(At(\mathfrak{A})\big), \cup, \cap, \bar{}\,, \emptyset, At(\mathfrak{A})\rangle.$$

1. Докажем взаимную однозначность h:

а) *разнозначность.*

Пусть $a, b \in |\mathfrak{A}|$ и $a \neq b$. Допустим, что $a \nleq b$, тогда $(a \cap \bar{b}) \neq 0$. Это значит, что существует атом d алгебры $\mathfrak{A}$, такой что $d \leq a \cap \bar{b}$. Следовательно, $d \leq a$, т. е. $d \in At(\mathfrak{A})$. Получим $d \in h(a)$.

С другой стороны, $d \leq \bar{b}$. Следовательно, $d \nleq b$, т. е. $d \notin h(b)$. Таким образом, получим $h(a) \neq h(b)$. Разнозначность доказана;

б) *отображение «на».*

Пусть $C \subseteq At(\mathfrak{A})$ и $a = \bigcup_{c \in C} c$. Достаточно проверить, что $C = h(a)$.

Возьмём некоторый $b \in C$. Очевидно, что $b \leq a$ и b – атом. Следовательно, $b \in At(a)$, т. е. $b \in h(a)$. Отсюда получаем, что $C \subseteq h(a)$.

Возьмём теперь $b \in h(a)$. Тогда $b \in At(a)$. Следовательно, $b \leq a$. Значит, $b = b \cap a$.

Пусть $C = \{c_1, \dots, c_k\}$ и $a = c_1 \cup \dots \cup c_k$. Тогда

$$b = b \cap a = b \cap (c_1 \cup \dots \cup c_k) = (b \cap c_1) \cup \dots \cup (b \cap c_k) \neq 0$$

(так как b – атом). Следовательно, найдётся такое i, что $b \cap c_i \neq 0$. Кроме того,

$$b \cap c_i \leq b \text{ и } b \cap c_i \leq c_i.$$

В силу того, что b – атом, имеем $b = b \cap c_i$, а так как c_i – атом, имеем $c_i = b \cap c_i$. Следовательно, $b = c_i$, т. е. $b \in C$. А значит, $h(a) \subseteq C$. Таким образом, $C = h(a)$.

2. Докажем сохранение операций и констант:

а) $h(a \cap b) = \{c \mid c \in At(a \cap b)\} = \{c \mid c \in (At(a) \cap At(b))\} =$
$= \{c \mid c \in At(a)\} \cap \{c \mid c \in At(b)\} = h(a) \cap h(b)$;

б) $h(\bar{a}) = \{c \mid c \in At(\bar{a})\} = \{c \mid c \in \overline{At(a)}\} = \overline{h(a)}$;

в) $h(a \cup b) = h\big(\overline{\bar{a} \cap \bar{b}}\big) = \overline{h\big(\bar{a} \cap \bar{b}\big)} =$
$= \overline{h(\bar{a}) \cap h(\bar{b})} = \overline{\overline{h(a)} \cap \overline{h(b)}} = h(a) \cup h(b)$.

г) $h(0) = h(a \cap \bar{a}) = h(a) \cap \overline{h(a)} = \emptyset$;

д) $h(1) = h(a \cup \bar{a}) = h(a) \cup \overline{h(a)} = At(\mathfrak{A})$.

Теорема 5.29 доказана.

Теорема 5.30 (Стоуна). *Любая булева алгебра изоморфна подалгебре алгебры всех подмножеств некоторого множества. Пусть* $\mathfrak{A}$ *– булева алгебра. Тогда найдётся такое множество* X*, что*

$$\mathfrak{A} \cong \mathfrak{B} \leq \langle \rho(X), \cup, \cap, {}^{-}, \emptyset, X \rangle.$$

Без доказательства.

Замечание 5.31. Если $\mathfrak{A}$ – счётная булева алгебра или безатомная булева алгебра, то для любого множества X имеем $\mathfrak{A} \ncong \langle p(X), U, \cap, {}^{-}, 0, 1 \rangle$.

Доказательство: упражнение.

6. МОЩНОСТЬ МНОЖЕСТВА

6.1. Равномощные множества. Теорема Кантора – Бернштейна

Определение 6.1. *Отображение $f: A \to B$ называется* ***взаимно-однозначным****, если*

1) f – разнозначно, т. е. $\forall\, a, b \in A$ если $a \neq b$, то $f(a) \neq f(b)$ (инъективность);

2) f – отображение «на», т. е. для любого $b \in B$ найдётся $a \in A$ такой, что $f(a) = b$ (сюръективность).

Определение 6.2. *Множества A и B называются* ***равномощными*** *(обозначается $\|A\| = \|B\|$), если существует взаимно-однозначное отображение A на B.*

Множество A ***имеет мощность меньшую, чем мощность*** *множества B (обозначается $\|A\| \leq \|B\|$), если существует множество $C \subseteq B$ такое, что $\|A\| = \|C\|$.*

Предложение 6.3. *Пусть $f: A \to B$ и $g: B \to C$. Тогда*

a. если f и g разнозначны, то $f \circ g$ – разнозначно;

b. если f и g – отображение «на», то $f \circ g$ – отображение «на»;

c. *если f и g взаимно-однозначны, то $f \circ g$ – взаимно-однозначно.*

Доказательство

a. Пусть f и g разнозначны. Тогда для любых $a, b \in A$ если $a \neq b$, то $f(a) \neq f(b)$. Поэтому

$$f \circ g\,(a) = g\big(f(a)\big) \neq g\big(f(b)\big) = f \circ g\,(b),$$

т. е. $f \circ g\,(a) \neq f \circ g\,(b)$.

b. Так как g является отображением «на», то для любого элемента $d \in C$ существует такой элемент $b \in B$, что $g(b) = d$. Так как f является отображением «на», то для элемента $b \in B$ существует такой элемент $a \in A$, что $f(a) = b$. Таким образом, получим $f \circ g(a) = g(f(a)) = d$.

c. Так как f и g – взаимно-однозначные отображения, то f и g являются и отображениями «на», и разнозначными отображениями. Следовательно, отображение $f \circ g$ также является и отображением «на», и разнозначным отображением. Поэтому отображение $f \circ g$ взаимно-однозначно.

Предложение 6.3 доказано.

Предложение 6.4. *Отношение равномощности множеств – отношение эквивалентности.*

Доказательство. Докажем, что отношение равномощности рефлексивно, симметрично и транзитивно.

a. $\|A\| = \|A\|$, так как отображение $id_A: A \to A$ – взаимно-однозначно.

b. Пусть $\|A\| = \|B\|$. Тогда существует взаимно-однозначное отображение $f: A \to B$. Следовательно, отображение $f^{-1}: B \to A$ также взаимно-однозначно. И, значит, $\|B\| = \|A\|$.

c. Пусть $\|A\| = \|B\|$ и $\|B\| = \|C\|$. Тогда существуют взаимно-однозначные отображения $f: A \to B$ и $g: B \to C$. Следовательно, отображение $f \circ g: A \to \mathrm{C}$ также взаимно-однозначно. И, значит, $\|A\| = \|C\|$.

Предложение 6.4 доказано.

Замечание 6.5. *Рассмотрим отображение* $f: A \to B$.

1. f – взаимно-однозначно тогда и только тогда, когда f – обратимо.

2. f – взаимно-однозначно тогда и только тогда, когда f^{-1} – взаимно-однозначно

Доказательство: упражнение.

Предложение 6.6. $\|A\| \leq \|B\|$ *тогда и только тогда, когда существует разнозначное отображение* $f: A \to B$.

Доказательство. (⇒) Пусть $\|A\| \leq \|B\|$. Тогда найдётся такое множество C⊆B, что $\|A\| = \|C\|$. Следовательно, существует взаимно-однозначное отображение $f: A \to C$. А значит, отображение f: A→B будет разнозначным.

(⇐) Пусть отображение $f: A \to B$ разнозначно. Определим множество $C \leftrightharpoons f(A) = \{f(a) | a \in A\}$. Очевидно, что отображение $f: A \to C$ является отображением «на» и разнозначным одновременно. Следовательно, оно взаимно-однозначно. А это означает, что $\|A\| = \|C\|$.

Предложение 6.6 доказано.

Предложение 6.7. *Отношение* $\leq$ *является отношением предпорядка.*

Доказательство. 1. Рефлексивность. $\|A\| \leq \|A\|$, так как отображение $id_A: A \to A$ – взаимно-однозначно.

2. Транзитивность. Пусть $\|A\| \leq \|B\|$ и $\|B\| \leq \|C\|$. Тогда существуют разнозначные отображения $f: A \to B$ и $g: B \to C$. Следовательно, по Предложению 6.3, отображение $f \circ g: A \to C$ также является разнозначным. Следовательно, $\|A\| \leq \|C\|$.

Предложение 6.7 доказано.

Теорема 6.8 (Кантора – Бернштейна). Если $\|A\| \leq \|B\|$ и $\|B\| \leq \|A\|$, то $\|A\| = \|B\|$.

Доказательство. Так как $\|A\| \leq \|B\|$ и $\|B\| \leq \|A\|$, то существуют разнозначные отображения $f: A \to B$ и $g: B \to A$.

Пусть

$$A_0 = A, A_1 = g(B), A_2 = f \circ g\,(A_0), \ldots, A_{i+2} = f \circ g\,(A_i).$$

Тогда отображения $g: B \to A_1$ и $f \circ g: A_i \to A_{i+2}$ являются взаимно-однозначными. Поэтому $\|A_1\| = \|B\|$. Следовательно, достаточно показать, что $\|A\| = \|A_1\|$.

Обозначим через $M_i = A_i \setminus A_{i+1}$. Пусть

$$a \in M_i \Rightarrow a \in A_i \setminus A_{i+1} \Rightarrow a \in A_i \text{ и } a \notin A_{i+1}.$$

Так как отображения

$$f \circ g: A_i \to A_{i+2} \text{ и } f \circ g: A_{i+1} \to A_{i+3}$$

взаимно-однозначны, выполнено

$$f \circ g(a) \in A_{i+2} \quad \text{и} \quad f \circ g(a) \notin A_{i+3}.$$

Следовательно,

$$f \circ g(a) \in A_{i+2} \setminus A_{i+3}.$$

А значит,

$$f \circ g(a) \in M_{i+2}.$$

Таким образом, мы получили, что $f \circ g(M_i) \subseteq M_{i+2}$.

Докажем, что $f \circ g: M_i \to M_{i+2}$ – взаимно-однозначно. Это отображение разнозначно как композиция разнозначных, поэтому достаточно показать, что оно является отображением «на». Пусть

$$b \in M_{i+2}, \text{ т. е. } b \in A_{i+2} \setminus A_{i+3}.$$

Тогда

$$b \in A_{i+2} \text{ и } b \notin A_{i+3}.$$

Следовательно, существует элемент $a \in A_i$ такой, что $f \circ g(a) = b$. Тогда $a \notin A_{i+1}$. А значит, $a \in A_i \setminus A_{i+1}$, т. е. $a \in M_i$. Таким образом, получили, что

$$M_{i+2} \subseteq f \circ g(M_i).$$

Следовательно, $M_{i+2} = f \circ g(M_i)$. Откуда следует, что отображение $f \circ g\colon M_i \to M_{i+2}$ взаимно-однозначно.

Обозначим

$$M = \bigcap_{\mathrm{n} \in \mathbb{N}} A_{\mathrm{n}}.$$

Рассмотрим отображение $h\colon A \to A_1$.

$$h(a) = \begin{cases} a & a \in \left(\bigcup_{\mathrm{n} \in \mathbb{N}} M_{2\mathrm{n}+1}\right) \cup M; \\ f \circ g(a), & a \in \bigcup_{\mathrm{n} \in \mathbb{N}} M_{2\mathrm{n}}. \end{cases}$$

Докажем, что отображение h взаимно-однозначно.

1) Покажем, что отображение h разнозначно. Пусть $a_1, a_2 \in A$ и $a_1 \neq a_2$. Рассмотрим 3 случая.

a. Пусть

$$a_1, a_2 \in \left(\bigcup_{\mathrm{n} \in \mathbb{N}} M_{2\mathrm{n}+1}\right) \cup M.$$

Тогда

$$h(a_1) = a_1 \text{ и } h(a_2) = a_2.$$

Очевидно, что тогда

$$h(a_1) \neq h(a_2).$$

b. Пусть

$$a_1 \in \left(\bigcup_{n \in N} M_{2n+1}\right) \cup M \quad \text{и} \quad a_2 \in \bigcup_{n \in N} M_{2n} .$$

Тогда

$$h(a_1) = a_1 \in \left(\bigcup_{\mathrm{n} \in \mathbb{N}} M_{2\mathrm{n}+1}\right) \cup M$$

и

$$h(a_2) = f \circ g\,(a_2) \in \bigcup_{\mathrm{n} \in \mathbb{N}} \mathrm{M}_{2\mathrm{n}+2}.$$

Очевидно, что тогда

$$h(a_1) \neq h(a_2).$$

c. Пусть

$$a_1, a_2 \in \bigcup_{\mathrm{n} \in \mathbb{N}} \mathrm{M}_{2\mathrm{n}}.$$

Тогда

$$f \circ g\ (a_1) \neq f \circ g\ (a_2),$$

поскольку $a_1 \neq a_2$, а отображение $f \circ g$ разнозначно. Значит, $h(a_1) \neq h(a_2)$. Следовательно, отображение h разнозначно.

2) Покажем, что h – отображение «на». Очевидно, что

$$A_1 = \bigcup_{\mathrm{n} \in \mathbb{N}} (M_{2\mathrm{n}+1} \cup M_{2\mathrm{n}+2}) \cup M.$$

Если $b \in A_1$, то

$$b \in \left(\bigcup_{n \in N} M_{2n+1} \right) \cup M \text{ или } b \in \bigcup_{n \in N} M_{2n+2}.$$

Рассмотрим два случая.

a. Пусть

$$b \in \left(\bigcup_{\mathrm{n} \in \mathbb{N}} M_{2\mathrm{n}+1} \right) \cup M.$$

Возьмём $a = b$. Тогда $h(a) = a = b$.

b. Пусть

$$b \in \bigcup_{n \in N} \mathrm{M}_{2\mathrm{n}+2}.$$

Тогда, в силу того, что отображение $f \circ g\colon M_{2\mathrm{n}} \to M_{2\mathrm{n}+2}$ взаимно-однозначно, существует

$$a \in \bigcup_{n \in N} M_{2\mathrm{n}}$$

такое, что $f \circ g(a) = b$. Следовательно, $h(a) = b$. Таким образом, h является отображением «на».

Таким образом, мы доказали, что h – взаимно-однозначное отображение и, следовательно, $\|A\| = \|A_1\| = \|B\|$.

Теорема 6.8 доказана.

6.2. Конечные и бесконечные множества. Теорема Кантора

Будем обозначать $\|A\| < \|B\|$, если $\|A\| \leq \|B\|$ и $\|A\| \neq \|B\|$.

Теорема Кантора 6.9. Мощность любого множества меньше мощности множества всех его подмножеств, т. е.

$$\|A\| < \|\rho(A)\|.$$

Доказательство. Рассмотрим отображение $f: a \mapsto \{a\}$. Отображение f разнозначно, так как если $a_1 \neq a_2$, то $\{a_1\} \neq \{a_2\}$. Значит, $\|A\| \leq \|\rho(A)\|$.

Предположим, что $\|A\| = \|\rho(A)\|$. Следовательно, существует $h: A \to \rho(A)$ – взаимно-однозначное отображение. Элемент a будем называть «хорошим» тогда и только тогда, когда $a \notin h(a)$.

Пусть

$$H = \{a \mid a - \text{"хороший"}\} = \{a \mid a \notin h(a)\}.$$

Очевидно $H \subseteq A$. Следовательно, $H \in \rho(A)$. Значит, существует b такой, что $h(b) = H$.

Пусть b – «хороший». Тогда

$$b \in H \text{ и } b \notin h(b) = H.$$

Приходим к противоречию.

Пусть b – «плохой», тогда $b \in h(b)$. Следовательно, $b \in H$, т. е. b – «хороший» и $b \notin h(b)$. Мы снова пришли к противоречию.

Таким образом, мы доказали, что взаимно-однозначного отображения $h: A \to \rho(A)$ не существует. Значит,

$$\|A\| \neq \|\rho(A)\| \text{ и } \|A\| < \|\rho(A)\|.$$

Следствие 6.10 (О бесконечности количества бесконечных мощностей). Количество бесконечных мощностей бесконечно, т. е.

$$\|A\| < \|\rho(A)\| < \|\rho(\rho(A))\| < \cdots.$$

Доказательство: упражнение.

6.3. Парадоксы теории множеств

Парадокс Кантора 6.11. Рассмотрим множество

$$A = \{ a \mid a - \text{множество} \}.$$

Если $X \in \rho(A)$, то $X \subseteq A$, следовательно X – множество, поэтому $X \in A$. Значит, $\rho(A) \subseteq A$. Следовательно,

$$\|\rho(A)\| \leq \|A\|.$$

Но по теореме Кантора имеем $\|A\| < \|\rho(A)\|$ – противоречие.

Парадокс Рассела 6.12. Рассмотрим множество $A = \{a \mid a \notin a\}$. Тогда

1) если $A \in A$, то $A \notin A$;
2) если $A \notin A$, то $A \in A$.

В обоих случаях получаем противоречие.

7. СЧЁТНЫЕ И КОНТИНУАЛЬНЫЕ МНОЖЕСТВА

7.1. Счётные множества

Определение 7.1. *Множество A называется* ***бесконечным****, если существует* $B \subseteq A$ *такое, что* $B \neq A$ *и* $\|B\| = \|A\|$.

Множество A называется ***счётным****, если оно равномощно множеству натуральных чисел:* $\|A\| = \|\mathbb{N}\|$. *Обозначается* $\|A\| = \omega$.

Предложение 7.2. *Следующие множества являются счётными:*

1) множество чётных натуральных чисел $2\mathbb{N}$*;*

2) множество целых чисел $\mathbb{Z}$.

Доказательство

1. Пусть $2\mathbb{N} = \{\, 2n \mid n \in \mathbb{N}\}$. Тогда функция $f(n) = 2n$ устанавливает взаимно-однозначное соответствие между множествами $\mathbb{N}$ и $2\mathbb{N}$.

2. Функция $f(n) = \begin{cases} k, & n = 2k + 1; \\ -k, & n = 2k. \end{cases}$ устанавливает взаимно-однозначное соответствие между множествами $\mathbb{N}$ и $\mathbb{Z}$.

Предложение 7.2 доказано.

Предложение 7.3.

1. $\|\mathbb{N}^2\| = \omega$.

2. Если $\|A\| = \omega$, *то* $\|A^2\| = \omega$.

3. Если $\|A\| = \omega$ *и* $\|B\| = \omega$, *то* $\|A \times B\| = \omega$.

Доказательство: упражнение.

Предложение 7.4.

1. Для любого $k \in \mathbb{N}$ *имеет место* $\|\mathbb{N}^k\| = \omega$.

2. Если $\|A\| = \omega$, *то для любого* $k \in \mathbb{N}$ *имеет место* $\|A^k\| = \omega$.

3. Для любого $k \in \mathbb{N}$ *если* $\|A_1\| = \dots = \|A_k\| = \omega$, *то*

$$\|A_1 \times \ldots \times A_k\| = \omega.$$

Доказательство: упражнение; по индукции из предыдущего предложения.

Обозначим

$$A^* = \bigcup_{k \in \mathbb{N}} A^k.$$

Предложение 7.5.

1. $\|\mathbb{N}^*\| = \omega$.

2. Если $\|A\| = \omega$, *то* $\|A^*\| = \omega$ *(множество всех конечных слов счётного алфавита счётно).*

Доказательство: упражнение.

Следствие 7.6.

1. Для любого языка программирования множество всех программ счётно.

2. Множество всех функций, вычислимых на машине Тьюринга, счётно.

3. Множество всех частично рекурсивных функций счётно.

4. Множество многочленов с целыми коэффициентами счётно.

5. Множество всех алгебраических чисел счётно.

Доказательство: упражнение.

Предложение 7.7. *Пусть множество A – счётно. Тогда множество*

$$\rho^f(A) = \{B \mid B \subseteq A;\ B - \textit{конечное}\}$$

тоже будет счётным (т. е. множество всех конечных подмножеств счётного множества счётно).

Доказательство. 1) Определим отображение $h: A \to \rho^f(A)$ следующим образом: $h(a) = \{a\}$. Ранее было показано, что h – разнозначно. Следовательно, $\|A\| \leq \|\rho^f(A)\|$.

2) Покажем сначала, что множество $\rho^f(\mathbb{N})$ счётно. Используя (1), достаточно показать, что $\|\rho^f(\mathbb{N})\| \leq \|\mathbb{N}\|$. Для этого, в силу Предложения 7.5, достаточно доказать, что $\|\rho^f(N)\| \leq \|\mathbb{N}^*\|$.

Определим отображение $g: \rho^f(\mathbb{N}) \to \mathbb{N}^*$. Рассмотрим конечное множество $C \subseteq \mathbb{N}$, тогда C можно представить как $C = \{m_1 < \cdots < m_k\}$. Положим $g(C) = < m_1, \dots, m_k >$. Легко проверить, что отображение $g: \rho^f(A) \to \mathbb{N}^*$ разнозначно. Следовательно, $\|\rho^f(\mathbb{N})\| \leq \|\mathbb{N}^*\|$. Поэтому $\|\rho^f(\mathbb{N})\| = \|\mathbb{N}^*\|$ и $\|\rho^f(\mathbb{N})\| = \|\mathbb{N}\|$.

Так как $\|A\| = \omega$, существует взаимно-однозначное отображение $f: A \to \mathbb{N}$. Построим отображение $f^\#: \rho^f(A) \to \rho^f(\mathbb{N})$ следующим образом: для произвольного конечного множества $C \subseteq A$ положим $f^\#(C) = \{f(a) \mid a \in C\}$. Несложно проверить, что отображение $f^\#: \rho^f(A) \to \rho^f(\mathbb{N})$ взаимно-однозначно. Поэтому

$$\|\rho^f(A)\| = \|\rho^f(\mathbb{N})\|$$

и, следовательно,

$$\|\rho^f(A)\| = \|\mathbb{N}\|.$$

Предложение 7.7 доказано.

Замечание 7.8. *Если A и B – конечные множества, то $A \cup \mathrm{B}$ и $A \cap \mathrm{B}$ конечны.*

Доказательство: упражнение.

Предложение 7.9. *Пусть A − бесконечное множество. Тогда существует множество $B \subseteq A$ такое, что $\|B\| = \omega$ (т. е. у любого бесконечного множества есть счётное подмножество).*

Доказательство. Пусть множество A бесконечно. Следовательно, найдётся $a_1 \in A$. Множество $A \setminus \{a_1\}$ бесконечно, следовательно найдётся $a_2 \in A \setminus \{a_1\}$. Множество $A \setminus \{a_1, a_2\}$ бесконечно и т. д.

Таким образом, мы построим счётное подмножество

$$B = \{ a_n \mid n \in \mathbb{N}\}$$

множества A.

Предложение 7.9 доказано.

Предложение 7.10. Если A – бесконечно, $a \in A$, то

$$\|A\| = \|A \setminus \{a\}\|.$$

Доказательство. $A \setminus \{a\}$ – бесконечно. Следовательно, существует множество $B \subseteq A \setminus \{a\}$ такое, что $\|B\| = \omega$. Значит, можно построить взаимно-однозначное соответствие между множествами $\mathbb{N}$ и B. Пусть $f\colon \mathbb{N} \to B$ – взаимно-однозначное отображение. Определим отображение $g\colon A \to A \setminus \{a\}$ следующим образом:

$$g(c) = \begin{cases} c, & c \notin B \cup \{a\}; \\ f(0), & c = a; \\ f(n+1), & c \in B \text{ и } c = f(n). \end{cases}$$

Нетрудно показать, что отображение $g\colon A \to A \setminus \{a\}$ является взаимно-однозначным.

Предложение 7.10 доказано.

Следствие 7.11. Множество A – бесконечно тогда и только тогда, когда $A \neq \emptyset$ и для любого $a \in A$ имеем

$$\|A\| = \|A \setminus \{a\}\|.$$

Доказательство: упражнение.

Следствие 7.12.

1. Если множество A бесконечно, $B \subseteq A$ и множество B конечно, то $\|A\| = \|A \backslash B\|$.
2. Если множество A бесконечно, а B конечно, то $\|A\| = \|A \cup B\|$.

Доказательство: упражнение.

7.2. Континуальные множества

Определение 7.13. *Множество A называется* ***континуальным*** (***имеющим мощность континуум***)*, если оно равномощно множеству действительных чисел, т. е.* $\|A\| = \|R\|$. *Обозначается*: $\|A\| = c$.

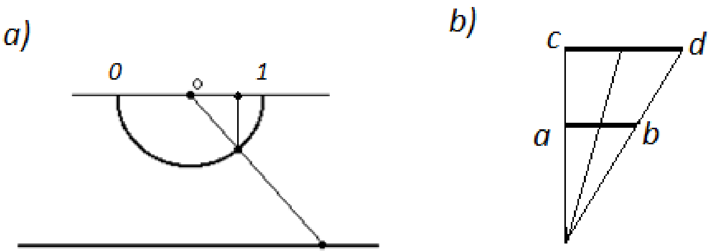

Рис. 3. Взаимно-однозначные соответствия

Предложение 7.14.

1. Для любых $a, b \in \mathbb{R}$, *таких что* $a < b$, *имеет место*

$$\|(a,b)\| = \|[a,b]\| = \|[a,b)\| = \|(a,b]\|.$$

2. $\|(0,1)\| = \|R\|$.

3. Для любых $a, b, c, d \in \mathbb{R}$, *таких что* $a < b$ и $c < d$, *имеет место*

$$\|(a,b)\| = \|(c,d)\|.$$

Доказательство. (1) Доказательство вытекает непосредственно из Следствия 7.12.

(2) Взаимно-однозначное соответствие между множествами $(0,1)$ и $\mathbb{R}$ представлено рис. 3(a).

(3) Допустим (без ограничения общности), что $b - a < d - c$. Тогда взаимно-однозначное соответствие между интервалами (a, b) и (c, d) представлено рис. 3(b).

Предложение 7.14 доказано.

Теорема 7.15 (о несчётности континуума). $\|\mathbb{N}\| < \|\mathbb{R}\|$.

Доказательство. Так как $\mathbb{N} \subset \mathbb{R}$, очевидно, что $\|\mathbb{N}\| \leq \|\mathbb{R}\|$. Поэтому нам необходимо показать, что $\|\mathbb{N}\| \neq \|\mathbb{R}\|$.

В Предложении 17.14 было доказано, что $\|(0,1)\| = \|\mathbb{R}\|$. Покажем, что $\|(0,1)\| \neq \|\mathbb{N}\|$. Будем доказывать от противного. Допустим, что $\|(0,1)\| = \omega$. Следовательно, существует взаимно-однозначное отображение множества $\mathbb{N}$ на интервал $(0,1) = \{ a_n \mid n \in \mathbb{N}\}$.

Пусть в десятичной записи

$$a_i = 0, \alpha_{i1}\, \alpha_{i2}\, \alpha_{i3} \ldots,$$

где $\alpha_{ij} \in \{0, 1, 2, 3, \ldots, 9\}$.

Таким образом, мы пронумеровали все числа на интервале (0, 1):

$$a_1 = 0, \alpha_{11}\, \alpha_{12}\, \alpha_{13} \ldots$$
$$a_2 = 0, \alpha_{21}\, \alpha_{22}\, \alpha_{23} \ldots$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$a_n = 0, \alpha_{n1}\, \alpha_{n2}\, \alpha_{n3} \ldots$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$

Пусть $b = 0, \beta_1\ \beta_2\ \beta_3\ \ldots$, где

$$\beta_i = \begin{cases} 1; & \alpha_{ii} \neq 1; \\ 2; & \alpha_{ii} = 1. \end{cases}$$

Очевидно, что тогда $b \in (0, 1)$. Значит, существует такой номер k, что $a_k = \beta$. Но, по построению, мы имеем $\beta_k \neq \alpha_{kk}$. Следовательно, $b \neq a_k$ – противоречие.

Таким образом, мы доказали, что нельзя построить взаимно-однозначное соответствие между множествами $\mathbb{R}$ и $\mathbb{N}$.

Стало быть,

$$\|\mathbb{N}\| \neq \|\mathbb{R}\| \text{ и } \|\mathbb{N}\| < \|\mathbb{R}\|.$$

Теорема 7.15 доказана.

Континуум-гипотеза. *Для любого бесконечного множества $A \subseteq \mathbb{R}$ имеет место $\|A\| = \|\mathbb{N}\|$ или $\|A\| = \|\mathbb{R}\|$.*

Определение 7.16. *Число $q \in \mathbb{R}$ называется* ***алгебраическим****, если существует многочлен с рациональными коэффициентами*

$$P(x) = a_n x^n + \dots + a_0 \quad (a_i \in \mathbb{Q})$$

такой, что $P(q) = 0$.

Число $q \in \mathbb{R}$ называется ***трансцендентным****, если оно не является алгебраическим.*

Следствие 7.17. Множество трансцендентных чисел континуально.

Доказательство: упражнение.

Теорема 7.18. *Если $\|A\| < \|C\|$, $\|B\| < \|C\|$ и множество C бесконечно, то $\|A \cup B\| < \|C\|$.*

Без доказательства.

Предложение 7.19.

1. $\|\mathbb{R}^2\| = \|(0,1)^2\|$.
2. $\|\mathbb{R}^n\| = \|(0,1)^n\|$.

Доказательство

1. По Предложению 17.17 существует взаимно-однозначное отображение $f\colon (0,1) \to \mathbb{R}$. Тогда отображение $f \times f\colon (0,1)^2 \to \mathbb{R}^2$, определённое следующим образом:

$$f \times f\colon (a,b) = \langle f(a),\ f(b)\rangle \text{ для любых } a,b \in (0,1),$$

также будет взаимно-однозначным.

2. Определим отображение

$$\underbrace{f \times \dots \times f}_{n \text{ раз}}\colon\ (0,1)^n \to R^n$$

следующим образом:

$f \times \dots \times f(a_1, \dots, a_n) = \langle f(a_1), \dots, f(a_n)\rangle$ для любых $a_1, \dots, a_n \in (0,1)$.

Легко показать, что отображение $f \times \dots \times f$ – взаимно-однозначно.

Предложение 7.19 доказано.

Теорема 7.20. $\|\mathbb{R}\| = \|\mathbb{R}^2\|$.

Доказательство. Покажем, что $\|(0,1)\| = \|(0,1)^2\|$.

Отображение $g\colon (0,1) \to (0,1)^2$ такое, что $g(a) = \left(a, \frac{1}{2}\right)$, является разнозначным. Следовательно, $\|(0,1)\| \le \|(0,1)^2\|$.

Покажем, что $\|(0,1)^2\| \le \|(0,1)\|$.

Определим отображение $h\colon (0,1)^2 \to (0,1)$ следующим образом. Пусть $a = 0,a_1a_2a_3a_4\ldots$ и $b = 0,b_1b_2b_3b_4\ldots$. Тогда положим $h(a,b) = 0,a_1b_1a_2b_2a_3b_3a_4\ldots$.

Очевидно, что отображение h разнозначно. Следовательно,

$\|(0,1)^2\| \le \|(0,1)\|$. Таким образом, получаем, что $\|(0,1)\| = \|(0,1)^2\|$. Следовательно, $\|\mathbb{R}\| = \|\mathbb{R}^2\|$.

Теорема 7.20 доказана.

Теорема 7.21. $\|\mathbb{R}\| = \|\rho(\mathbb{N})\|$.

Доказательство. 1) Покажем, что $\|\rho(\mathbb{N})\| \le \|\mathbb{R}\|$. Будем строить отображение $f\colon \rho(\mathbb{N}) \to (0,1)$ следующим образом: множеству $A \subseteq \mathbb{N}$ поставим в соответствие действительное число $f(A) = 0,1\ b_0\ b_1\ b_2\ b_3\ldots$, где

$$b_n = \begin{cases} 1; & \mathrm{n} \in \mathrm{A}; \\ 0; & \mathrm{n} \notin \mathrm{A}. \end{cases}$$

Очевидно, что f – разнозначное отображение. Следовательно,

$$\|\rho(\mathbb{N})\| \le \|(0,1)\|.$$

И, по Предложению 17.17, получаем $\|\rho(\mathbb{N})\| \le \|\mathbb{R}\|$.

2) Покажем, что $\|\mathbb{R}\| \le \|\rho(\mathbb{N})\|$о. Для этого достаточно показать, что $\|(0,1)\| \le \|\rho(\mathbb{N})\|$.

Построим отображение $g\colon (0,1) \to \rho(\mathbb{N})$ следующим образом. Рассмотрим число $a \in (0,1)$. Его можно представить в виде бесконечной двоичной дроби

$$a = 0,\alpha_1\ \alpha_2\ \alpha_3\ \ldots, \text{ где } \alpha_i \in \{0,1\}.$$

Положим

$$g(a) \leftrightharpoons \{n \mid \alpha_n = 1\} \subseteq \mathbb{N}.$$

Очевидно, что отображение $g\colon (0,1) \to \rho(\mathbb{N})$ разнозначно. Следовательно, $\|(0,1)\| \le \|\rho(\mathbb{N})\|$.

Теорема 7.21 доказана.

Теорема 7.21 позволяет нам переформулировать континуум-гипотезу.

Континуум-гипотеза (другая формулировка). Если для множества A имеет место $\|\mathbb{N}\| < \|A\| \le \|\rho(\mathbb{N})\|$, то $\|A\| = \|\rho(\mathbb{N})\|$.

Исходя из этой формулировки, мы можем обобщить континуум-гипотезу на случай произвольного множества (а не только множества $\mathbb{N}$).

Обобщенная континуум-гипотеза. Если для множеств A и B имеет место $\|B\| < \|A\| \leq \|\rho(B)\|$, тогда $\|A\| = \|\rho(B)\|$.

7.3. Ординалы и кардиналы

Определение 7.22. ***Ординальными числами*** (***ординалами***) *называются*:

$$\alpha_0 = 0 = \emptyset;$$
$$\alpha_1 = 1 = \{\emptyset\};$$
$$\alpha_2 = 2 = \{\emptyset;\ \{\emptyset\}\};$$
$$\alpha_3 = 3 = \{\emptyset;\ \{\emptyset\}; \{\emptyset;\ \{\emptyset\}\}\};$$
$$\dots$$
$$\alpha_{n+1} = \alpha_n \cup \{\alpha_n\};$$
$$\omega = \{\alpha_0, \alpha_1, \dots, \alpha_n \dots\};$$
$$\omega + 1 = \omega \cup \{\omega\} = \{\alpha_0, \alpha_1, \dots, \alpha_n \dots, \omega\};$$
$$2\omega = \{\alpha_0, \alpha_1, \dots, \alpha_n, \dots, \omega, \omega + 1, \dots, \omega + n, \dots\};$$
$$\dots$$
$$\alpha = \{\beta \mid \beta < \alpha\}.$$

Определение 7.23. α *называется* ***непредельным*** *ординалом, если существует ординал* β *такой, что* $\alpha = \beta + 1$.

α *называется* ***предельным*** *ординалом, если не существует ординала* β *такого, что* $\alpha = \beta + 1$.

Замечание 7.24. $\alpha < \beta \iff \alpha \in \beta$.

Доказательство: упражнение.

Замечание 7.25.

1. $\|\omega\| = \|\omega + 1\|$.
2. $\|\omega\| = \|\omega + n\|$.
3. $\|\omega\| = \|2\omega\|$.

Доказательство: упражнение.

Определение 7.26. *Ординал α называется* ***кардиналом****, если для любого ординала $\beta < \alpha$ имеет место $\| \beta \| \neq \| \alpha \|$.*

Замечание 7.27.
1. $\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots, \omega$ – кардиналы.
2. $\omega + 1, \omega + 2, \ldots, 2\omega, \ldots$ – не кардиналы.

Доказательство: упражнение.

Предложение 7.28. Любой бесконечный кардинал является предельным ординалом.

Доказательство. Пусть α – бесконечный кардинал и $\alpha = \beta + 1$. Следовательно, β – бесконечный ординал. Тогда $\alpha = \beta \cup \{ \beta \}$, значит, $\|\alpha\| = \|\beta\|$. Приходим к противоречию с определением кардинала, так как $\beta < \alpha$.

Предложение 7.28 доказано.

8. МАШИНЫ ТЬЮРИНГА

8.1. Формальное описание машины Тьюринга. Функции, вычислимые на машине Тьюринга

Машина Тьюринга – абстрактная вычислительная машина. В состав машины Тьюринга входит бесконечная в обе стороны *лента*, разделённая на ячейки, и *управляющее устройство*, способное находиться в одном из *множества состояний*. Число возможных состояний управляющего устройства конечно.

Управляющее устройство может перемещаться влево и вправо по ленте, читать и записывать в ячейки ленты символы некоторого конечного алфавита (мы будем рассматривать алфавит $\{0,1\}$).

Состояние q_0 машины Тьюринга является *терминальным*, переход в него означает конец работы машины Тьюринга, остановку выполнения алгоритма. Мы будем считать, что машина Тьюринга начинает работу в состоянии q_1.

Напомним обозначение:

$$\{0,1\}^* \leftrightharpoons \bigcup_{n\in N}\{0,1\}^n = \{(a_1,\dots,a_n) \mid n \in \mathbb{N}, a_i \in \{0,1\}\}.$$

Определение 8.1. *Множество* $\{0,1\}$ *назовем* ***внешним алфавитом***. *Множество* $Q = \{q_0, q_1, \dots, q_m\}$ *назовем* ***внутренним алфавитом***. *Машинным словом будем называть конечную последовательность*

$$S \leftrightharpoons \alpha q_i j \beta, \text{ где } \alpha, \beta \in \{0,1\}^*,\ j \in \{0,1\},\ q_i \in Q.$$

Определение 8.2. ***Командой*** *машины Тьюринга назовем последовательность:* $q_i\, j \to q_s k\, \xi$, где $q_i, q_s \in Q$, $j, k \in \{0,1\}$, $\xi \in \{R, L, \emptyset\}$.

Определение 8.3. *Введем следующие обозначения*:

a) $S_1 \xrightarrow{\Pi} S_2$, если машина Тьюринга с программой П слово S_1 за один такт работы переводит в слово S_2;

b) $S \overset{\Pi}{\Rightarrow} S'$, если $S = S_1 \xrightarrow{\Pi} \dots \xrightarrow{\Pi} S_n = S'$, т. е. машина Тьюринга с программой П за конечное число шагов переводит слово S в слово S';

c) $S \Rrightarrow S'$, если $S \overset{\Pi}{\Rightarrow} S'$ и при этом не достраиваются ячеек слева;

d) $S \mid\Rrightarrow S'$, если $S \overset{\Pi}{\Rrightarrow} S'$ и при этом не достраивает ячеек ни слева, ни справа.

Мы будем рассматривать k-местные частичные функции, определённые на натуральных числах, а именно функции

$$f\colon \mathbb{N}^k \to \mathbb{N} \cup \{\,\text{н}\,\},$$

где $f(n_1, \dots, n_k) = \text{н}$ означает, что на кортеже натуральных чисел $(n_1, \dots, n_k)$ функция f не определена. Для удобства такие частичные функции в дальнейшем мы будем называть просто функциями $f\colon \mathbb{N}^k \to \mathbb{N}$.

Определение 8.4. *Обозначим* $1^n = \underbrace{1 \dots 1}_{n\ \text{раз}}$. *Запись* $01^{n+1}0$ *на ленте машины Тьюринга кодирует число n. Кодом кортежа натуральных чисел* $(n_1, \dots, n_k)$ *является запись* $01^{n_1+1}0 \dots 01^{n_k+1}$ *на ленте машины Тьюринга.*

Функция $f\colon \mathbb{N}^k \to \mathbb{N}$ *называется* ***вычислимой*** *на машине Тьюринга с программой* Π*, если для любых* $n_1, \dots, n_k, m \in \mathbb{N}$ *выполнены следующие условия*:

а) если $f(n_1, \dots, n_k) = m$, то

$$q_1 01^{n_1+1}0 \dots 01^{n_k+1}0 \overset{\Pi}{\Rrightarrow} \alpha q_0 01^{m+1}0\beta;$$

б) если $f(n_1, \dots, n_k)$ не определена, то машина Тьюринга работает бесконечно.

Определение 8.5. *Функция* $f\colon \mathbb{N}^k \to \mathbb{N}$ *называется* ***правильно вычислимой*** *на машине Тьюринга с программой* Π*, если для любых* $n_1, \dots, n_k, m \in \mathbb{N}$ *выполнены следующие условия*:

а) если $f(n_1, \dots, n_k) = m$, то

$$q_1 01^{n_1+1}0 \dots 01^{n_k+1}0 \overset{\Pi}{\Rrightarrow} q_0 01^{m+1}0\beta;$$

б) если $f(n_1, \dots, n_k)$ не определена, то машина Тьюринга работает бесконечно.

8.2. Композиция машин Тьюринга. Условный оператор

Определение 8.6. *Машина Тьюринга с программой* Π *называется* ***композицией*** *машин Тьюринга с программами* Π_1 *и* Π_2 *и обозначается* $\Pi = \Pi_1 \circ \Pi_2$ *, если* $S \overset{\Pi}{\Rightarrow} S'$ *в том случае, когда*

$$S \overset{\Pi_1}{\Rightarrow} \alpha q_0 j\, \beta \ \text{ и } \ \alpha q_1 j\, \beta \overset{\Pi_2}{\Rightarrow} S'.$$

При этом если на соответствующих машинных словах машина с программой Π_1 *или машина с программой* Π_2 *не останавливается, то машина с программой* Π *не останавливается.*

Пусть программы Π_1 и Π_2 имеют множества состояний

$$Q_1 = \{q_0, q_1, \dots, q_n\} \text{ и } Q_2 = \{q_0, q_1, \dots, q_m\}$$

соответственно. Тогда

$$\Pi = \Pi_1 \circ \Pi_2 = [\,\Pi_1]^{q_0}_{q_{n+1}} \cup [\,\Pi_2]^{q_i}_{q_{i+n},\ i \neq 0}.$$

Определение 8.7. *Машина Тьюринга с программой* Π *называется полученной с помощью* ***условного оператора*** *из машин Тьюринга с программами* Π_1, Π_2, Π_3 *и обозначается* $\Pi = \Pi_1\left[\begin{matrix}\Pi_2\\ \Pi_3\end{matrix}\right.$, *если* $\mathrm{S} \overset{\Pi}{\Rightarrow} \mathrm{S}'$, *когда*

$$S \overset{\Pi_1}{\Rightarrow} \alpha q_0 010\beta \text{ и } \alpha q_1 010\,\beta \overset{\Pi_2}{\Rightarrow} S', S \overset{\Pi}{\Rightarrow} S'$$

либо

$$S \overset{\Pi_1}{\Rightarrow} \alpha q_0 \gamma, \gamma \neq 010\beta, \text{ и } \ \alpha q_1 \gamma \overset{\Pi_3}{\Rightarrow} \mathrm{S}'.$$

При этом если на соответствующих машинных словах машина с программой Π_1, *или машина с программой* Π_2, *или машина с программой* Π_3 *не останавливается, то машина с программой* Π *не останавливается.*

Пусть программы Π_1, Π_2 и Π_3 имеют множества состояний

$$Q_1 = \{q_0, q_1, \dots, q_n\},\ Q_2 = \{q_0, q_1, \dots, q_m\} \text{ и } Q_3 = \{q_0, q_1, \dots, q_k\}$$

соответственно. Рассмотрим программу Π_4:

$$\begin{aligned} &q_1 0 \to q_2 0 R\\ &q_1 1 \to q_{n+1} 1\\ &q_2 0 \to q_{n+1} 0 L \end{aligned}$$

$$q_2 1 \to q_3 1R$$
$$q_3 0 \to q_5 0L$$
$$q_3 1 \to q_4 1L$$
$$q_4 1 \to q_{n+1} 1L$$
$$q_5 1 \to q_{n+k+1} 1L$$

Тогда

$$\Pi = [\Pi_1]^{q_0}_{q_{n+m+k+1}} \cup [\Pi_2]^{q_i,\ i\neq 0}_{q_{i+n+k}} \cup [\Pi_3]^{q_i,\ i\neq 0}_{q_{i+n}} \cup [\Pi_4]^{q_i,\ i\leq 5}_{q_{i+n+m+k}}.$$

Определение 8.8. *Машина Тьюринга с программой* Π *называется полученной с помощью **условного оператора с циклом** из машин Тьюринга с программами* Π_1, Π_2, Π_3 *(и обозначается* $\Pi = \Pi_1 \circ [{}^{\Pi_2}_{\Pi_3})$*, если*

$$S \overset{\Pi_1}{\Rightarrow} \ \alpha q_0 010\beta, \alpha q_1 010\,\beta \overset{\Pi_2}{\Rightarrow} S', S \overset{\Pi}{\Rightarrow} S'$$

либо

$$S \overset{\Pi_1}{\Rightarrow} \alpha q_0 \gamma,\ \gamma \neq 010\,\beta,\ \alpha q_1 \gamma \overset{\Pi_3}{\Rightarrow} S',$$

и снова запускается Π_1.

При этом если на соответствующих машинных словах машина с программой Π_1, *или машина с программой* Π_2, *или машина с программой* Π_3 *не останавливается, то машина с программой* Π *не останавливается.*

Построить программу для условного оператора с циклом – упражнение.

8.3. Базовые машины Тьюринга

Определение 8.9. *Базовые Машины Тьюринга:*

А. Перенос нуля: $q_1 001^x 0 \ \models\!\Rightarrow\ q_0 01^x 00$;

Б$^+$. Правый сдвиг: $q_1 01^x 0 \ \models\!\Rightarrow\ 01^x q_0 0$;

Б$^-$. Левый сдвиг: $01^x q_1 0 \ \models\!\Rightarrow\ q_0 01^x 0$;

В. Транспозиция: $01^x q_1 01^y 0 \ \models\!\Rightarrow\ 01^y q_0 01^x 0$;

Г. Удвоение: $q_1 01^x 0^{x+2} \ \models\!\Rightarrow\ q_0 01^x 01^x 0$;

Ц$_n$. Циклический сдвиг:

$$q_1 01^{x_1} 01^{x_2} 0 \dots 01^{x_n} 0 \ \models\Rightarrow \ q_0 01^{x_2} 0 \dots 01^{x_n} 01^{x_1} 0;$$

K_n. Копирование:

$$q_1 01^{x_1} \dots 01^{x_n} 0^{x_1 + \dots + x_n + n + 1} \ \models\Rightarrow$$
$$q_0 01^{x_1} \dots 01^{x_n} \ 01^{x_1} \dots 01^{x_n} 0;$$

Л. Ликвидация: $q_1 01^x 0 \ \models\Rightarrow \ q_0 0^{x+2}$;

R. Вычитание единицы: $q_1 01^{x+1} 0 \ \models\Rightarrow \ q_0 01^x 00$;

S. Добавление единицы: $q_1 01^x 00 \ \models\Rightarrow \ q_0 01^{x+1} 0$.

Пример реализации базовой машины А (перенос нуля):

$q_1 0 \ \to \ q_2 0 R$ --- $\underline{00}111...110$
$q_2 0 \ \to \ q_3 1 R$ --- $0\underline{11}11...110$
$q_3 1 \ \to \ q_3 1 R$ --- $01\underline{111...11}0$
$q_3 0 \ \to \ q_4 0 L$ --- $01111...1\underline{10}$
$q_4 1 \ \to \ q_5 0 L$ --- $01111...\underline{10}0$
$q_5 1 \ \to \ q_5 1 L$ --- $0\underline{1111...1}00$
$q_5 0 \ \to \ q_0 0$ --- $01111...100$

Предложение 8.10. *Следующие функции являются правильно вычислимыми на машине Тьюринга:*

а) $\mathrm{O}(x) = 0$;

б) $S(x) = x + 1$;

в) $I_m^n(x_1, \dots, x_n) = x_m, \ m \le n$;

г) $x + y$;

д) $x \dot{-} 1 = \begin{cases} x - 1, & x \ne 0; \\ 0, & x = 0; \end{cases}$

е) $x \dot{-} y = \begin{cases} x - y, & y \le x; \\ 0, & x \le y; \end{cases}$

ж) $x \cdot y$.

Доказательство: упражнение.

9. ПРИМИТИВНО-РЕКУРСИВНЫЕ, ОБЩЕРЕКУРСИВНЫЕ И ЧАСТИЧНО-РЕКУРСИВНЫЕ ФУНКЦИИ

9.1. Основные определения и обозначения

Определение 9.1. *Следующие функции называются* ***простейшими***:

а) $O(x) = 0$;

б) $S(x) = x + 1$;

в) $I_m^n\,(x_1, \dots, x_n) = x_m,\ m \le n$.

Определение 9.2.

a) ***Оператор суперпозиции***. *Рассмотрим функции*

$$g(x_1, \dots, x_k), \ \text{ и } \ h_1(x_1, \dots, x_n), \dots, h_k(x_1, \dots, x_n).$$

Говорят, что функция

$$f(x_1, \dots, x_n) = g(h_1(x_1, \dots, x_n), \dots, h_k(x_1, \dots, x_n))$$

получена из функций $g, h_1, \dots, h_k$ *применением* ***оператора суперпозиции***.

b) ***Оператор примитивной рекурсии***. *Рассмотрим функции*

$$g(x_1, \dots, x_n) \ \text{ и } \ h(x_1, \dots, x_n, y, z).$$

Пусть выполнено

$$\begin{cases} f(x_1, \dots, x_n, 0) = g(x_1, \dots, x_n); \\ f(x_1, \dots, x_n, y+1) = h\big(x_1, \dots, x_n, y, f(x_1, \dots, x_n, y)\big). \end{cases}$$

Тогда говорят, что функция f *получена из функций* g *и* h *применением* ***оператора примитивной рекурсии***.

c) ***Оператор минимизации***. *Рассмотрим функцию* $g(x_1, \dots, x_n, y)$. *Пусть выполнено:*

$$f(x_1, \dots, x_n) = \begin{cases} y, & \begin{array}{c} g(x_1, \dots, x_n, y) = 0, \\ \forall i < y \ \ g(x_1, \dots, x_n, i) \text{ определена} \\ \text{и } \forall i < y \ \ g(x_1, \dots, x_n, i) \neq 0; \end{array} \\ \text{не определена}, & \text{в противном случае.} \end{cases}$$

Тогда говорят, что функция f *получена из функции* g *применением* ***оператора минимизации***. *Это обозначается так:*

$$f(x_1, \dots, x_n) = \mu y[g(x_1, \dots, x_n, y) = 0].$$

Определение 9.3. ***Примитивно-рекурсивные функции (прф):***

а) простейшие функции являются примитивно-рекурсивными;

б) функция, полученная из примитивно-рекурсивных функций однократным применением оператора суперпозиции или оператора примитивной рекурсии, является примитивно-рекурсивной;

в) других примитивно-рекурсивных функций нет.

Частично-рекурсивные функции (чрф):

а) простейшие функции являются частично-рекурсивными;

б) функция, полученная из частично-рекурсивных функций однократным применением оператора суперпозиции, оператора примитивной рекурсии или оператора минимизации, является частично-рекурсивной;

в) других частично-рекурсивных функций нет.

Общерекурсивными функциями (орф) *называются всюду определённые частично-рекурсивные функции.*

Класс всех примитивно-рекурсивных функций обозначается ***ПРФ****, класс всех общерекурсивных функций –* ***ОРФ****, а класс всех частично-рекурсивных функций –* ***ЧРФ****.*

Замечание 9.4. *Каждая примитивно-рекурсивная функция всюду определена.*

Доказательство. Будем доказывать индукцией по построению функции.

1. $O(x)$, $S(x)$ и $I_m^n(x_1, \dots, x_n)$ всюду определены.

2. а) если функция получена из всюду определённых функций однократным применением оператора суперпозиции, то она всюду определена.

б) если функция получена из всюду определённых функций однократным применением оператора примитивной рекурсии, то она всюду определена.

Замечание 9.4 доказано.

Следствие 9.5. *ПРФ* $\subseteq$ *ОРФ* $\subseteq$ *ЧРФ.*

Доказательство: упражнение.

Замечание 9.6. *ОРФ* $\neq$ *ЧРФ.*

Доказательство. Рассмотрим функцию $\omega(x) = \mu y[S(y) = 0]$. Эта функция является частично-рекурсивной; она нигде не определена, поэтому она не является общерекурсивной функцией.

Замечание 9.6 доказано.

Предложение 9.7. Пусть $g(x_1, \dots, x_n, y)$ – ПРФ. Тогда следующие функции являются примитивно-рекурсивными:

1) $f(x) = n$;

2) $f(x) = x + n$;

3) $f(x, y) = x + y$;

4) $f(x, y) = x \cdot y$;

5) $f(x, y) = x^y$;

6) $sg(x) = \begin{cases} 1, & x > 0; \\ 0, & x = 0; \end{cases}$

7) $sg(x) = \begin{cases} 0, & x > 0; \\ 1, & x = 0; \end{cases}$

8) $f(x, y) = x \dot{-} 1$;

9) $f(x, y) = x \dot{-} y$;

10) $f(x, y) = |x - y|$;

11) $f(x, y) = \max(x, y)$;

12) $f(x, y) = \min(x, y)$;

13) $f(x_1, \dots, x_{n+1}) = \sum_{i=0}^{x_{n+1}} g(x_1, \dots, x_n, i)$;

14) $f(x_1, \dots, x_{n+2}) = \begin{cases} 0, & x_{n+1} > x_{n+2}; \\ \sum_{i=x_{n+1}}^{x_{n+2}} g(x_1, \dots, x_n, i), & x_{n+1} \le x_{n+2}; \end{cases}$

15) $f(x_1, \dots, x_{n+1}) = \prod_{i=0}^{x_{n+1}} g(x_1, \dots, x_n, i)$;

16) $f(x_1, \dots, x_{n+2}) = \begin{cases} 1, & x_{n+1} > x_{n+2}; \\ \prod_{i=x_{n+1}}^{x_{n+2}} g(x_1, \dots, x_n, i), & x_{n+1} \le x_{n+2}; \end{cases}$

17) $\left[\frac{x}{y}\right]$, где $\left[\frac{x}{0}\right] = x$, – целочисленное деление;

18) $rest(x, y)$, где $rest(x, 0) = x$ и $rest(0, y) = 0$, – остаток от деления x на y;

19) $\tau(x)$, где $\tau(0) = 0$, – количество делителей числа x;

20) $\sigma(x)$, где $\sigma(0) = 0$, – сумма всех делителей числа x;

21) $lh(x)$, где $lh(0) = 0$, – количество простых делителей числа x;

22) $\pi(x)$, где $\pi(0) = 0$, $\pi(1) = 0$ – количество простых чисел, не превосходящих числа x;

23) $K(x, y) = \text{НОК}(x, y)$, где $k(x, 0) = k(0, y) = 0$;

24) $D(x, y) = \text{НОД}(x, y)$, где $D(0,0) = 0$;

25) $p(x)$ – x-тое простое число ($p(0) = 2$, $p(1) = 3$, $p(2) = 5$ и т. д.);

26) $ex(x, y)$ – показатель степени x-го простого числа в каноническом разложении числа y;

27) $[\sqrt{x}]$.

Доказательство: упражнение.

9.2. Операторы ограниченной минимизации и возвратной рекурсии

Определение 9.8. *Рассмотрим функции* $g(x_1, \dots, x_n, y)$ *и* $h(x_1, \dots, x_n)$. *Пусть выполнено*

$$f(x_1, \dots, x_n) =$$

$$= \begin{cases} y & \begin{array}{c} g(x_1, \dots, x_n, y) = 0, \\ h(x_1, \dots, x_n) \text{ определена} \\ y \le h(x_1, \dots, x_n), \\ \forall i < y \;\; g(x_1, \dots, x_n, i) \text{ определена}, \\ g(x_1, \dots, x_n, i) \ne 0; \end{array} \\ h(x_1, \dots, x_n) + 1, & \begin{array}{c} h(x_1, \dots, x_n) \text{ определена}, \\ \forall i \le h(x_1, \dots, x_n) \\ g(x_1, \dots, x_n, i) \text{ определена} \\ g(x_1, \dots, x_n, i) \ne 0; \end{array} \\ \text{не определена}, & \text{в противном случае.} \end{cases}$$

Тогда говорят, что функция f получена из функций g и h применением оператора ***ограниченной минимизации****. Это обозначается так:*

$$f(x_1, \dots, x_n) = \mu y \leq h(x_1, \dots, x_n)[g(x_1, \dots, x_n, y) = 0].$$

Предложение 9.9. Пусть $g(x_1, \dots, x_n, y)$ и $h(x_1, \dots, x_n)$ – примитивно-рекурсивные функции и функция $f(x_1, \dots, x_n)$ получена из функций g и h с помощью оператора ограниченной минимизации. Тогда функция f также является примитивно-рекурсивной. (Т. е. ограниченная минимизация сохраняет примитивную рекурсивность функций.)

Доказательство. Из Предложения 9.7 следует, что функция

$$\sum_{i=0}^{h(x_1,\dots,x_n)} sg\left(\prod_{j=0}^{i} g(x_1, \dots, x_n, j)\right)$$

является примитивно-рекурсивной. Покажем, что она совпадает с функцией f.

Пусть существует такое $y \leq h(x_1, \dots, x_n)$, что

$$g(x_1, \dots, x_n, y) = 0,$$

и для любого $z < y$ выполнено

$$g((x_1, \dots, x_n, z) \neq 0.$$

Тогда для любого $i < y$ имеем

$$\prod_{j=0}^{i} g(x_1, \dots, x_n, j) \neq 0.$$

Следовательно,

$$sg\left(\prod_{j=0}^{i} g(x_1, \dots, x_n, j)\right) = 1.$$

Если $y \leq i \leq h(x_1, \dots, x_n)$, то

$$\prod_{j=0}^{i} g(x_1, \dots, x_n, j) = 0.$$

В этом случае получим

$$sg\left(\prod_{j=0}^{i} g(x_1, \dots, x_n, j)\right) = 0.$$

Значит,

$$f(x_1, \dots, x_n) = y = \sum_{i=0}^{h(x_1,\dots,x_n)} sg\left(\prod_{j=0}^{i} g(x_1, \dots, x_n, j)\right)$$

– сумма y единиц.

Пусть теперь функция $g(x_1, \dots, x_n, y)$ и функция $h(x_1, \dots, x_n)$ определены и для любого $i \le h(x_1, \dots, x_n)$ выполнено $g(x_1, \dots, x_n, i) \neq 0$. Тогда для любого $i \le h(x_1, \dots, x_n)$ выполнено

$$\prod_{j=0}^{i} g(x_1, \dots, x_n, j) \neq 0.$$

Следовательно,

$$sg\left(\prod_{j=0}^{i} g(x_1, \dots, x_n, j)\right) = 1.$$

Значит,

$$f(x_1, \dots, x_n) = h(x_1, \dots, x_n) + 1 = \sum_{i=0}^{h(x_1,\dots,x_n)} sg\left(\prod_{j=0}^{i} g(x_1, \dots, x_n, j)\right)$$

– сумма $h(x_1, \dots, x_n) + 1$ единицы.

Предложение 9.9 доказано.

Определение 9.10. *Рассмотрим функции*

$$g(x_1, \dots, x_n), g_1(x_1, \dots, x_n, y), \dots, g_k(x_1, \dots, x_n, y),$$
$$h(x_1, \dots, x_n, y, z_1, \dots, z_k)$$

такие, что для любых $x_1, \dots, x_n, y$ *выполняются неравенства*

$$g_1(x_1, \dots, x_n, y) \le y, \ \dots, \ g_n(x_1, \dots, x_n, y) \le y.$$

Пусть функция f *определена следующим образом*:

$$\begin{cases} f(x_1, \dots, x_n, 0) = g(x_1, \dots, x_n); \\ f(x_1, \dots, x_n, y+1) = h\begin{pmatrix} x_1, \dots, x_n, y, f(x_1, \dots, x_n, g_1(x_1, \dots, x_n, y)), \dots, \\ f(x_1, \dots, x_n, g_k(x_1, \dots, x_n, y)) \end{pmatrix} \end{cases}$$

Тогда говорят, что функция f *получена из функций* $g, g_1, \dots, g_k$ и h *применением* ***оператора возвратной рекурсии***.

Предложение 9.11. Пусть

$$g(x_1,\dots,x_n),\ g_1(x_1,\dots,x_n,y),\ \dots,\ g_k(x_1,\dots,x_n,y),$$
$$h(x_1,\dots,x_n,y,z_1,\dots,z_k)$$

– примитивно-рекурсивные функции и пусть функция $f(x_1,\dots,x_n,y)$ получена из функций g, $g_1,\dots$, g_k и h применением оператора возвратной рекурсии. Тогда функция f также является примитивно-рекурсивной. (Т. е. оператор возвратной рекурсии сохраняет примитивную рекурсивность функций.)

Доказательство. Пусть

$$F(x_1,\dots,x_n,y)=\prod_{i=0}^{y} p_i^{f(x_,\dots,x_n,)},$$

где $p_i - i$-е простое число. Покажем, что функция F является примитивно-рекурсивной. Рассмотрим однократное применение оператора примитивной рекурсии:

$$\begin{cases} F(x_1,\dots,x\,,0)=2^{g(x_1,\dots,x_n)}; \\ F(x_1,\dots,x_n,y+1)=F(x_1,\dots,x_n,y)\times p_{y+1}^{h\left(\begin{smallmatrix} x_1,\dots,x_n,y, \\ ex(g_1(x_1,\dots,x_n,y),F(x_1,\dots,x_n,y)),\dots, \\ ex(g_k(x_1,\dots,x_n,y),F(x_1,\dots,x_n,y))\end{smallmatrix}\right)}. \end{cases}$$

Пусть

$$H\left(x_{1,}\dots,x_n,y,z\right)=z\times p_{y+1}^{h\left(\begin{smallmatrix} x_1,\dots,x_n,y, \\ ex(g_1(x_1,\dots,x_n,y),z),\dots, \\ ex(g_k(x_1,\dots,x_n,y),z)\end{smallmatrix}\right)};$$

нетрудно проверить, что функция $H\left(x_{1,}\dots,x_n,y,z\right)$ является примитивно-рекурсивной как суперпозиция примитивно-рекурсивных функций. Тогда задание функции $F(x_1,\dots,x_n,y)$ однократным применением оператора примитивной рекурсии можно записать следующим образом:

$$\begin{cases} F(x_1,\dots,x\,,0)=2^{g(x_1,\dots,x_n)}; \\ F(x_1,\dots,x_n,y+1)=H\left(x_{1,}\dots,x_n,y,F(x_1,\dots,x_n,y)\right). \end{cases}$$

Следовательно, функция $F(x_1,\dots,x_n,y)$ получена из примитивно-рекурсивных функций $2^{g(x_1,\dots,x_n)}$ и $H\left(x_{1,}\dots,x_n,y,z\right)$ однократным применением оператора примитивной рекурсии. Поэтому функция $F(x_1,\dots,x_n,y)$ также является примитивно-рекурсивной.

Стало быть, и функция

$$f(x_1, \dots, x_n, y) = ex\big(y, F(x_1, \dots, x_n, y)\big)$$

является примитивно-рекурсивной.

Предложение 9.11 доказано.

9.3. Канторовская нумерация

Определение 9.12. *Функция* $c(x,y) = \left[\frac{(x+y)^2+3x+y}{2}\right]$, $c\colon \mathbb{N}^2 \to \mathbb{N}$, *называется* ***канторовской нумерующей функцией*** (***канторовской нумерацией***).

Предложение 9.13. *Существуют функции* $l\colon \mathbb{N} \to \mathbb{N}$ *и* $r\colon \mathbb{N} \to \mathbb{N}$ *такие, что*

а) для любых $x, y \in \mathbb{N}$ *если* $c(x,y) = m$*, то* $l(m) = x$ *и* $r(m) = y$*;*

б) для любого $m \in \mathbb{N}$ *выполнено* $c\big(l(m), r(m)\big) = m$*.*

Доказательство. Упражнение – нужно показать, что требуемыми свойствами обладают функции

$$l(m) = m \dot- \left[\frac{\left[\frac{[\sqrt{8m+1}]+1}{2}\right]\cdot\left[\frac{[\sqrt{8m+1}]\dot-1}{2}\right]}{2}\right]$$

и

$$r(m) = \left[\frac{[\sqrt{8m+1}]+1}{2}\right] \dot- (l(m)+1).$$

Предложение 9.13 доказано.

Следствие 9.14. *Отображение* $c\colon \mathbb{N}^2 \to \mathbb{N}$ *является взаимно-однозначным.*

Доказательство: упражнение.

Замечание 9.15. *Функции* $c(x,y), l(m), r(m)$ *являются примитивно-рекурсивными.*

Доказательство: упражнение.

Определение 9.16.

1. $c_2(x,y) = c(x,y)$.
2. $c_1^2(m) = l(m)$.

3. $c_2^2(m) = r(m)$.

4. $c_{n+1}(x_1, \dots, x_{n+1}) = c(c_n(x_1, \dots, x_n), x_{n+1})$.

5. $c_k^{n+1}(m) = c_k^n(l(m)),\ k \leq n$.

6. $c_{n+1}^{n+1}(m) = r(m)$.

Замечание 9.17. *Функции* $c_n(x_1, \dots, x_n)$ *и* $c_n^k(m)$, $k \leq n$, *являются примитивно-рекурсивными.*

Доказательство: упражнение.

Замечание 9.18.

а. *Для любых* $x_1, \dots, x_n \in \mathbb{N}$ *если* $c_n(x_1, \dots, x_n) = m$, *то*

$$c_k^n(m) = x_k,\ k \leq n.$$

б. Для любого $m \in \mathbb{N}$ *выполнено*

$$c_n(c_1^n(m), \dots, c_n^n(m)) = m.$$

Доказательство: упражнение.

Следствие 9.19. *Отображение* $c_n \colon \mathbb{N}^n \to \mathbb{N}$ *является взаимно-однозначным.*

Доказательство: упражнение.

Замечание 9.20.

1. Если функция $f(x_1, \dots, x_n)$ *является примитивно-рекурсивной, то функция* $h(y) = f\left(c_n^1(y), \dots, c_n^n(y)\right)$ *также является примитивно-рекурсивной.*

2. *Если функция* $h(y)$ *является примитивно-рекурсивной, то функция* $f(x_1, \dots, x_n) = h\left(c_n(x_1, \dots, x_n)\right)$ *также является примитивно-рекурсивной.*

Доказательство: упражнение.

Предложение 9.21. *Имеют место следующие включения:*

$$\text{ПРФ} \subseteq \text{ОРФ} \subseteq \text{ЧРФ} \ \text{ и } \ \text{ПРФ} \neq \text{ОРФ} \neq \text{ЧРФ}.$$

Без доказательства: ПРФ ≠ ОРФ.

Учебное издание

Пальчунов Дмитрий Евгеньевич

МАТЕМАТИЧЕСКАЯ ЛОГИКА И ТЕОРИЯ АЛГОРИТМОВ

ЧАСТЬ ПЕРВАЯ

Учебное пособие

Редактор *Д. И. Ковалева*
Оригинал-макет *Д. Е. Пальчунова*
Обложка *Е. В. Неклюдовой*

Подписано в печать 14.07.2016.
Формат 60 x 84 1/16. Уч.-изд. л. 6. Усл. печ. л. 5,6
Тираж 150 экз. Заказ №
Редакционно-издательский центр НГУ
630090, Новосибирск-90, ул. Пирогова, 2.