

Коллоквиум №1 (20.11.2019)

GROUPS №19137, №19144

2019

1. Множество: способы задания, операции над множествами
Не существует явного определения множества.
Пусть A некоторое мн-во, тогда существует 2 способа задания мн-ва

(a) $A = \{1, 2, 3, 4, 5\}$ - явное задание эл-тов мн-ва

(b) Пусть $\Phi(x)$ - некоторое условие, тогда
 $A = \{x \mid \Phi(x)\}$ - Задание множества с помощью некоторого условия $\Phi(x)$

Пусть A, B - некоторые множества

Обозначение (Подмножество). A - подмножество B , если $A \subseteq B = \{x \mid x \in A \Rightarrow x \in B\}$

Обозначение (Собственное подмножество). A - собственное подмножество B , если $A \subset B$, если $A \subseteq B$ и $A \neq B$

Обозначение (Пустое множество). \emptyset - множество, не содержащее эл-тов ("Пустое множество")

Обозначение (Множество всех подмножеств множества A). $P(A) = \{C \mid C \subseteq A\}$

Обозначение (Универсум). Универсум (условное множество все множеств) U

Операции над множествами:

- Объединение множеств:
 $A \cup B = \{x \mid x \in A \vee x \in B\}$
- Пересечение множеств:
 $A \cap B = \{x \mid x \in A \wedge x \in B\}$
- Разность множеств:
 $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$
- Дополнение множества:
 $\neg A = \{x \mid x \in U \wedge x \notin A\}$
- Симметрическая разность множеств:
 $A \Delta B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (B \cap A)$

Пусть S - семейство множеств:

- Объединение семейства множеств

$$\bigcup S = \{ x \mid \exists A_i \in S : x \in A_i \}$$

- Пересечение семейства множеств

$$\bigcap S = \{ x \mid \forall A_i \in S : x \in A_i \}$$

2. Упорядоченный набор (кортеж), предложение о равенстве n-ок, декартово произведение, декартова степень.

Определение (Упорядоченный набор (кортеж)). Упорядоченный набор (кортеж) длины n определяется по индукции

$$\langle \rangle = \emptyset$$

$$\langle a \rangle = a$$

$$\langle a, b \rangle = \{ \{a\}, \{a, b\} \}$$

...

$$\langle a_1, a_2, \dots, a_{n-1}, a_n \rangle = \langle \langle a_1, a_2, \dots, a_{n-1} \rangle, a_n \rangle$$

Определение (пара). Набор $\langle a, b \rangle$ длины 2 называют *парой*

Предложение (о равенстве n-ок). Если

$$\langle a_1, \dots, a_n \rangle = \langle b_1, \dots, b_n \rangle \Leftrightarrow a_1 = b_1, \dots, a_n = b_n$$

Доказательство. для $n = 1$ очевидно в обе стороны. Докажем для $n = 2$:

$$\langle a_1, a_2 \rangle = \langle b_1, b_2 \rangle \Leftrightarrow \{ \{a_1\}, \{a_1, a_2\} \} = \{ \{b_1\}, \{b_1, b_2\} \}$$

$$\text{Пусть } a_1 = a_2 \Rightarrow \begin{cases} \{a_1\} = \{b_1, b_2\} \\ \{a_1, a_2\} = \{b_1, b_2\} \end{cases} \Rightarrow a_1 = a_2 = b_1 = b_2$$

для $b_1 = b_2$ аналогично.

Рассмотрим $a_1 \neq a_2, b_1 \neq b_2$

$$\Rightarrow \begin{cases} \{a_1\} = \{b_1\} \\ \{a_1\} = \{b_1, b_2\} \end{cases} \Rightarrow \{a_1\} = \{b_1\} \Rightarrow a_1 = b_1$$

По аналогии для $\{a_1, a_2\} = \{b_1, b_2\}$

Т.к справедливо для $n = 2$, а определение n-ок индуктивно следовательно верно для n \square

Определение (Декартово произведение). Пусть даны множества A_1, \dots, A_n , тогда их декартовым произведением называют

$$A_1 \times A_2 \times \dots \times A_n = \{ \langle a_1, \dots, a_n \rangle \mid \forall i \in \{1, \dots, n\} a_i \in A_i \}$$

Определение (Декартова степень). В случае, если $A_1 = A_2 = \dots = A_n$, тогда $A_1 \times A_2 \times \dots \times A_n$ называют декартовой степенью и обозначают, как $A^n = A_1 \times A_2 \times \dots \times A_n$

3. Бинарные отношения, обратное отношение, произведение отношений, лемма о бинарных отношениях.

Определение. Бинарным отношением между элементами множеств A и B называется произвольное подмножество $C \subseteq A \times B$

Определение. Обратным бинарным отношением называется $R^{-1} = \{ \langle y; x \rangle \mid \langle x; y \rangle \in R \}$

Определение. Произведением бинарных отношений называется $R_1 \times R_2 = \{ \langle x; z \rangle \mid \exists y \mid \langle x; y \rangle \in R_1 \wedge \langle y; z \rangle \in R_2 \}$

Лемма (Лемма о бинарных отношениях). Для любых бинарных отношений R_1, R_2, R_3 :

$$(a) \quad R_1 \cdot (R_2 \cdot R_3) = (R_1 \cdot R_2) \cdot R_3$$

$$(b) \quad (R_1 \cdot R_2)^{-1} = R_2^{-1} \cdot R_1^{-1}$$

Доказательство. (a) Покажем, что $R_1 \cdot (R_2 \cdot R_3) \subseteq (R_1 \cdot R_2) \cdot R_3$.

Пусть $\langle x; t \rangle \in R_1 \cdot (R_2 \cdot R_3)$, тогда существует y такое, что $\langle x; y \rangle \in R_1$ и $\langle y; t \rangle \in R_2 \cdot R_3$. Далее существует z такое, что $\langle y; z \rangle \in R_2$ и $\langle z; t \rangle \in R_3$. Получаем, что $\langle x; z \rangle \in R_1 \cdot R_2$ и $\langle z; t \rangle \in R_3$. Обратное включение доказывается аналогично.

(b) Покажем, что $(R_1 \cdot R_2)^{-1} \subseteq R_2^{-1} \cdot R_1^{-1}$.

Пусть $\langle z; x \rangle \in (R_1 \cdot R_2)^{-1}$, тогда существует y такое, что $\langle x; y \rangle \in R_1$ и $\langle y; z \rangle \in R_2$. Тогда $\langle y; x \rangle \in R_1^{-1}$ и $\langle z; y \rangle \in R_2^{-1}$. Получаем, что $\langle z; x \rangle \in R_2^{-1} \cdot R_1^{-1}$. Обратное включение доказывается аналогично.

□

4. Область определения отношения, множество значений отношения, образ и прообраз множества относительно отношений, функция, замечание о равенстве функций, тождественная функция.

Определение (Функция). Бинарное отношение f называется функцией, если выполняется: $\langle x, y_1 \rangle, \langle x, y_2 \rangle \in f \Rightarrow y_1 = y_2$

Определение (Область определения). $dom(f) = \{x \mid \exists y : \langle x, y \rangle \in f\}$

Определение (Область значений). $ran(f) = \{y \mid \exists x : \langle x, y \rangle \in f\}$

Обозначение. f - функция из A в B , если f - функция, $dom(f) = A$ и $ran(f) \subseteq B$

Тогда функцию обозначают $f : A \rightarrow B$

Замечание. Если $f : A \rightarrow B$ и $x \in A$, то существует единственный y такой, что $\langle x, y \rangle \in f$. Этот y лежит в B , называется значение функции f в точке x и обозначается $f(x)$.

Замечание (о равенстве функций). Если f, g - функции, то $f = g \Leftrightarrow dom(f) = dom(g)$ и $\forall x \in dom(f) \quad f(x) = g(x)$

Определение (Тождественная функция). Для любого множества A $\exists f = \{ \langle x, x \rangle \mid x \in A \} = id_A$. Ясно, что $id_A : A \rightarrow A$ и $\forall x \in A \ id_A(x) = x$

5. Композиция функций, лемма о композиции функций:

Определение (Композиция функций). Если f и g - функции, то их композиция $g \circ f$ определяется, как произведение бинарных отношений $f \cdot g$ (В обратном порядке)

Лемма (о композиции функций). Если $f : A \rightarrow B, g : B \rightarrow C$, то их композицией $g \circ f : A \rightarrow C$ и $[g \circ f](x) = g(f(x))$ при $x \in A$

6. Сюръекция, инъекция, биекция, обратная функция, лемма о свойствах биекций

Пусть $f : A \rightarrow B$

Определение (Сюръекция). f - функция из A на B (сюръективная функция, сюръекция), если $\forall y \in B \ \exists x \in A \mid f(x) = y$

Обозначение (Сюръекция). $f : A \xrightarrow[на]{} B$.

Определение (Инъекция). f - инъективная функция (1 - 1 функция, инъекция), если $\forall x_1, x_2 \in A$ из $f(x_1) = f(x_2)$ следует $x_1 = x_2$

Обозначение (Инъекция). $f : A \xrightarrow{1-1} B$

Определение (Биекция). f - биекция из A на B , если f одновременно и инъекция, и сюръекция.

Обозначение (Биекция). $f : A \xrightarrow[на]{1-1} B$

Определение (Обратная функция). Запись f^{-1} означает обратное бинарное отношение к f . Если f^{-1} при этом является функцией, то она называется *обратной функцией* к f .

Лемма (о свойствах биекций).

(a) Если $f : A \xrightarrow[на]{1-1} B$, то $f^{-1} : B \xrightarrow[на]{1-1} A$, $f^{-1}(f(x)) = x \ \forall x \in A$ и $f(f^{-1}(y)) = y \ \forall y \in B$.

(b) Если $f : A \xrightarrow[на]{1-1} B, g : B \xrightarrow[на]{1-1} C$, то $f \circ g : A \xrightarrow[на]{1-1} C$.

Доказательство. (a) Покажем, что f^{-1} - функция.

Пусть $\langle y, x_1 \rangle, \langle y, x_2 \rangle \in f^{-1}$. Тогда $\langle x_1, y \rangle, \langle x_2, y \rangle \in f$ и $f(x_1) = f(x_2) = y$. Поскольку f инъективна, $x_1 = x_2$.

Ясно, что $dom(f^{-1}) = ran(f)$ и $ran(f^{-1}) = dom(f)$. Поскольку f сюръективна, $ran(f) = B = dom(f^{-1})$. Поскольку $ran(f^{-1}) = A$, f^{-1} сюръективна. Инъективность f^{-1} легко проверяется. Тем самым $f^{-1} : B \xrightarrow[на]{1-1} A$.

Покажем, что $f^{-1}(f(x)) = x$ при $x \in A$. Пусть $x \in A$ и $y = f(x)$. Тогда $\langle x, y \rangle \in f$ и $\langle y, x \rangle \in f^{-1}$. Получаем, что $f^{-1}(y) = x$.

- (b) выше доказано, что $g \circ f : A \rightarrow C$ и $[g \circ f](x) = g(f(x))$. Инъективность: если $g(f(x_1)) = g(f(x_2))$, то $f(x_1) = f(x_2)$ и отсюда $x_1 = x_2$. Сюръективность доказывается похожим способом.

□

7. Отношения эквивалентности, классы эквивалентности, лемма о классах эквивалентности.
8. Частичный порядок, ч.у.м., минимальные, максимальные, наименьшие, наибольшие элементы, связи между ними. Замечание о строгом порядке.
9. Фундированные частичные порядки, критерий фундированности порядка.
10. Предложение об индукции в фундированном ч.у.м., изоморфизм ч.у.м., замечание об изоморфизме ч.у.м.
11. Линейные порядки, л.у.м., начальные сегменты и отрезки, лемма о свойствах начальных сегментов.

2.6. Линейно упорядоченные множества

Пусть \leq — частичный порядок на A , $x, y \in A$. Говорим, что x, y *сравнимы* относительно \leq , если $x \leq y$ или $y \leq x$. Частичный порядок \leq называется *линейным*, если $x \leq y$ или $y \leq x$ для любых $x, y \in A$, т.е. если любые два элемента в A сравнимы. В этом случае пара (A, \leq) называется *линейно упорядоченным множеством* (л.у.м.).

Замечание. Если (A, \leq) — л.у.м. и элемент $x \in A$, то:

- а) x является минимальным тогда и только тогда, когда является наименьшим;
- б) x является максимальным тогда и только тогда, когда является наибольшим.

Множество $S \subseteq A$ называется *начальным сегментом* л.у.м. (A, \leq) , если для любых $x, y \in A$ из $x \in S$ и $y \leq x$ следует $y \in S$.

Лемма (о свойствах начальных сегментов). Пусть дано л.у.м. (A, \leq) . Тогда:

- а) если S_1, S_2 — начальные сегменты, то $S_1 \subseteq S_2$ или $S_2 \subseteq S_1$;
- б) если S — начальный сегмент, а x — минимальный элемент в $A \setminus S$, то $S \cup \{x\}$ — тоже начальный сегмент;
- с) объединение любого семейства начальных сегментов — снова начальный сегмент.

а): предположим, что $S_1 \not\subseteq S_2$, и покажем, что $S_2 \subseteq S_1$. Пусть $x \in S_1 \setminus S_2$. Рассмотрим $y \in S_2$. Случай $x \leq y$ невозможен, так как тогда $x \in S_2$. Значит, $y \leq x$. Получаем, что $y \in S_1$.

б): пусть $z \in S \cup \{x\}$ и $y \leq z$. Покажем, что $y \in S \cup \{x\}$. Если $z \in S$, то $y \in S$. Пусть $z = x$. Если $y = x$, то $y \in S \cup \{x\}$. Если же $y < x$, то y не может лежать в $A \setminus S$. Значит, $y \in S$.

с): пусть D — семейство начальных сегментов и $S' = \bigcup_{S \in D} S$. Проверим, что S' — начальный сегмент. Пусть $x \in S'$ и $y \leq x$. Тогда существует $S \in D$ т.ч. $x \in S$. Следовательно, $y \in S$ и $y \in S'$.

Начальным отрезком л.у.м. (A, \leq) , отсекаемым элементом $x \in A$, называется множество $A_x = \{y \in A \mid y < x\}$.

Замечание. Начальный отрезок всегда является начальным сегментом.

12. Изоморфизм ч.у.м., изоморфизм л.у.м., признак изоморфизма л.у.м., лемма о монотонной инъекции в.у.м.

f — *изоморфизм между* (A, \leq_A) и (B, \leq_B) , если f — биекция из A на B и $x \leq_A y \Leftrightarrow f(x) \leq_B f(y)$ при любых $x, y \in A$.

Ч.у.м. называются *изоморфными*, если между ними существует изоморфизм. Обозначим это как $(A, \leq_A) \cong (B, \leq_B)$.

Замечание. Изоморфность обладает свойствами отношения эквивалентности:

- а) $(A, \leq_A) \cong (A, \leq_A)$;
- б) если $(A, \leq_A) \cong (B, \leq_B)$, то $(B, \leq_B) \cong (A, \leq_A)$;
- с) если $(A, \leq_A) \cong (B, \leq_B)$ и $(B, \leq_B) \cong (C, \leq_C)$, то $(A, \leq_A) \cong (C, \leq_C)$.

а): функция id_A является искомым изоморфизмом; б): если $f : A \rightarrow B$ — изоморфизм, то $f^{-1} : B \rightarrow A$ — тоже изоморфизм; с): если $f : A \rightarrow B$ и $g : B \rightarrow C$ — изоморфизмы, то $g \circ f$ — тоже изоморфизм. Всё это легко проверяется.

Лемма (признак изоморфизма л.у.м.). Если (A, \leq) , (B, \leq) — л.у.м. и $f : A \rightarrow B$ — монотонная биекция, то f — изоморфизм.

Нужно лишь проверить переход $f(x) \leq f(y) \Rightarrow x \leq y$. Пусть $f(x) \leq f(y)$. Допустим, что $x \not\leq y$. Тогда $y \leq x$, $f(y) \leq f(x)$ и $f(y) = f(x)$. В силу инъективности $x = y$, $\uparrow\downarrow$.

Лемма. Если (A, \leq) — в.у.м. и $f : A \xrightarrow{1-1} A$ — монотонная инъекция, то $f(x) \geq x$ при всех $x \in A$.

Заметим: если $x, y \in A$ и $x < y$, то $f(x) < f(y)$. Из монотонности получаем, что $f(x) \leq f(y)$, а из инъективности — что $f(x) \neq f(y)$.

Допустим, что утверждение неверно: существует $x \in A$ т. ч. $f(x) \not\geq x$. Поскольку порядок линейен, $f(x) < x$. Тогда

$$f(f(x)) < f(x), f(f(f(x))) < f(f(x)), \text{ и т. д.}$$

Получаем последовательность $x > f(x) > f(f(x)) > \dots$, $\uparrow\downarrow$.

13. Полный порядок, в.у.м., лемма о начальных сегментах в.у.м.

Определение (Вполне упорядоченное множество). *Вполне упорядоченное множество* (в.у.м.) — это пара (A, \leq) , где \leq — линейный фундаментальный порядок на A . Иногда такой порядок называют *полным*.

Лемма (о начальных сегментах в.у.м.). *Любой начальный сегмент в.у.м. (A, \leq) либо равен A , либо является начальным отрезком.*

Доказательство. Пусть S — начальный сегмент в A и $S \neq A$. Тогда $A \setminus S \neq \emptyset$. Пусть x — минимальный элемент в $A \setminus S$. Покажем, что $S = A_x$. Если $y \in S$, то либо $y < x$, либо $x \leq y$. Второй случай невозможен, так как тогда $x \in S$. \square

14. Предложение об изоморфизме начальных сегментов, теорема о сравнимости в.у.м. (без доказательства).

Предложение (об изоморфизме начальных сегментов). Различные начальные сегменты в.у.м. не могут быть изоморфны друг другу.

Доказательство. Пусть S_1 и S_2 — два различных сегмента в.у.м. (A, \leq) . Тогда сначала докажем лемму о том, что если (A, \leq) — в.у.м. и $f : A \xrightarrow{1-1} A$ — монотонная инъекция, то $f(x) \geq x \forall x \in A$.

Заметим: если $x, y \in A$ и $x < y$, то $f(x) < f(y)$. Из монотонности получаем, что $f(x) \leq f(y)$, а из инъективности — что $f(x) \neq f(y)$.

Допустим, что утверждение неверно: существует $x \in A$ | $f(x) \not\geq x$.

Поскольку ряд линейен, $f(x) < x$. Тогда

$$f(f(x)) < f(x), f(f(f(x))) < f(f(x)), \text{ и т. д.}$$

Получаем последовательность $x > f(x) > f(f(x)) > \dots$, противоречие.

По доказанной лемме $S_1 \subseteq S_2$ или $S_2 \subseteq S_1$. Пусть $S_1 \subseteq S_2$. Выберем $x_0 \in S_2 \setminus S_1$.

Мы рассматриваем эти сегменты как в.у.м. с индуцированным из A порядком. Допустим, что $f : S_2 \rightarrow S_1$ - изоморфизм. Рассматривая f как функцию из S_2 в S_2 , видим, что она инъективна и монотонна. Следовательно, $f(x_0) \geq x_0$. Поскольку S_1 начальный сегмент и $f(x_0) \in S_1$, получаем, что $x_0 \in S_1$, противоречие. \square

Теорема (о сравнимости в.у.м.). *Если даны два в.у.м., то одно из них изоморфно начальному сегменту другого.*

15. Аксиома выбора, лемма Цорна (без доказательства), теорема Цермело (без доказательства), эквивалентность утверждений.

Аксиома выбора. Для любого множества A существует функция $f : P(A) \setminus \{\emptyset\} \rightarrow A$ т. ч. $f(X) \in X$ для всех $X \in P(A) \setminus \{\emptyset\}$.

Пусть (A, \leq) — ч.у.м. Подмножество $B \subseteq A$ называется *цепью*, если любые два элемента из B сравнимы, т. е. $x \leq y$ или $y \leq x$ для любых $x, y \in B$.

Элемент $x \in A$ называется *верхней гранью* подмножества $B \subseteq A$, если $y \leq x$ для всех $y \in B$, и *нижней гранью*, если $x \leq y$ для всех $y \in B$. Если в множестве всех верхних граней B есть наименьший элемент, то он называется *супремумом* B и обозначается $\sup(B)$. Наибольший элемент множества всех нижних граней называется *инфимумом* B и обозначается $\inf(B)$.

Лемма Цорна (принцип максимума). Если в ч.у.м. у каждой цепи есть верхняя грань, то в этом ч.у.м. есть максимальный элемент.

Говорим, что множество можно *вполне упорядочить*, если на нём существует линейный фундированный порядок, т. е. порядок, при котором оно станет вполне упорядоченным.

Теорема Цермело. Любое множество можно вполне упорядочить.

Ниже будет показано, что аксиома выбора, лемма Цорна и теорема Цермело в некотором смысле равносильны.

16. Парадокс Рассела, аксиоматика ZFC.

Парадокс (Парадокс Рассела). Рассмотрим совокупность: $M_R = \{A \mid A - \text{множество и } A \notin A\}$.

Предположим, что само M_R является множеством. Возможны два варианта:

- (a) $M_R \notin M_R$. Тогда $A = M_R$ подходит под определение, и $M_R \notin M_R$. Противоречие.
- (b) $M_R \in M_R$. Вновь полагая, $A = M_R$, получаем, что по определению $M_R \notin M_R$. Противоречие.

Это рассуждение показывает, что совокупность M_R нельзя считать множеством.

Аксиоматика ZFC.

Можно с собой на листочке!!!

17. Равномощные множества, замечание о равномощности.

Обозначение (мощность множества). Мощность множества A обозначается $|A|$.

Определение (равномощные множества). Говорим, что множества A и B равномощные, если существует биекция $f : A \xrightarrow[\text{на}]{1-1} B$.
Обозначим это символической записью $|A| = |B|$.

Замечание (о равномощности). Равномощность обладает свойствами отношения эквивалентности - для любых множеств A, B, C верно:

- (a) $|A| = |A|$;
- (b) $|A| = |B| \Rightarrow |B| = |A|$;
- (c) $|A| = |B|$ и $|B| = |C| \Rightarrow |A| = |C|$;

Доказательство. Следует из леммы о свойствах биекций. □

18. Лемма о порядке на мощностях.

Лемма (Лемма о порядке на мощностях). Для всяких непустых множеств A и B следующие условия эквивалентны:

- (a) $|A| \leq |B|$
- (b) Существует функция $g : B \xrightarrow{HA} A$
- (c) A равномощно некоторому подмножеству B

Доказательство.

- (a) $a \Rightarrow c$
Пусть $|A| \leq |B|$.
Тогда существует $f : A \xrightarrow{1-1}_{\text{на}} B$.
Тогда $\text{ran}(f) \subseteq B$ и $f : A \xrightarrow[\text{на}]{1-1} \text{ran}(f)$.

- (b) $c \Rightarrow b$
Пусть $h : B_1 \xrightarrow[\text{на}]{1-1} A$, где $B_1 \subseteq B$.
Выберем произвольное $a_0 \in A$ и построим $g : B \xrightarrow[\text{на}} A$ так: $g(y) =$

$$\begin{cases} h(y), & \text{если } y \in B_1 \\ a_0, & \text{если } y \in B \setminus B_1 \end{cases}$$

(с) $b \Rightarrow a$

Пусть $g : B \rightarrow A$.

Построим $f : B \rightarrow A$.

Рассмотрим $x \in A$

Множество $\{y \in B \mid g(y) = x\}$ непусто.

Выберем в качестве $f(x)$ некоторый элемент из этого множества.

Проверим, что f инъективна. Пусть $f(x_1) = f(x_2)$

Тогда $g(f(x_1)) = g(f(x_2))$, а по построению $g(f(x_i)) = x_i$ при $i = 1, 2$.

□

19. Теорема Кантора-Бернштейна.

20. Теорема о сравнимости мощностей, теорема Кантора.

Теорема (о сравнимости мощностей). Если A, B — множества, то $|A| \leq |B|$ или $|B| \leq |A|$.

По теореме Цермело A и B можно вполне упорядочить: найдутся порядки \leq_A и \leq_B т. ч. (A, \leq_A) и (B, \leq_B) — в.у.м. По теореме о сравнимости в.у.м. одно из них изоморфно начальному сегменту второго. Предположим, что (A, \leq_A) изоморфно S — начальному сегменту (B, \leq_B) . Тогда $|A| = |S| \leq |B|$.

Теорема Кантора. $|A| < |P(A)|$ для любого множества A .

Покажем, что $|A| \leq |P(A)|$. Построим $f : A \rightarrow P(A)$ так: $f(x) = \{x\}$. Ясно, что f инъективна.

Допустим теперь, что $|A| = |P(A)|$. Тогда существует биекция $g : A \xrightarrow[\text{на}]{1-1} P(A)$. Положим $B = \{x \in A \mid x \notin g(x)\}$. Поскольку $B \in P(A)$, найдётся $x_0 \in A$ т. ч. $g(x_0) = B$. Тогда либо $x_0 \in B$, либо $x_0 \notin B$. Если $x_0 \in B$, то $x_0 \in g(x_0)$ и $x_0 \notin B$. Если же $x_0 \notin B$, то $x_0 \notin g(x_0)$ и $x_0 \in B$, $\uparrow\downarrow$.

Заметим, что теорема Кантора тоже показывает, что множества всех множеств не существует: если M — множество всех множеств, то $P(M) \subseteq M$, и тем самым $|P(M)| \leq |M|$. Это рассуждение называется *парадоксом Кантора*.

Множество A называется *конечным множеством мощности k* , если $|A| = |\mathbb{N}_k|$, где $k \in \mathbb{N}$, а $\mathbb{N}_k = \{x \in \mathbb{N} \mid x < k\}$. Множество *бесконечно*, если оно не является конечным. Множество A *счётно*, если $|A| = |\mathbb{N}|$, и *континуально*, если $|A| = |\mathbb{R}|$, где \mathbb{R} — множество вещественных чисел.

Мы не будем доказывать некоторые простые свойства конечных множеств, считая их очевидными: например то, что подмножество конечного множества является конечным. Они могут быть доказаны через свойства натуральных чисел и индукцию.

21. Конечные, бесконечные, счетные, континуальные множества, описание не более чем счетных множеств.

Определение (Конечное множество). Множество A называется *конечным множеством мощности k* , если $|A| = |\mathbb{N}_k|$, где $k \in \mathbb{N}$, а $\mathbb{N}_k = \{x \in \mathbb{N} | x < k\}$

Определение (Бесконечное множество). Множество *бесконечно*, если оно не является конечным.

Определение (Счётное множество). Множество A *счётно*, если $|A| = |\mathbb{N}|$.

Определение (Континуальное множество). Множество A *континуально*, если $|A| = |\mathbb{R}|$.

Определение (Не более чем счётное множество). Множество A *не более чем счётно*, если $|A| \leq |\mathbb{N}|$

Следствие (Описание не более чем счётных множеств). Множество не более чем счётно тогда и только тогда, когда оно конечно или счётно.

Доказательство. \Leftarrow : счётное множество не более чем счётно. Если A конечно, то $|A| = |\mathbb{N}_k| \leq |\mathbb{N}|$.

\Rightarrow : Пусть A не более чем счётно. Предположим, что оно бесконечно. Тогда в A есть счётное подмножество B . Получаем, что $|\mathbb{N}| - |B| \leq |A| \leq |\mathbb{N}|$. По теореме Кантора-Бернштейна $|A| = |\mathbb{N}|$. \square

22. Лемма о сохранении мощностей, теорема о мощности объединения (без доказательства).

Лемма (Лемма о сохранении мощностей).

(a) Если $|A| = |A_1|$ и $|B| = |B_1|$, то $|A \times B| = |A_1 \times B_1|$

(b) Если при этом $A \cap B = A_1 \cap B_1 = \emptyset$, то $|A \cup B| = |A_1 \cup B_1|$

Доказательство.

(a) Пусть даны биекции

$$f : A \xrightarrow[\text{на}]{1-1} A_1 \text{ и } g : B \xrightarrow[\text{на}]{1-1} B_1.$$

Построим $h : A \times B \xrightarrow[\text{на}]{1-1} A_1 \times B_1$ так: $h_1(\langle x; y \rangle) = \langle f(x), g(y) \rangle$.

Легко проверить, что h_1 - нужная биекция.

(b) Построим $h_2 : A \cup B \xrightarrow[\text{на}]{1-1} A_1 \cup B_1$ так: $h_2(x) = \begin{cases} f(x), & \text{если } x \in A \\ g(x), & \text{если } x \in B \end{cases}$

Условие $A \cap B = \emptyset$ гарантирует, что определение корректно. Вновь нетрудно доказать, что h_2 - биекция. Проверим в качестве примера, что h_2 инъективна. Пусть $h_2(x) = h_2(y)$. Если $x, y \in A$, то получаем $f(x) = f(y)$ и $x = y$. Если $x, y \in B$, рассуждения аналогичны. Если же $x \in A, y \in B$ (или наоборот), то $h_2(x) \in A_1$ и $h_2(y) \in B_1$, что невозможно в силу $A_1 \cap B_1 = \emptyset$.

□

Лемма (о мощности объединения). *Если хотя бы одно из множеств A, B бесконечно, то $|A \cup B| = \max\{|A|, |B|\}$.*

23. Теорема о мощности квадрата бесконечного множества (доказательства для счетного и континуального), теорема о мощности произведения (без доказательства).

Теорема (о мощности квадрата бесконечного множества). *Если A - бесконечное множество, то $|A \times A| = |A|$*

Доказательство.

- Докажем, что $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$
 Построим $f : \mathbb{N} \times \mathbb{N} \xrightarrow{1-1} \mathbb{N}$ и $g : \mathbb{N} \xrightarrow{1-1} \mathbb{N} \times \mathbb{N}$
 $f(x, y) = 2^x + 3^y$
 $g(x) = \langle x, 0 \rangle$
 Заметим, что обе функции инъективны, а значит $\begin{cases} |\mathbb{N} \times \mathbb{N}| \leq |\mathbb{N}| \\ |\mathbb{N} \times \mathbb{N}| \geq |\mathbb{N}| \end{cases}$
 тогда по теореме *Кантора-Бернштейна* получаем, что $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$

- Докажем, что $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$
 По аналогии с \mathbb{N} построим две инъекции:

- (a) $f : \mathbb{R} \times \mathbb{R} \xrightarrow{1-1} \mathbb{R}$
 Для построения данной функции докажем, равномощность \mathbb{R} и $(0, 1)$:
 Для этого построим биекцию $h : (0, 1) \xrightarrow[\text{на}]{1-1} \mathbb{R}$
 $h(x) = \text{ctg}(x * \pi)$ - функция биекция из-за $E(\text{ctg}x) = \mathbb{R}$
 Значит $|\mathbb{R}| = |(0, 1)|$
 Докажем, что $\mathbb{R} \times \mathbb{R}$ равномощно $(0, 1) \times (0, 1)$:
 Для этого построим $w : (0, 1) \times (0, 1) \xrightarrow[\text{на}]{1-1} \mathbb{R} \times \mathbb{R}$
 $w(x, y) = \langle h(x), h(y) \rangle$
 Значит $|\mathbb{R} \times \mathbb{R}| = |(0, 1) \times (0, 1)|$
 Построим инъекцию $u : (0, 1) \times (0, 1) \xrightarrow{1-1} (0, 1)$
 $u(x, y) = 0, \frac{10*a_1}{2} \frac{10*b_1}{2} \frac{10*a_2}{2} \frac{10*b_2}{2} \dots$
 Где $x = 0, a_1 a_2 \dots$, а $y = 0, b_1 b_2 \dots$
 Т.к в формуле присутствует умножение на 10, то на каждое число из $\frac{10*a_1}{2} \frac{10*b_1}{2} \frac{10*a_2}{2} \frac{10*b_2}{2} \dots$ отводится по две цифры, т.е $\frac{10*4}{2} = 20$, а $\frac{10*9}{2} = 45$, также $\frac{10*0}{2} = 00$
 u - инъекция, тогда $f(x, y) = h \circ u \circ w^{-1}(x, y)$
- (b) $g : \mathbb{R} \xrightarrow{1-1} \mathbb{R} \times \mathbb{R}$
 Построим $g(x) = \langle x, 0 \rangle$

Т.к f и g - инъекции, значит значит $\begin{cases} |\mathbb{R} \times \mathbb{R}| \leq |\mathbb{R}| \\ |\mathbb{R} \times \mathbb{R}| \geq |\mathbb{R}| \end{cases}$ тогда по теореме *Кантора-Бернштейна* получаем, что $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$

□

Теорема (о мощности произведения). *Если A, B - непустые множества и одно из них бесконечно, то:*

$$|A \times B| = \max\{|A|, |B|\}$$

24. Континуум-гипотеза, теорема Гёделя-Коэна (без доказательства), обобщенная континуумгипотеза.

Гипотеза (Континуум-гипотеза). Не существует множества A такого, что

$$|\mathbb{N}| < |A| < |\mathbb{R}|$$

Теорема (Теорема Гёделя-Коэна). *Если теория множеств ZFC непротиворечива, то континуум-гипотезу нельзя ни доказать, ни опровергнуть в рамках ZFC.*

Гипотеза (Обобщенная континуумгипотеза). Если множество B - бесконечно, то не существует множества A такого, что

$$|B| < |A| < |P(B)|$$

25. Ординалы, лемма об элементах ординала

Определение (Ординал). Ординалом называется транзитивное множество все элементы которого сравнимы относительно включения.

Определение (Транзитивное множество). Множество α называется транзитивным, если из $x \in \alpha$ и $y \in x$ следует, что $x \in \alpha$.

Лемма (Лемма об элементах ординала). *Если α - ординал и $\beta \in \alpha$, то β - ординал.*

Доказательство. Пусть $x, y \in \beta$. Тогда $x, y \in \alpha$. Следовательно, x и y равны или сравнимы относительно \in . Докажем, что β транзитивно. Пусть $y \in x \in \beta$. Тогда $x \in \alpha$ и $y \in \alpha$. Возможны три случая:

- (a) $\beta \in y$ Тогда получаем, что $\beta \in y \in x \in \beta$ - противоречие.
- (b) $\beta = y$ Получаем, что $\beta \in x \in \beta$ - противоречие.
- (c) $y \in \beta$. Следовательно, β - ординал.

□

26. Лемма о порядке на ординалах, теорема о свойствах ординалов.

Лемма (о порядке на ординалах). *Для любых ординалов α, β равносильно:*

- (a) $\alpha \leq \beta$;
- (b) $\alpha \subseteq \beta$.

Доказательство. (a \Rightarrow b): если $\alpha = \beta$, то $\alpha \subseteq \beta$. Если же $\alpha \in \beta$ и $x \in \alpha$, то $x \in \beta$

(b \Rightarrow a): если $\alpha = \beta$, то $\alpha \leq \beta$. Предположим, что $\alpha \subset \beta$. Тогда $\beta \setminus \alpha \neq \emptyset$. По аксиоме регулярности $\exists \gamma \in \beta \setminus \alpha$ т. ч. $\gamma \cap (\beta \setminus \alpha) \neq \emptyset$. Покажем, что $\alpha = \gamma$.

Если $x \in \gamma$, то $x \in \beta$ и $x \notin \beta \setminus \alpha$, следовательно, $x \in \alpha$.

Если $x \in \alpha$, то $x \in \beta$ и возможны три случая:

(a) $\gamma \in x$. Тогда $\gamma \in \alpha$, противоречие.

(b) $\gamma = x$. Вновь $\gamma \in \alpha$, противоречие.

(c) $x \in \gamma$.

Получаем, что $\alpha \in \beta$ и $\alpha \leq \beta$. □

Теорема (о свойствах ординалов). *Класс ординалов с порядком \leq обладает свойствами в.у.м. - для любых ординалов α, β, γ верно:*

(a) $\alpha \leq \alpha$;

(b) $\alpha \leq \beta$ и $\beta \leq \alpha \Rightarrow \alpha = \beta$;

(c) $\alpha \leq \beta$ и $\beta \leq \gamma \Rightarrow \alpha \leq \gamma$;

(d) $\alpha \leq \beta$ или $\beta \leq \alpha$;

(e) в любом непустом множестве ординалов есть минимальный элемент.

Доказательство. (a) очевидно.

(b) если $\alpha \subseteq \beta$ и $\beta \subseteq \alpha$, то $\alpha = \beta$.

(c) если $\alpha \subseteq \beta$ и $\beta \subseteq \gamma$, то $\alpha \subseteq \gamma$.

(d) пусть $\delta = \alpha \cap \beta$. Легко проверить, что δ является ординалом. По лемме о порядке на ординалах $\delta \leq \alpha$ и $\delta \leq \beta$. Если $\delta = \alpha$ или $\delta = \beta$, утверждение доказано. Допустим, что $\delta \neq \alpha, \beta$. Тогда $\delta \in \alpha, \delta \in \beta$ и $\delta \in \alpha \cap \beta = \delta$, противоречие.

(e) пусть S - непустое множество ординалов. По аксиоме регулярности $\exists \alpha \in S$, т.ч. $\alpha \cap S = \emptyset$. Если $\beta < \alpha$, то $\beta \in \alpha$ и $\beta \notin S$. Ясно, что α - минимальный элемент в S . □

27. Предложение о супремуме множества ординалов (без доказательства), теорема о связи в.у.м. и ординалов (без доказательства), предложение о принципе трансфинитной индукции (без доказательства).

Предложение (о супремуме множества ординалов). Пусть A - некоторое множество ординалов. Тогда $\cup A$ - ординал, являющийся супремумом множества A .

Теорема (о связи в.у.м. и ординалов). *Для любого в.у.м. существует единственный изоморфный ему ординал.*

Предложение (о трансфинитной индукции). Пусть $\Phi(x)$ - некоторое условие. Пусть для любого ординала α из того, что $\Phi(\beta)$ верно для всех $\beta < \alpha$, следует, что верно $\Phi(\alpha)$. Тогда $\Phi(\alpha)$ верно для всех ординалов α .

28. Сумма и произведение ординалов, кардинал, мощность множества.

Предложение (принцип трансфинитной рекурсии). Пусть существует условие, которое для каждого ординала α однозначно задаёт некоторое множество f_α в предположении, что при $\beta < \alpha$ множества f_β уже определены. Тогда каждому ординалу α действительно можно сопоставить множество f_α так, чтобы указанная связь между f_α и f_β , $\beta < \alpha$ выполнялась. При этом f_α определено однозначно.

Пример. На классе ординалов можно задать операции $+$ и \cdot так, что для любых ординалов α, β будет верно:

- (a) $\alpha + 0 = \alpha$ и $\alpha \cdot 0 = 0$;
- (b) $\alpha + (\beta + 1) = (\alpha + \beta) + 1$ и $\alpha \cdot (\beta + 1) = (\alpha \cdot \beta) + \alpha$;
- (c) $\alpha + \lambda = \sup\{\alpha + \beta \mid \beta < \lambda\}$ и $\alpha \cdot \lambda = \sup\{\alpha \cdot \beta \mid \beta < \lambda\}$, если λ - предельный ординал.

Доказательство. Зафиксируем γ и определим $\gamma + \alpha$ трансфинитной рекурсией по α . Предположим, что при $\beta < \alpha$ ординал $\gamma + \beta$ уже определён. Определим $\gamma + \alpha$, просто повторив формулировку для трёх случаев:

- (a) $\alpha = 0$, тогда $\gamma + \alpha = \gamma$;
- (b) $\alpha = \beta + 1$, тогда $\gamma + \alpha = (\gamma + \beta) + 1$;
- (c) α - предельный, тогда $\gamma + \alpha = \sup\{\gamma + \beta \mid \beta < \alpha\}$.

Произведение $\gamma \cdot \alpha$ определяется аналогично. □

Определение (Кардинал). Ординал μ называется *кардиналом*, если он не равномошен никакому строго меньшему ординалу.

Определение (Мощность множества). *Мощность* множества A - это единственный кардинал, равномошный A , т.е. $|\mu_A| = |A|$.

29. Алфавит ИВ, формула ИВ, подформула, представление формул ИВ.

30. Принцип математической индукции и возвратной индукции.

Определение (Принцип математической индукции). Если $\Delta(0)$ истинно и для всех n из истинности $\Delta(n)$ следует истинность $\Delta(n + 1)$, то $\Delta(n)$ истинно для всех n .

Определение (Возвратная индукция). Пусть для каждого n из того, что $\Delta(k)$ истинно при любом $k < n$, следует, что истинно $\Delta(n)$. Тогда $\Delta(n)$ истинно для всех n .

Доказательство. Оба принципа индукции легко вытекают из следующего факта: в любом непустом множестве натуральных чисел есть минимальный элемент. Покажем, как отсюда выводится возвратная индукция.

Допустим, что $\Delta(n)$ ложно при некотором n . Рассмотрим множество $A = \{n | \Delta(n) \text{ ложно}\}$. Оно не пусто, следовательно, в нём есть минимальный элемент n_0 . Тогда $\Delta(n_0)$ ложно, а если $n < n_0$, то $n \notin A$ и $\Delta(n)$ истинно. Получаем, что $\Delta(n_0)$ тоже истинно, противоречие. \square

31. Алфавит ИС, секвенция, аксиома, правило вывода, дерево вывода, доказуемость, пример вывода.
32. Семантика ИВ: означивание, значение формулы при означивании, выполнимые, опровержимые, тождественно истинные, тождественно ложные формулы, примеры.
33. Тождественно истинные секвенции, теорема о корректности ИС.

Определение (Тождественно истинные секвенции). Секвенция называется тождественно истинной, если она истинна при любом означивании переменных.

Теорема (о корректности ИС). *Любая доказуемая в ИС секвенция тождественно истинна.*

Доказательство. Пусть S - доказуемая секвенция, D - её дерево вывода. Индукцией по числу секвенций в D докажем, что S тождественно истинна.

Предположим, что в D одна секвенция. Тогда она совпадает с S и является аксиомой вида $\Phi \vdash \Phi$. Ясно, что она тождественно истинна.

Предположим, что в D n секвенций, $n > 1$, и для меньшего числа секвенций утверждение уже доказано. Дерево D имеет вид $\frac{D_1; \dots; D_k}{S}$, где D_i - деревья вывода секвенций S_i , а $\frac{S_1; \dots; S_k}{S}$ - правило вывода. По предположению индукции все S_i , $i \leq k$, тождественно истинны. Чтобы доказать, что S тождественно истинна, нужно перебрать все возможные правила вывода.

Рассмотрим случай, когда последнее правило в D имеет вид $\frac{\Gamma \vdash \Phi; \Gamma \vdash (\Phi \rightarrow \Psi)}{\Gamma \vdash \Psi}$.

Рассмотрим произвольное означивание и покажем, что секвенция $\Gamma \vdash \Psi$ истинна при этом означивании. Если одна из формул в Γ ложна, секвенция истинна. Предположим, все формулы в Γ истинны. Тогда истинны формулы Φ и $(\Phi \rightarrow \Psi)$. Ясно, что Ψ тоже истинна.

Остальные правила разбираются аналогично. \square

34. Допустимые правила вывода, примеры.

Предложение (о допустимых в ИС правилах). Следующие правила допустимы в ИС:

$$\begin{array}{c}
\frac{\Gamma \vdash \Phi; \Gamma, \Phi \vdash \Psi}{\Gamma \vdash \Psi} \text{ (сечение)}, \quad \frac{\Gamma, \Phi \vdash \Delta; \Gamma, \Psi \vdash \Delta}{\Gamma, (\Phi \vee \Psi) \vdash \Delta} \text{ (разбор случаев)}, \\
\frac{\Gamma \vdash (\Phi \rightarrow \Psi)}{\Gamma, \Phi \vdash \Psi} \text{ (удаление } \rightarrow \text{)}, \quad \frac{\Gamma, \Phi, \Psi \vdash \Delta}{\Gamma, (\Phi \& \Psi) \vdash \Delta} \text{ (соединение посылок)}, \\
\frac{\Gamma, (\Phi \& \Psi) \vdash \Delta}{\Gamma, \Phi, \Psi \vdash \Delta} \text{ (разделение посылок)}, \quad \frac{\Gamma, \neg \Phi \vdash \neg \Psi}{\Gamma, \Psi \vdash \Phi} \\
\frac{\Gamma, \Phi \vdash \Psi}{\Gamma, \neg \Psi \vdash \neg \Phi} \text{ (контрапозиция)}, \quad \frac{\Gamma, \Phi \vdash \neg \Psi}{\Gamma, \Psi \vdash \neg \Phi} \quad \frac{\Gamma, \neg \Phi \vdash \Psi}{\Gamma, \neg \Psi \vdash \Phi} \\
\frac{\Phi_1, \dots, \Phi_n \vdash \Psi}{\Delta_1, \dots, \Delta_m \vdash \Psi} \quad \text{и} \quad \frac{\Phi_1, \dots, \Phi_n \vdash}{\Delta_1, \dots, \Delta_m \vdash} \text{ (структурные), где} \\
\{\Phi_1, \dots, \Phi_n\} \subseteq \{\Delta_1, \dots, \Delta_m\}.
\end{array}$$

Докажем допустимость правила $\frac{\Gamma, \Phi \vdash \Psi}{\Gamma, \neg \Psi \vdash \neg \Phi}$, построив следующее дерево:

$$\begin{array}{c}
\frac{\Gamma, \Phi \vdash \Psi}{\Gamma, \Phi, \neg \Psi \vdash \Psi} \quad \frac{\neg \Psi \vdash \neg \Psi}{\vdots} \\
\hline
\Gamma, \neg \Psi, \Phi \vdash \Psi; \quad \Gamma, \neg \Psi, \Phi \vdash \neg \Psi \\
\hline
\Gamma, \neg \Psi, \Phi \vdash \\
\hline
\Gamma, \neg \Psi \vdash \neg \Phi.
\end{array}$$

Пример. Доказуема секвенция $\vdash \Phi \vee \neg \Phi$.

Построим допустимое дерево вывода, используя новые правила:

$$\begin{array}{c}
\frac{\neg \Phi \vdash \neg \Phi}{\neg \Phi \vdash \Phi \vee \neg \Phi} \quad \frac{\Phi \vdash \Phi}{\Phi \vdash \Phi \vee \neg \Phi} \\
\hline
\neg(\Phi \vee \neg \Phi) \vdash \Phi; \quad \neg(\Phi \vee \neg \Phi) \vdash \neg \Phi \\
\hline
\neg(\Phi \vee \neg \Phi) \vdash \\
\hline
\vdash \Phi \vee \neg \Phi.
\end{array}$$

35. Лемма об основных эквивалентностях, теорема о замене для ИВ.

Лемма (об основных эквивалентностях). Для любых формул Φ, Ψ, Φ', Ψ' и Δ верно:

- (a) $\Phi \equiv \Phi$;
- (b) $\Phi \equiv \Psi \Rightarrow \Psi \equiv \Phi$;
- (c) $\Phi \equiv \Psi, \Psi \equiv \Delta \Rightarrow \Phi \equiv \Delta$;
- (d) $\Phi \equiv \Phi' \Rightarrow \neg \Phi \equiv \neg \Phi'$;

(e) $\Phi \equiv \Phi', \Psi \equiv \Psi' \Rightarrow (\Phi' \circ \Psi) \equiv (\Phi' \circ \Psi')$, где $\circ \in \{ \&, \vee, \rightarrow \}$.

Доказательство. Пункты a), b) очевидны; c): предположим, что доказуемы секвенции $\Phi \vdash \Psi, \Psi \vdash \Phi, \Psi \vdash \Delta, \Delta \vdash \Psi$. Покажем доказуемость секвенции $\Phi \vdash \Delta$, построив допустимое дерево:

$$\frac{\Phi \vdash \Psi \quad \frac{\Phi \vdash \Delta}{\Phi, \Psi \vdash \Delta}}{\Phi \vdash \Delta}$$

Дерево для $\Delta \vdash \Phi$ строится симметрично. Далее будем указывать только деревья.

d) :

$$\frac{\Phi' \vdash \Phi}{\neg \Phi \vdash \neg \Phi'}$$

e) : построим три дерева для случаев $\circ = \rightarrow, \circ = \&$ и $\circ = \vee$. Далее мы иногда будем пропускать структурные правила, соединяя несколько структурных правил с одним основным или допустимым в один переход дерева.

$$\frac{\frac{\Phi' \vdash \Phi; \quad (\Phi \rightarrow \Psi) \vdash (\Phi \rightarrow \Psi)}{(\Phi \rightarrow \Psi), \Phi' \vdash \Psi; \quad} \quad \frac{\Psi \vdash \Psi'}{(\Phi \rightarrow \Psi), \Phi', \Psi \vdash \Psi'}}{(\Phi \rightarrow \Psi), \Phi' \vdash \Psi'}{(\Phi \rightarrow \Psi) \vdash (\Phi' \rightarrow \Psi')}$$

$$\frac{\frac{\frac{\Phi \vdash \Phi'}{\Phi, \Psi \vdash \Phi'}}{(\Phi \& \Psi) \vdash \Phi'; \quad} \quad \frac{\frac{\Psi \vdash \Psi'}{\Phi, \Psi \vdash \Psi'}}{(\Phi \& \Psi) \vdash \Psi'}}{(\Phi \& \Psi) \vdash (\Phi' \& \Psi')} \quad \frac{\frac{\Phi \vdash \Phi'}{\Phi \vdash (\Phi' \vee \Psi'); \quad} \quad \frac{\Psi \vdash \Psi'}{\Psi \vdash (\Phi' \vee \Psi')}}{(\Phi \vee \Psi) \vdash (\Phi' \vee \Psi')}$$

□

Теорема (о замене для ИВ). Пусть Ψ - подформула формулы Φ . Обозначим через Φ' результат замены Ψ на Ψ' . Если $\Psi \equiv \Psi'$, то и $\Phi \equiv \Phi'$.

Доказательство. Индукцией по $|\Phi|$ докажем, что Φ' - формула, эквивалентная Φ . Если $\Phi = \Psi$, то $\Phi' = \Psi'$ и $\Phi \equiv \Phi'$. Поэтому будем рассматривать только случай $\Phi \neq \Psi$.

Пусть $|\Phi| = 1$. Тогда $\Phi = \Psi$, и этот случай уже рассмотрен.

Пусть $|\Phi| > 1$, и для формул меньшей длины утверждение уже доказано. Если $\Phi = \neg \Phi_1$, то Ψ - подформула Φ_1 , и по предположению индукции $\Phi_1 \equiv \Phi'_1$. Тогда $\Phi = \neg \Phi_1 \equiv \neg \Phi'_1 = \Phi'$.

Если $\Phi = (\Phi_1 \circ \Phi_2)$, где $\circ \in \{ \&, \vee, \rightarrow \}$, то Ψ - подформула Φ_1 или Φ_2 .

Предположим, что Ψ - подформула Φ_1 . По предположению индукции $\Phi_1 \equiv \Phi'_1$, отсюда $\Phi = (\Phi_1 \circ \Phi_2) \equiv (\Phi'_1 \circ \Phi_2) = \Phi'$. \square

36. Д.н.ф., к.н.ф., теорема о приведении к д.н.ф. и к.н.ф.

37. Предложение о тождественно истинных к.н.ф.

Предложение (о тождественно истинных к.н.ф.).

К.н.ф. Φ тождественно истинна тогда и только тогда, когда каждая её элементарная дизъюнкция содержит компоненты P и $\neg P$ для некоторой переменной P .

Пусть Φ — к.н.ф. и $\Phi = (\Psi_1 \& \dots \& \Psi_n)$, где Ψ_i — элементарные дизъюнкции. Если фиксировано означивание γ , то

$$\Phi[\gamma] = \mathbf{и} \Leftrightarrow \forall i \leq n \quad \Psi_i[\gamma] = \mathbf{и}.$$

Это почти очевидно и формально может быть доказано индукцией по n . Если, в свою очередь, $\Psi_i = (\Delta_1 \vee \dots \vee \Delta_k)$, то

$$\Psi_i[\gamma] = \mathbf{и} \Leftrightarrow \exists j \leq k \quad \Delta_j[\gamma] = \mathbf{и}.$$

Переход (\Leftarrow) очевиден: если $\Psi_i = (\dots \vee P \vee \dots \vee \neg P \vee \dots)$, то Ψ_i истинна при любом означивании. Получаем, что Φ тождественно истинна.

(\Rightarrow): если Φ тождественно истинна, то все Ψ_i , $i \leq n$, тоже тождественно истинны. Зафиксируем $i \leq n$ и покажем, что Ψ_i содержит P и $\neg P$. Допустим, что это не так. Пусть в Ψ_i входят переменные P_1, \dots, P_m . Зададим их означивание: если $j \leq m$ и P_j входит в Ψ_i без отрицания, положим $P_j = \mathbf{л}$, а если входит с отрицанием, то $P_j = \mathbf{и}$. Это можно сделать, так как мы предположили, что P_j не может входить одновременно с отрицанием и без него. Ясно, что при этом Ψ_i станет ложна, $\uparrow \downarrow$.

38. Теорема о полноте ИС.

39. Совершенные нормальные формы, теорема о совершенных нормальных формах.

40. Гильбертовское исчисление высказываний: аксиоматика, выводимость, примеры выводов.

41. Теорема о дедукции.

42. Связь гильбертовского и секвенциального исчисления.