Содержание

1 Множества

1.1 Вопросы на удос

1.1.1 Включение и равенство множеств. Основные способы задания множеств

Включение и равенство множеств

Лемма о свойствах включения

1. $A \subseteq A$
2. $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$
3. $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$

Лемма о свойствах равенства

1. $A = A$
2. $A = B \wedge B = C \Rightarrow A = C$
3. $A = B \Rightarrow B = A$

Основные способы задания множеств

1. Множество можно задать, назвав все его элементы, когда число этих элементов конечно и все они уже определены.
2. Другим способом задания множества является выделение всех элементов какого-нибудь уже определённого множества A, обладающих некоторым точно определённы свойством φ
3. Ещё один способ получить новое множество B из данного множества A - рассмотреть множество всех подмножеств множества A. Такое множество B обозначают выражением $\mathcal{P}(A)$
4. Располагая каким-нибудь множеством X, чьи элементы, как мы помним, тоже обязаны быть множествами, можно рассмотреть его объединение, обозначаемое $\cup X$ и состоящее из всевозможных элементов множеств, принадлежащих X.

1.1.2 Операции алгебры множеств и их основные свойства

Эквивалентные свойства множества, включённого в другое множество Для любых множеств A и B равносильны утверждения:

1. $A \subseteq B$
2. $A \cap B = A$
3. $A \cup B = B$

Доказательство:

Пусть $A \subseteq B$. Очевидно, что $A \cap B \subseteq A$. Покажем, что $A \subseteq A \cap B$. Предположим для произвольного x, что $x \in A$. Тогда $x \in B$ в силу $A \subseteq B$. Следовательно, $x \in A \cap B$. Значит $A \cap B = A$.

Пусть теперь $A \cap B = A$. Очевидно, что $B \subseteq A \cup B$. Остаётся проверить $A \cup B \subseteq B$. Если $x \in A \cup B$, то $x \in A \vee x \in B$. В первом случае, в силу $A = A \cap B$, верно $x \in A \cap B$, откуда $x \in B$. Тем более, $x \in B$ во втором случае.

Пусть, наконец, $A \cup B = B$. Очевидно, что $A \subseteq A \cup B$ и, по предположению, $A \cup B \subseteq B$, откуда $A \subseteq B$.

Основные тождества алгебры множеств Для любых множеств A, B, C и любого включающего их универсума U верно:

1. $A \cap B = B \cap A;\ A \cup B = B \cup A$
2. $(A \cap B) \cap C = A \cap (B \cap C);\ (A \cup B) \cup C = A \cup (B \cup C)$
3. $A \cap A = A;\ A \cup A = A$
4. $A \cap (A \cup B) = A;\ A \cup (A \cap B) = A$
5. $\overline{\overline{A}} = A$
6. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C);\ A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
7. $\overline{A \cap B} = \overline{A} \cup \overline{B};\ \overline{A \cup B} = \overline{A} \cap \overline{B}$
8. $A \cap \varnothing = \varnothing;\ A \cup \varnothing = A;\ A \cap U = A;\ A \cup U = U;\ \overline{\varnothing} = U;\ \overline{U} = \varnothing$
9. $A \cap \overline{A} = \varnothing;\ A \cup \overline{A} = U$

Доказательство очевидное.

1.1.3 Бинарные отношения. Композиция и обращение отношений. Ассоциативность композиции. Обращение композиции. Образ и прообраз множества под действием отношения.

Бинарные отношения Множество R называется бинарным отношением, если каждый его элемент является упорядоченной парой множеств.

Композиция и обращение отношений

Композиция Для любых отношений P и Q определена композиция отношений P и Q:

$$Q \circ P = \{(a, c) \in \text{dom } P \times \text{rng } Q \mid \exists b((a, b) \in P \wedge (b, c) \in Q)\}$$

Обращение Пусть R - бинарное отношение. Обратным отношением к R называется отношение

$$R^{-1} = \{(b, a) \in \text{rng } R \times \text{dom } R \mid (a, b) \in R\}$$

Ассоциативность композиции Пусть P, Q, R суть бинарные отношения. Тогда:

$$R \circ (Q \circ P) = (R \circ Q) \circ P$$

Доказательство:
Для произвольной пары (a, d) имеем
$(a, d) \in R \circ (Q \circ P) \Leftrightarrow \exists c(a(Q \circ P)c \wedge cRd) \Leftrightarrow \exists c \exists b(aPb \wedge bQc \wedge cRd) \Leftrightarrow \exists b(aPb \wedge \exists C(bQc \wedge cRd)) \Leftrightarrow \exists b(aPb \wedge b(R \circ Q)d) \Leftrightarrow (a, d) \in (R \circ Q) \circ P$

Обращение композиции Пусть P и Q - бинарные отношения. Тогда $(Q \circ P)^{-1} = P^{-1} \circ Q^{-1}$
Доказательство:
Для произвольной пары (a, c) получаем
$(a, c) \in (Q \circ P)^{-1} \Leftrightarrow (c, a) \in Q \circ P \Leftrightarrow \exists b(cPb \wedge bQa) \Leftrightarrow \exists b((b, c) \in P^{-1} \wedge (a, b) \in Q^{-1}) \Leftrightarrow (a, c) \in P^{-1} \circ Q^{-1}$.

Образ и прообраз множества под действием отношения Пусть R - бинарное отношение и X - некоторое множество. Мы называем образом под действием отношения R множества X множество

$$R[X] = \{b \in \text{rng } R \mid \exists a \in X \; aRb\}$$

Множество $R^{-1}[X]$ называют прообразом множества X под действием R

1.1.4 Функциональные, инъективные, тотальные и сюръективные отношения. Композиция и обращение таких отношений.

Функциональные, инъективные, тотальные и сюръективные отношения Бинарное отношение R называется:

1. Функциональным, если $\forall x \forall y \forall z((xRy) \wedge (xRz) \Rightarrow y = z)$
2. Инъективным, если $\forall x \forall y \forall z((xRy) \wedge (zRy) \Rightarrow x = z)$
3. Тотальным для множества Z, если $\forall x \in Z \; \exists y \; (x, y) \in R$
4. Сюръективным для множества Z, если $\forall y \in Z \; \exists x \; (x, y) \in R$

Композиция таких отношений Пусть $Q \subseteq A \times B \wedge R \subseteq B \times C$. Тогда:

1. Если Q и R функциональны, то функционально $R \circ Q$;
2. Если Q и R инъективны, то инъективно $R \circ Q$;
3. Если Q и R тотальны, то тотально $R \circ Q$;
4. Если Q и R сюръективны, то сюръективно $R \circ Q$;

Обращение таких отношений

1. R функционально $\Leftrightarrow R^{-1}$ инъективно.
2. R тотально для $Z \Leftrightarrow R^{-1}$ сюръективно для Z.

Доказывается непосредственной проверкой.

1.1.5 Частичные функции. Значение частичной функции. Область опеределения и область значений. Критерий равенства частичных функций. Ограничение (инъективной, тотальной) частичной функцию. (Тотальные) функции

Частичные функции Функциональное отношение $f \subseteq A \times B$ называется частичной функцией на множестве A во множество B. В таком случае пишем $f : A \xrightarrow{p} B$.

Значение частичной функции Элемент (т.е. множество) b назовём значением частичной функции $f : A \xrightarrow{p} B$ на элементе a, если afb. Функциональность гарантирует, что для каждого a существует не более одного такого значения b, причём $b \in B$. Значение f на элементе a обозначается $f(a)$.

Критерий равенства частичных функций Пусть $f : A \xrightarrow{p} B$ и $g : C \xrightarrow{p} D$. Тогда:

$$f = g \Leftrightarrow \forall x f(x) \simeq g(x)$$

Доказательство:

Пусть $f = g$. Тогда, очевидно, $\mathrm{dom}\ f = \mathrm{dom}\ g$. Рассмотрим произвольное множество x. Если $x \notin \mathrm{dom}\ f$, то $x \notin \mathrm{dom}\ g \Rightarrow f(x) \simeq g(x)$. Если же $x \in \mathrm{dom}\ f$, то $x \in \mathrm{dom}\ g$. В таком случае существуют $y \in B, z \in D$, т.ч. $(x, y) \in f, (x, z) \in g$. Из $f = g$ следует $(x, y), (x, z) \in f \Rightarrow y = z$ по функциональности. Итак, $f(x) = y = z = g(x) \Rightarrow f(x) \simeq g(x)$.

Обратно, пусть $f(x) \simeq g(x)$ для всех x. Предположим, что $(x, y) \in f$. Тогда $x \in \mathrm{dom}\ f, f(x) = y$. По условию имеем также $x \in \mathrm{dom}\ g(x) = f(x) = y$. Значит $(x, y) \in g$. Обратное включение аналогично.

Ограничение (инъективной, тотальной) частичной функции Пусть $f : A \xrightarrow{p} B$. Тогда:

1. $f \restriction X : X \xrightarrow{p} B$
2. Если f инъективно, то инъективно и $f \restriction X$
3. Если f тотальна для A и $X \subset A$, то $f \restriction X$ тотальна для X.

1.1.6 Инъекции, сюръекции и биекции. Критерий биективности отношения

Инъекции, сюръекции и биекции Если функция $f : A \to B$ инъективна, она называется инъекцией из A в B. Если сюръективна, - называется сюръекцией из A в B. Наконец, если f инъективна и сюръективна, она называется биекцией из A в B.

Критерий биективности отношения Отношение $R \subseteq A \times B$ является биекцией из A в B тогда и только тогда, когда:

$$R^{-1} \circ R = \mathrm{id}_A \wedge R \circ R^{-1} = \mathrm{id}_B$$

Доказательство.

Пусть $R : A \to B$ является биекцией. Допустим, что $(x, y) \in R^{-1} \circ R$. Тогда найдётся $z \in B$, т.ч. xRz и $zR^{-1}y$, т.е. xRz и yRZ. По инъективности R имеем $x = y$, т.е. $(x, y) \in \mathrm{id}_A$. Обратно, пусть $(x, x) \in \mathrm{id}_A$. По тотальности R найдётся $z \in B$, т.ч. xRz, и, следовательно, $zR^{-1}x$. Значит, $(x, x) \in R^{-1} \circ R$. Второе равенство устанавливается аналогично с использованием функциональности и сюръективности R.

Предположим теперь, что наши равенства выполнены. Тогда для любого $z \in B$ имеем $(z, z) \in R \circ R^{-1}$, т.е. найдётся $x \in A$, т.ч. xRz. Значит, R сюръективно. Пусть xRz и xRw. Тогда также $zR^{-1}x$, откуда $(z, w) \in R \circ R^{-1} = \mathrm{id}_B$. Следовательно, $z = w$ и R функционально. Инъективность и тотальность R извлекаются из первого равенства аналогичным образом.

1.1.7 Аксиома выбора. Существование правой обратной у каждой сюръекции

Аксиома выбора Пусть множество A таково, что $\varnothing \notin A$. Тогда существует функция $f : A \to \cup A$, т.ч. $f(a) \in a$ для всех $a \in A$.

Существование правой обратной у каждой сюръекции Пусть $f : A \to B$. Правая обратная $g : B \to A$ (т.ч. $f \circ g = \mathrm{id}_B$) функции f существует тогда и только тогда, когда f есть сюръекция.

Доказательство.

Пусть правая обратная g существует, т.е. $f \circ g = \mathrm{id}_B$. Для любого $b \in B$ имеем $(b, b) \in f \circ g$, значит найдётся $a \in A$ для некоторого $(b, a) \in g, (a, b) \in f$. Последнее означает сюръективность f.

Допустим теперь, что f сюръективна. Ясно, что тогда множества $f^{-1}[\{b\}]$ непусты для всех $b \in B$. Определим функцию $g : B \to A$, полагая

$$g(b) = \text{ какой-нибудь элемент множества } f^{-1}[\{b\}]$$

при всех $b \in B$. Поскольку $g(b) \in f^{-1}[\{b\}]$, имеем $f(g(b)) = b$ для всех $b \in B$, т.е. $f \circ g = \mathrm{id}_B$.

1.1.8 Индексированное семейство множеств. Его объединение и декартово произведение. Непустота декартова произведения.

Индексированное семейство множеств Пусть I - некоторое множество индексов, а U - ещё какое-либо множество. Назовём индексированным семейством произвольное отображение $F : I \to U$. Говорят, что A принадлежит семейству F, если $A \in F[I]$, и что A есть i-й элемент семейства F, если $i \in I$ и $A = F(i)$.

Обыкновенно пишут A_i вместо $F(i)$ и $\{A_i\}_{i \in I}$ вместо $F[I]$. Более того, символом $\{A_i\}_{i \in I}$ обозначают всё семейство, так что отображение $F : i \mapsto A_i$ лишь подразумевается.

Его объединение и декартово произведение Под объединением $\bigcup\limits_{i\in I} A_i$ индексированного семейства множеств $\{A_i\}_{i\in I}$ мы понимаем множество $\cup F[I]$, а под пересечением $\bigcap\limits_{i\in I} A_i$ соответственно множество $\cap F[I]$.

Декартовым произведением индексированного семейства $\{A_i\}_{i\in I}$ называют

$$\prod_{i\in I} A_i = \{f \in (\bigcup_{i\in I} A_i)^I \mid \forall i \in I\ f(i) \in A_i\}$$

Непустота декартова произведения Элементы $f \in \prod\limits_{i\in I} A_i$ тесно связаны с функциями выбора. Именно, композиции $\xi \circ F$, где ξ суть всевозможные функции выбора для множества $F[I] = \{A_i\}_{i\in I}$, принадлежат множеству $\prod\limits_{i\in I} A_i$. В частности, если $A_i \neq \varnothing$ при всех $i \in I$, из аксиомы выбора следует $\prod\limits_{i\in I} A_i \neq \varnothing$.

1.1.9 Свойства (ир)рефлексивности, (анти)симметричности и транзитивности отношения. Представление этих свойств в терминах операций над множествами.

Свойства (ир)рефлексивности, (анти)симметричности и транзитивности отношения. Бинарное отношение R называется:

1. Рефлексивным для множества Z, если $\forall x \in Z\ (x, x) \in R$
2. Иррефлексивным, если $\forall x\ (x, x) \notin R$
3. Симметричным, если $\forall x\, \forall y\ (xRy \Rightarrow yRx)$
4. Антисимметричным, если $\forall x\, \forall y\ ((xRy \wedge yRx) \Rightarrow x = y)$
5. Транзитивным, если $\forall x, \forall y, \forall z\ ((xRy \wedge yRz) \Rightarrow xRz)$

Представление этих свойств в терминах операций над отношениями Отношение $R \subseteq A^2$

1. Рефлексивно $\Leftrightarrow \mathrm{id}_A \subseteq R$
2. Иррефлексивно $\Leftrightarrow \mathrm{id}_A \cap R = \varnothing$
3. Симметрично $\Leftrightarrow R \subseteq R^{-1} \Leftrightarrow R = R^{-1} \Leftrightarrow R^{-1} \subseteq R$
4. Антисимметрично $\Leftrightarrow R \cap R^{-1} \subseteq \mathrm{id}_A$
5. Транзитивно $\Leftrightarrow R \circ R \subseteq R$

Доказательство.

Проверим три последних утверждения. Если R симметрично и $(x, y) \in R$, то, по определению, $(y, x) \in R$, откуда $(x, y) \in R^{-1}$. Поэтому $R \subseteq R^{-1}$. Но отсюда имеем $R^{-1} \subseteq (R^{-1})^{-1}$, а значит, и $R = R^{-1}$, чего, в свою очередь, достаточно для симметричности.

Условие $R \cap R^{-1} \subseteq \mathrm{id}_A$ означает, что для любых x и y из $xRy \wedge xR^{-1}y$ следует $x\mathrm{id}_A y$, или, равносильно, из $xRy \wedge yRx$ следует $x = y$. Это и есть условие антисимметричности

Пусть R транзитивно и $(x, y) \in R \circ R$. Тогда найдётся z, т.ч. $(x, z) \in R \wedge (z, y) \in R$. По транзитивности $(x, y) \in R$. Обратно, пусть $R \circ R \subseteq R, xRz, zRy$. Но тогда $(x, y) \in R \circ R, xRy$. Следовательно, R транзитивно.

1.1.10 Частично упорядоченное множество. Понятия минимального и максимального, наибольшего и наименьшего элемента (в т.ч. в подмножестве); понятия верхней (нижней) грани и супремума (инфимума) подмножества

Частично упорядоченное множество

Строгий частичный порядок Отношение R на каком-либо множестве называется строгим частичным порядком (или просто строгим порядком) на этом множестве, если R иррефлексивно и транзитивно.

Нестрогий частичный порядок Отношение R на каком-либо множестве называется нестрогим частичным порядком (или просто нестрогим порядком) на этом множестве, если R рефлексивно, транзитивно и антисимметрично.

Ч.у.м. Если R есть строгий или нестрогий частичный порядок на множестве A, пара (A, R) называется частично упорядоченным множеством (ч.у.м.). Если ясно, какой порядок рассматривается, частично упорядоченным множеством называют и само A.

Понятие минимального и максимального, наибольшего и наименьшего элемента (в т.ч. в подмножестве)

Максимальный элемент Если на множестве A задан строгий частичный порядок P, элемент $x \in A$ называется (P-)максимальным, если

$$\forall y \in A \neg xPy$$

Минимальный элемент Если на множестве A задан строгий частичный порядок P, элемент $x \in A$ называется (P-)минимальным, если

$$\forall y \in A \neg yPx$$

На подмножестве Пусть дано ч.у.м. $(A, <)$. Понятие максимального и минимального элемента естественно распространить на любое подмножество $B \subseteq A$, положив $\max_< B = \{x \in B \mid \forall y \in B\ x \not< y\}$, и аналогично определяя $\min_< B$.

Наибольший и наменьший элемент Элемент $x \in B$ называется наибольшим в подмножестве B ч.у.м. $(A, <)$, если $\forall y \in B\ y \leqslant x$, и наименьшим, если $\forall y \in B\ x \leqslant y$.

Понятия верхней (нижней) грани и супремума (инфимума) подмножества

Понятия верхней (нижней) грани Пусть $(A, <)$ ч.у.м. и $B \subseteq A$. Элемент $x \in A$ назовём верхней гранью множества B, если $\forall y \in B\ y \leqslant x$. Аналогично определяются нижние грани.

Понятия супремума (инфимума) подмножества Мы говорим, что $x \in A$ есть точная верхняя грань (или супремум) множества B, если x есть наименьшая верхняя грань множества B. Аналогично определяется точная нижняя грань (или инфимум) множества B - его наибольшая нижняя грань.

1.1.11 Цепи и антицепи; решётки; линейные порядки; примеры. Изоморфизм ч.у.м. (примеры)

Цепи и антицепи

Определение Пусть $(A, <)$ ч.у.м. Множество $C \subseteq A$ называется цепью в A, если

$$\forall x, y \in C\ x \leqslant y \vee y \leqslant x$$

Напротив, множество $D \subseteq A$ называется антицепью, если никакие два его (различные) элемента несравнимы.

Примеры В ч.у.м. $(\mathbb{N}, |)$ множество $\{2^n \mid n \in \mathbb{N}\}$ образует цепь, а множество простых чисел - антицепь.

Решётки

Определение Решётки - такие ч.у.м. $(A, <)$, где для любых $x, y \in A$ существуют $\sup\{x, y\}$ и $\inf\{x, y\}$. Ч.у.м. $(A, <)$ называется полной решёткой, если для всех $X \subseteq A$ существуют $\sup A$ и $\inf A$.

Примеры Для любого множества A ч.у.м. $(\mathcal{P}(A), \subseteq)$ есть полная решётка.
Ч.у.м. $(\mathbb{N} \setminus \{0\}, |)$ является решёткой, но не полной решёткой.

Линейные порядки

Определение Порядок $<$ на множестве A называется линейным, если любые два элемента A сравнимы.

Примеры Естественные порядки на множествах $\mathbb{N}, \mathbb{Q}, \mathbb{Z}, \mathbb{R}$ являются линейными, а порядки $\subseteq$ на $\mathcal{P}(A)$ (если в A есть хотя бы два различных элемента) и $|$ на $\mathbb{N}$ не являются.

Изоморфизм ч.у.м.

Определение Структуры $\mathcal{A} = (A, R), \mathcal{B} = (B, Q)$ изоморфны, если существует функция $\alpha : A \to B$, т.ч. $A \overset{\alpha}{\sim} B$ и

$$xRy \Leftrightarrow \alpha(x)R\alpha(y)$$

Примеры $(\mathbb{Z},\ <) \cong (\mathbb{Z},\ >)$, но $(\mathbb{Z},\ <) \ncong (\mathbb{R},\ <)$.

1.1.12 Отношение эквивалентности. Классы эквивалентности и их свойства. Фактор-множество и разбиение множества (определения, формулировки и примеры)

Отношение эквивалентности Отношение $R \subset A^2$ называется отношением эквивалентности (или просто эквивалентностью) на A, если R рефлексивно, симметрично и транзитивно.

Классы эквивалентности и их свойства

Определение Пусть E есть эквивалентность на множестве A и $x \in A$. Назовём множество

$$[x]_E = \{z \in A \mid xEz\}$$

классом эквивалентности элемента x по отношению E.

Свойства Пусть E - эквивалентность на множестве A. Тогда для произвольных $x, y \in A$ верно:

1. $x \in [x]_E$
2. $[x]_E \cap [y]_E \neq \varnothing \Leftrightarrow xEy \Leftrightarrow [x]_E = [y]_E$

Доказательство.
Первое утверждение следует из xEx. Для второго допустим, что $z \in [x]_E \cap [y]_E$. Тогда $xEz, zEy \Rightarrow xEy$. В свою очередь, пусть $xEy, z \in [x]_E$. Вновь применяя симметричность и транзитивность E, получаем yEz. Итак, $[x]_E \subseteq [y]_E$. Наконец, предположим, что $[x]_E = [y]_E$. Но тогда, по первому утверждению, $x \in [x]_E \cap [y]_E \neq \varnothing$.

Фактор-множество и разбиение множества

Определение фактор-множества Множество

$$A/E = \{\sigma \in \mathcal{P}(A) \mid \exists x \in A\, [x]_E = \sigma\} = \{[x]_E \mid x \in A\}$$

называется фактор-множеством множества A по отношению E.

Примеры фактор-множеств Множество A/A^2 есть просто $\{A\}$, множество A/id_A есть множество всех одноэлементных подмножеств A. Следовательно $A/\mathrm{id}_A \sim A$.

Определение разбиение множества Назовём множество $\Sigma \subseteq \mathcal{P}(A)$ разбиением множества A, если:

$$\varnothing \notin \Sigma,\ \cup\Sigma = A, \forall \sigma, \tau \in \Sigma\, (\sigma \cap \tau \neq \varnothing \Rightarrow \sigma = \tau)$$

Пример разбиения множества Любое фактор-множество A/E является разбиением A. $\{\mathbb{R}_-, \{0\}, \mathbb{R}_+\}$ есть разбиение $\mathbb{R}$.

1.1.13 Натуральные числа и множества $\underline{n}$. Определение конечного множества. Подмножества и характеристические функции; $\mathcal{P}(A) \sim \underline{2}^A$. Примеры рассуждений с характеристическими функциями.

Натуральные числа и множества $\underline{n}$. Натуральные числа, неформально говоря, выражающие "конечные количества позволяют дать строгое определение конечного множества. При всех $n \in \mathbb{N}$ положим

$$\underline{n} = \{k \in \mathbb{N} \mid k < n\}$$

В частности, $\underline{0} = \varnothing, \underline{n+1} = \underline{n} \cup \{n\}$

Определение конечного множества Множество A конечное, если $A \sim \underline{n}$ для некоторого $n \in \mathbb{N}$. В противном случае множество называется бесконечным.

Подмножества и характеристические функции $\chi_B : A \to \underline{2}$ есть характеристическая функция (или индикатор) подмножества B множества A, определяемая так:

$$\chi_B(x) = \begin{cases} 1, & x \in B \\ 0, & x \notin B \end{cases}$$

$\mathcal{P}(A) \sim \underline{2}^A$ Для любого множества A имеет место $\mathcal{P}(A) \sim \underline{2}^A$.

Доказательство.

В самом деле, рассмотрим отображение $\varphi : \mathcal{P}(A) \to \underline{2}^A$, т.ч. $\varphi(B) = \chi_B$ при всех $B \subseteq A$.

Проверим инъективность φ. Пусть $B \neq C$. Без ограничения общности, существует $x \in B \setminus C$. Тогда $\chi_B(x) = 1 \neq 0 = \chi_C(x)$. Значит $\varphi(B) \neq \varphi(C)$. Проверим сюръективность. Пусть $f : A \to \underline{2}$. Положим $B = f^{-1}[\{1\}]$. Очевидно, что $f = \chi_B = \varphi(B)$. Итак, $\mathcal{P}(A) \sim \underline{2}^A$.

Примеры рассуждений с характеристическими функциями.

Упражнение 1 Докажите, что для любых $B, C \in \mathcal{P}(A), x \in A$ имеют место:

$$\chi_{B \cup C}(x) = \chi_B(x) \cdot \chi_C(x)$$

$$\chi_{B \cap C}(x) = \chi_B(x) + \chi_C(x) - \chi_B(x) \cdot \chi_C(x)$$

$$\chi_{\overline{B}}(x) = 1 - \chi_B(x)$$

а $B \subseteq C$ равносильно тому, что $\chi_B(x) \leqslant \chi_C(x)$ для всех $x \in A$.

Упражнение 2 Пусть $A = B \cup C$. Тогда с помощью характеристических функций можно доказать, что $\overline{B} \cap \overline{C} = \overline{B \cup C}$. Действительно, для любого $x \in A$ имеем

$$\chi_{\overline{B} \cap \overline{C}}(x) = (1 - \chi_B(x))(1 - \chi_C(x)) = 1 - (\chi_B(x) + \chi_C(x) - \chi_B(x)\chi_C(x)) = \chi_{\overline{B \cup C}}(x)$$

Упражнение 3 Докажем, что из $B \cap C = B \cup C$ следует $B = C$. Из условия для всех $x \in A$ получаем

$$0 = \chi_{B \cup C}(x) - \chi_{B \cap C}(x) = \chi_B(x) + \chi_C(x) - 2\chi_B(x)\chi_C(x) =$$

$$\chi_B^2(x) + \chi_C^2(x) - 2\chi_B(x)\chi_C(x) = (\chi_B(x) - \chi_C(x))^2$$

Отсюда $\chi_B(x) = \chi_C(x)$ для всех $x \in A$, а значит $B = C$.

1.1.14 Мощности множеств ...

Про $\mathbb{N}^2$ Убедимся, что $\mathbb{N}^2 \sim \mathbb{N}$.

Итак, положим $\forall (m,n) \in \mathbb{N}^2 : \ f(m,n) = 2^m(2n+1) - 1$. Если $f(m,n) = f(m',n')$, то $2^m(2n+1) = 2^{m'}(2n'+1)$. Допустим, что $m \neq m'$ и, без ограничения общности, $m < m'$. Тогда $2n+1 = 2^{m'-m}(2n'+1)$, причём второе число чётно, а первое нечётно. Противоречие показывает, что $m = m'$. Но тогда $2n+1 = 2n'+1$, откуда $n = n'$. Итак, f - инъекция. Установим сюръективность. Пусть некоторое положительное натуральное число не имеет вида $2^m(2n+1)$. Тогда найдётся наименьшее такое число k. Это число чётно (иначе оно имело бы вид $2^0(2n+1)$). Следовательно, $k = 2k'$. Однако $k' < k$, а значит $k' = 2^{m'}(2n'+1)$ для некоторых $m', n' \in \mathbb{N}$. Но тогда $k = 2^{m'+1}(2n'+1)$. Противоречие. Итак, каждое положительное натуральное число вид $f(m,n)+1$. Очевидно, тогда f - сюръекция из $\mathbb{N}^2$ в $\mathbb{N}$.

Континуум-гипотеза Из анализа известно, что $\mathbb{R} \sim \mathcal{P}(\mathbb{N})$. Множество $\mathcal{P}(\mathbb{N})$ называется континуум, поскольку равномощно непрерывной совокупности точек прямой. Как видим, $\mathbb{N} \not\sim \mathbb{R}$, т.е. невозможно взаимно однозначное соответствие между точками прямой и натуральным ряда.

Континуум-гипотеза утверждает, что если $\mathbb{N} \lesssim X \lesssim \mathcal{P}(\mathbb{N})$, то $X \sim \mathbb{N}$ или $X \sim \mathcal{P}(\mathbb{N})$

Про $\mathbb{R}^2, \mathbb{N}^{\mathbb{N}}$ и $\mathbb{R}^{\mathbb{N}}$ Как мы знаем, $\mathbb{R} \sim \mathcal{P}(\mathbb{N})$. Поэтому $\mathbb{R} \sim \underline{2}^{\mathbb{N}}$, откуда

$$\mathbb{R} \sim \mathbb{R} \times \{0\} \lesssim \mathbb{R} \times \mathbb{R} \sim \underline{2}^{\mathbb{N}} \times \underline{2}^{\mathbb{N}} \sim (\underline{2} \times \underline{2})^{\mathbb{N}} \sim \underline{4}^{\mathbb{N}} \leqslant \mathbb{N}^{\mathbb{N}} \leqslant \mathbb{R}^{\mathbb{N}} \sim (\underline{2}^{\mathbb{N}})^{\mathbb{N}} \sim \underline{2}^{\mathbb{N}\times\mathbb{N}} \sim \underline{2}^{\mathbb{N}} \sim \mathbb{R}$$

В силу теоремы Кантора-Берштейна-Шрёдера и континуум-гипотезы, заключаем $\mathbb{R}^2 \sim \mathbb{N}^{\mathbb{N}} \sim \mathbb{R}^{\mathbb{N}} \sim \mathbb{R}$.

1.1.15 Наборы множеств и конечные последовательности; ... (допустимо неформальное доказательство)

Наборы множеств и конечные последовательности Для произвольного множества A и каждого $n \in \mathbb{N}$ определили множество A^n наборов длины n из элементов A. На такие наборы можно также посмотреть как на функции $\underline{n} \to A$

Каждой функции $f : \ n \to A$ ставится в соответствие набор $(f(0), f(1), \ldots, f(n-1)) \in A^n$ или, с другой стороны, набору $(a_0, a_1, \ldots, a_{n-1})$ ставится в соответствие функция $k \mapsto a_k$ из $\underline{n}$ в A. Однако аккуратное (формальное) воплощение этих идей использует индукцию. Как нетрудно понять, главной трудностью для аккуратного изложения является определение набора $(f(0), f(1), \ldots, f(n-1))$ (или функции $k \mapsto a_k$) с помощью "основных способов задания множества".

1.1.16 Слова и формальные языки. Мощность языка над счётным алфавитом. Конкатенация слов, пустое слово. Префиксы и суффиксы. Отношение "префиксности"как частичный порядок.

Слова и формальные языки Алфавитом назовём произвольное непустое множество. Элементы алфавита A станем называть символами или буквами. Если $n \in \mathbb{N}$, любое отображение $\sigma : \ \underline{n} \to A$ мы назовём словом над алфавитом (или в алфавите) A. Ясно, что $|\sigma| = n$. Число $|\sigma|$ называют также длиной слова σ. Как мощность конечного множества, длина определена однозначно.

Множество всевозможных слов над A обозначается A^*. Иначе говоря, $A^* = \bigcup\limits_{n\in\mathbb{N}} A^{\underline{n}}$. Индексированное семейство $\{A^{\underline{n}}\}_{n\in\mathbb{N}}$ определено корректно, поскольку определена функция $F:\ n \to A^{\underline{n}}$.

Мощность языка над счётным алфавитом Если алфавит A конечный или счётный, то множество A^* счётно

Доказательство.

Согласно какой-то теореме, множество A^* конечно или счётно. По рекурсии определим функцию $f:\ \mathbb{N} \to A^*$, т.ч.:

$$f(0) = \varepsilon \wedge f(n+1) = f(n) \cup \{(n, a)\}, a \in A$$

при всех $n \in \mathbb{N}$. Индукцией по n легко проверить, что $f(n) \in A^{\underline{n}}$ и, в частности, $|f(n)| = n$. Поэтому $\mathbb{N} \overset{f}{\lesssim} A^*$. Согласно какой-то лемме, множество A^* счётно.

Конкатенация слов, пустое слово

Пустое слово Над любым алфавитом существует единственное слово длины 0, называемое пустым и обозначаемое ε. В самом деле, $A^{\underline{0}} = \{\varnothing\}$ и $\varepsilon = \varnothing$.

Конкатенация слов Конкатенацией слов σ и τ в алфавите A называется слово длины $|\sigma| + |\tau|$, обозначаемое $\sigma\tau$, т.ч.

$$\sigma\tau(i) = \begin{cases} \sigma(i), & i < |\sigma| \\ \tau(i - |\sigma|), & i \geqslant |\sigma| \end{cases}$$

Префиксы и суффиксы Если $\sigma = \tau\rho$, то говорят, что τ есть начало (или префикс) слова σ, а ρ есть окончание (или суффикс) слова σ. Пишут соответственно $\tau \sqsubseteq \sigma$ и $\rho \sqsupseteq \tau$

Отношение префиксности, как частичный порядок $(A^*,\ \sqsubseteq)$ есть ч.у.м. для любого алфавита A.

Доказательство.

Очевидно, $\sigma \sqsubseteq \sigma\varepsilon = \sigma$. Если $\rho \sqsubseteq \tau \wedge \tau \sqsubseteq \sigma$, то $\sigma = \tau\sigma' \wedge \tau = \rho\tau'$, откуда $\sigma = (\rho\tau')\sigma' = \rho(\tau'\sigma')$, а значит $\rho \sqsubseteq \sigma$. Если $\tau \sqsubseteq \sigma \wedge \sigma \sqsubseteq \tau$, то $\sigma\varepsilon = \sigma = \tau\sigma' = (\sigma\tau')\sigma' = \sigma(\tau'\sigma')$, что даёт $\varepsilon = \tau'\sigma'$ по закону сокращения. Имеем $|\tau'| + |\sigma'| = 0$ и, следовательно, $\tau' = \sigma' = \varepsilon$, откуда $\sigma = \tau\varepsilon = \tau$. Итак, $\sqsubseteq$ есть отношение нестрогого порядка.

1.1.17 Примеры индуктивных определений (в т.ч. для формальных языков)

Индуктивное определение множества чётных натуральных чисел Множество $E \subseteq \mathbb{N}$ чётных натуральных чисел, как известно, выделяется следующими равносильными свойствами:

$$n \in E \Leftrightarrow 2 \mid n \Leftrightarrow \exists m:\ n = 2m \Leftrightarrow \exists m:\ n = m + m$$

Из свойств сложения и умножения видно, что $0 \in E$ и для любых $n, m \in E$ верно $n+2 \in E$ и $n+m \in E$. Оказывается, эти свойства можно положить в основу другого определения чётности. Именно, рассмотрим множества $X \subseteq \mathbb{N}$, т.ч.

$$0 \in X \wedge \forall n\,(n \in X \Rightarrow n+2 \in X)$$

Пусть $\mathcal{X} \subset \mathcal{P}(\mathbb{N})$ есть множество всех подходящих X. Положим $E' = \bigcap \mathcal{X}$. Поскольку $\mathcal{X} \neq \varnothing$, для каждого $n \in \mathbb{N}$ имеем

$$n \in E' \Leftrightarrow \forall X \in \mathcal{X} :\ n \in X$$

Получаем $E' \subseteq X$ для каждого $X \in \mathcal{X}$. Раз $0 \in X$ для всех $X \in \mathcal{X}$, то $0 \in E'$. Для всех $X \in \mathcal{X}$ из $n \in \mathcal{X}$ следует $n+2 \in X$; поэтому $n \in E'$ влечёт $n+2 \in E'$. Значит, $E' \in \mathcal{X}$. Таким образом, множество E' является $\subseteq$-наименьшим подходящим.

Убедимся, что $E' = E$. Поскольку $E \in \mathcal{X}$, имеем $E' \subseteq E$. Обратно, предположим противное. Пусть $n = \min(E \setminus E')$. Раз $0 \in E', 1 \notin E$, то $n \geqslant 2$, т.е. $n = m+2$. По минимальности n, число $m \in E$ должно принадлежать E'. Но тогда и $n = m+2 \in E' \in \mathcal{X}$. Противоречие.

Индуктивное определение транзитивного замыкания Пусть R - отношение на множестве A. Транзитивным замыканием $\hat{R}$ отношения R называется $\subseteq$-наименьшее отношение $Q \subseteq A^2$, т.ч.

$$R \subseteq Q \wedge \forall x\,\forall y, \forall z\,((xQy \wedge yQz) \rightarrow xQz)$$

Иными словами, $\hat{R}$ есть наименьшее транзитивное надмножество отношения R. Пусть $\mathcal{Q} \subseteq \mathcal{P}(A^2)$ будет множество всех транзитивных надмножеств R. Очевидно, $A^2 \in \mathcal{Q} \neq \varnothing$. Тогда легко проверить, что $\hat{R} = \bigcap \mathcal{Q}$.

Неформально говоря, транзитивное замыкание получится, если добавить к R все те и только те стрелки, которых не хватает для транзитивности.

Добавлять стрелки можно "по шагам однако новые стрелки создают новые нарушения транзитивности и влекут очередные шаги. Сейчас мы убедимся, что "шагать вдоль $\mathbb{N}$"достаточно, чтобы добавить все нужные стрелки.

Пусть $R \subseteq A^2$. Положим $(R)_1 = R \wedge (R)_{n+1} = (R)_n \circ R$ при всех $n > 0$. Индукцией легко доказать, что $(R)_{n+m} = (R)_n \circ (R)_m$.

$$\hat{R} = \bigcup_{n \in \mathbb{N}_+} (R)_n$$

Обозначим $U = \bigcup\limits_{n \in \mathbb{N}_+} (R)_n \subset A^2$. Очевидно, $R \subseteq U$. Если $(x,y), (y,z) \in U$, то $\exists m, n \in \mathbb{N} :\ x(R)_m y \wedge y(R)_n z$. Тогда $(x,z) \in (R)_{n+m} \in \subseteq U$. Поэтому $U \in \mathcal{Q}$, откуда $\hat{R} = \bigcap \mathcal{Q} \subseteq U$. Обратно. Пусть $Q \in \mathcal{Q}$. Индукцией по n докажем, что $(R)_n \subseteq Q$. При $n = 1$ это ясно. Если $(R)_n \subseteq Q$, то $(R)_{n+1} = (R)_n \circ R \subseteq Q \circ Q \subseteq Q$ в силу транзитивности Q. Следовательно, $U \subseteq Q$ при всех $Q \in \mathcal{Q}$, откуда $U \subseteq \bigcap \mathcal{Q} = \hat{R}$

Индуктивное определение двоичных записей Определим множество B' как $\subseteq$-наименьшее такое $X \subseteq \underline{2}^*$, что

$$\{0,1\} \subseteq X \wedge \forall \sigma\,(\sigma \in X \setminus \{0\} \Rightarrow \sigma 0, \sigma 1 \in X)$$

Как и в предыдущих примерах, $B' = \bigcap \mathcal{X}$, где $\mathcal{X}$ есть непустое множество всех подходящих X.

Приведённое определение отражает естественный принцип образования новых двоичных записей из имеющихся: к любой ненулевой записи справа можно приписать ещё один разряд.

Индуктивное определение множества всех правильных скобочных последовательностей Определим множество S как $\subseteq$-наименьшее такое $X \subseteq \mathcal{B}^*$, что

$$\varepsilon \in X \wedge \forall\sigma\,\forall\tau\,(\sigma,\tau \in X \Rightarrow \langle\sigma\rangle, \sigma\tau \in X)$$

Индуктивное определение собственного языка Опередим язык Ar замкнутых арифметических термов, состоящих из выражений вроде $\langle\langle 3{+}2\rangle{\cdot}5\rangle$, где натуральные числа сами выступают своими обозначениями. Итак, Ar есть наименьшее $X \subseteq (\mathbb{N} \cup \{+,\,\cdot\,,\langle,\rangle\})^*$, т.ч.

$$\forall n \in \mathbb{N}:\ n \in \ \mathrm{Ar}\ \wedge \forall\sigma\,\forall\tau(\sigma,\tau \in X \Rightarrow \langle\sigma+\tau\rangle, \langle\sigma\cdot\tau\rangle \in X)$$

1.1.18 Вполне упорядоченные множества (в.у.м.): существование последователя ненаибольшего элемента и супремума ограниченного множества. Предельные элементы в.у.м. и их свойства

Определение Порядок $<$ на множестве X фундирован (или множество X фундировано), если во всяком непустом $Y \subseteq X$ существует минимальный элемент. Множество вполне упорядоченно, если оно линейно и фундировано. При этом, конечно, минимальные и наименьшие элементы совпадают.

Существование последователя ненаибольшего элемента и супремума ограниченного множества Пусть $(X,\,<)$ непустое в.у.м. и $Y \subseteq X$

1. В X есть наименьший элемент (обозначаемый 0 или 0_X)
2. Y есть в.у.м. относительно $<|_{Y^2}$
3. Если $Y \neq \varnothing$, то существует $\inf Y$
4. Если $x < s$, то существует и единственен y, называемый последователем x (обозначение $y = x+1$), т.ч. $x < y \wedge \forall z > x\,(y \leqslant z)$ (эквивалентно, $y = \min\{z \mid z > x\}$)
5. Если существует верхняя грань Y, то существует (и единственен) $\sup Y$.

Доказательство. В третьем пункте за инфимум берём $\min Y$. В двух последних пунктах нужно рассмотреть множество $\{z \mid z > x\}$ и множество верхних граней Y, непустые по условию, и взять их наименьшие элементы.

Определение предельных элементов Для элемента x в.у.м. $(X,\,<)$ введём обозначение $[0,x) := \{y \mid y < x\}$. Элемент x называется предельным (обозначение $x \in \mathrm{Lim}$), если $x = \sup[0,x) \wedge x \neq 0$. Наименьший элемент в.у.м. 0 тоже иногда считают предельным, поскольку $0 = \sup\varnothing = \sup[0,0)$, мы не станем этого делать, но обозначим $\mathrm{Lim}^* = \mathrm{Lim} \cup \{0\}$

Предельные элементы в.у.м. и их свойства Следующие условия равносильны:

1. $x \in \mathrm{Lim}^*$
2. $\forall y\, \neg(y+1=x)$
3. $\forall y < x\, (y+1<x)$

Доказательство.

$1 \Rightarrow 2$. Пусть $x \in \mathrm{Lim}^*$. Допустим найдётся y, т.ч. $y+1=x$, откуда $y<x$. Тогда y является верхней гранью $[0,x)$: если $z>y$, то по определению последователя $z \geqslant y+1=x$ и $z \notin [0,x)$. Это противоречит тому, что x - наименьшая верхняя грань.

$2 \Rightarrow 3$. Пусть $y<x$. По определению последователя, $y+1 \leqslant x$. Имеемм $y+1<x$

$3 \Rightarrow 1$. Пусть $\forall y<x\,(y+1<x)$. Допустим, существует $z<x$ - верхняя грань множества $[0,x)$. Но тогда $z<z+1 \in [0,x)$. Противоречие.

1.1.19 Теорема о строении элементов в.у.м.

Всякий элемент $x \in X$ однозначно представим в виде $x=y+n$, где $y \in \mathrm{Lim}^*$.

Доказательство.

Если $x=0$, то всё доказано. Пусть $x>0$. Рассмотрим множество $C=\{z \in X \mid \exists k \in \mathbb{N}_+\ (z+k=x)\}$. Если $C=\varnothing$, то для всех $z \in X$ имеем $z+1 \neq x$. В силу предыдущей леммы, полагаем $y=x \in \mathrm{Lim}$ и $n=0$. Рассмотрим случай $C \neq \varnothing$. Тогда в C есть наименьший элемент z', и для некоторого $k'>0$ верно $x=z'+k'$. Если $z'=0$, то $y=0, n=k'$. Иначе $z' \in \mathrm{Lim}$. Действительно, очевидная индукция по $n \in \mathbb{N}$ показывает, что $(u+1)+n=u+(n+1)$. Поэтому если $z'=z''+1$, то $z'' \in C \wedge z''<z'$. Что не так вследствие предыдущей теоремы. Теперь можно взять $y=z', n=k'$

Пусть $x=y_1+n_1=y_2+n_2$. Легко показать, что $u+1=v+1$ влечёт $u=v$. Поэтому если $n_1 \neq n_2$, без ограничения общности, $n_1<n_2$, то имеем $y_1=y_2+(n_2-n_1)$, что по предыдущей лемме влечёт $y_1 \notin \mathrm{Lim}$. Следовательно $n_1=n_2$, откуда $y_1=y_2$.

1.1.20 Сложение и умножение в.у.м. свойства этих операций

Умножение в.у.м. Произведением AB в.у.м. $(A,\ <_A)$ и $(B,\ <_B)$ называется $(A\times B,\ <)$, где

$$(a_1,b_1)<(a_2,b_2) := (b_1 <_B b_2) \vee (b_1=b_2 \wedge a_1 <_A a_2)$$

Сложение в.у.м. Сумма в.у.м. $A+B$ есть $(A\times\{0\} \cup B\times\{1\},\ <)$, где

$$(x,\varepsilon)<(y,\delta) := (\varepsilon<\delta) \vee (\varepsilon=\delta=0 \wedge x <_A y) \vee (\varepsilon=\delta=1 \wedge x <_B y)$$

Свойства этих операций Сложение и умножение обладают свойствами ассоциативности и левой дистрибутивности. Именно, для произвольных в.у.м. (и даже просто линейно упорядоченных множеств) A,B,C выполнены:

1. $A+(B+C) \cong (A+B)+C$
2. $A(BC) \cong (AB)C$
3. $C(A+B) \cong CA+CB$

Доказательство. Требуемые изоморфизмы несложно построить непосредственно.

1.1.21 Строение в.у.м. без наибольшего элемента

Если в.у.м. A не имеет наибольшего элемента, то $A \cong \mathbb{N} \cdot B$. Для некоторого в.у.м. B.

Доказательство.

Положим $B = \mathrm{Lim}^*_A \subseteq A$. Согласно лемме о представлении элементов в.у.м., существует функция $f : A \to \mathbb{N} \times B$, т.ч. $f(a) = (n, y)$. Очевидно, f является инъекцией и даже монотонной функцией. Действительно, если $a_1 = y_1 + n_1 < y_2 + n_2 = a_2$, то $y_2 < y_1$, по лемме о свойствах предельных элементов, влекло бы $y_2 + n_2 < y_1$, что не так. Значит, $y_1 \leqslant y_2$, причём, если $y_1 = y_2$, очевидно, $n_1 < n_2$. Во всяком случае $f(a_1) = (n_1, y_1) < (n_2, y_2) = f(a_2)$.

Проверим сюръективность f. Допустим, что $y \in B$. Индукцией по n докажем, что все $y + n \in A$. В самом деле, по условию элемент $y + n$ не максимален в A, а значит имеет последователь $y + (n + 1) \in A$. Но тогда $f(y + n) = (n, y)$ в силу единственности представления элементов в.у.м.

Итак, $f : A \to \mathbb{N} \times B$ есть монотонная биекция и, как легко заметить, искомый изоморфизм.

1.1.22 Начальные отрезки в.у.м. и их свойства. Множество (собственных) начальных отрезков как в.у.м.

Начальные отрезки Подмножество I в.у.м. X называется начальным отрезком, если оно "замкнуто вниз": $\forall x \in I \, \forall y < x \, (y \in I)$. Если $I \neq X$, то это собственный начальный отрезок.

Свойства н.о., множество (собственных) начальных отрезков как в.у.м. Пусть $(X, <)$ в.у.м.

1. X есть свой начальный отрезок.
2. Пусть I_a суть н.о. X при всех $a \in A$. Тогда $\bigcup\limits_{a \in A} I_a$ есть н.о. X.
3. Если $x \in X$, то $[0, x)$ есть н.о. X.
4. Если I собственный н.о. X, то существует и единственен такой $x \in X$, что $I = [0, x)$.
5. Пусть $\mathcal{I} = \{I \mid I \text{ н.о. } X\}$. Тогда $(\mathcal{I}, \subset)$ есть в.у.м.
6. $(\mathcal{I}, \subset) \cong X + 1, (\mathcal{I} \setminus \{X\}, \subset) \cong X$.

Доказательство.

Проверим п.2. Пусть $x \in \bigcup\limits_{a \in A} I_a$ и $y < x$. Тогда найдётся н.о. $I_a \ni x$. Поэтому $y \in I_a \subseteq \bigcup\limits_{a \in A} I_a$.

П.4. Имеем $X \setminus I \neq \varnothing$. Возьмём наименьший x элемент этого множества. Очевидно $y < x \to y \in I$. Пусть $y \in I$, но $x \leqslant y$. Тогда $x \in I$, что не так. Значит, $y < x \leftarrow y \in I$. Единственность следует из линейности $<$.

П.5. Порядок $(\mathcal{I}, \subset)$ линеен: все собственные н.о. вложены в X и сравнимы между собой по предыдущему пункту. Выделим в семействе $\mathcal{J} \subseteq \mathcal{I}$ наименьший элемент. Если $\mathcal{J} = \{X\}$, то всё ясно. Иначе возьмём в непустом множестве $\{x \mid [0, x) \in \mathcal{J} \setminus \{X\}\}$ наименьший элемент x'. Ясно, что $[0, x') \in \mathcal{J}$ будет наименьшим в смысле $\subset$.

П.6. Изоморфизм строится так: $[0, x) \mapsto x$ для всех $x \in X$, а X переходит в наибольший элемент множества $X + 1$.

1.1.23 Невозможность изоморфизма в.у.м. и его собственного начального отрезка. Сравнение в.у.м. (определение). Невозможность бесконечной убывающей последовательности в.у.м.

Невозможность изоморфизма в.у.м. и его с.н.о.

Вспомогательная лемма Пусть $(X, <)$ - в.у.м. и функция $f : X \to X$ монотонна. Тогда $\forall x \in X : (f(x) \geqslant x)$

Доказательство.

Допустим противное. Тогда подмножество $\{x \mid f(x) < x\}$ непусто. Пусть x' его наименьший элемент. Имеем $f(x') < x'$ и по монотонность $f(f(x')) < f(x')$, т.е. элемент $f(x')$ тоже лежит в этом множестве, что не так.

Невозможность изоморфизма Пусть I собственный н.о. в.у.м. $(X, <)$. Тогда $X \ncong I$.

Доказательство.

По лемме о свойствах с.н.о. $I = [0, x)$ для некоторого $x \in X$. Пусть есть изоморфизм $f : X \to I$. По предыдущей лемме имеем $f(x) \geqslant x$. С другой стороны, $f(x) \in I$ и $f(x) < x$.

Сравнение в.у.м.

$$A < B \Leftrightarrow A \text{ изоморфно собственному н.о. множества} B$$

Получаем строгий частичный порядок.

$$A \leqslant B \Leftrightarrow (A < B \vee A \cong B)$$

Получаем транзитивное и рефлексивное, но не антисимметричное отношение (предпорядок).

Невозможность бесконечной убывающей последовательности в.у.м. Порядок $<$ на классе в.у.м. фундирован.

Доказательство.

Пусть дано непустое семейство в.у.м. X. Возьмём произвольное множество $A \in X$. Если оно минимальное в X, всё доказано. В противном случае непусто семейство $X_A = \{B \in X \mid B < A\}$. По определению $<$, кажому $B \in X_A$ соответствует собственный н.о. $[0, x_B)$ множества A, причём изоморфным множествам соответствует один н.о. Среди элементов x_B имеется наименьший x'_B. Любое из соответствующих множеств B' является минимальным в X.

1.1.24 Сравнение в.у.м. и его подмножества. Монотонность сложения и умножения в.у.м.

Сравнение в.у.м. и его подмножества Пусть C - в.у.м. и $B \subseteq C$. Тогда $B \leqslant C$.

Доказательство.

Допустим $B > C$. Тогда, по определению, $C \overset{f}{\cong} [0_B, b) \subset B$ для некоторого $b \in B$. Поскольку $b \in C$, имеем $f(b) < b$. С другой стороны $f(b) \geqslant b$. Противоречие.

Монотонность сложения и умножения в.у.м. Пусть A, B, C в.у.м. и $B < C$. Тогда

1. $A + B < A + C$
2. $B + A \leqslant C + A$
3. $A \neq \varnothing \Rightarrow AB < AC$
4. $BA \leqslant CA$

Доказательство.

1. Имеем $B \overset{f}{\cong} [0_C, c)$. Строим отображение $(a, 0) \mapsto (a, 0)$ для $a \in A$ и $(b, 1) \mapsto (f(b), 1)$ для $b \in B$. Ясно, что оно задаёт изоморфизм $A + B$ и $A + [0_C, c) = [0_{A+C}, (c, 1))$ для некоторого $c \in C$.
2. Как и в предыдущем пункте, легко получаем $B + A \cong [0_C, c) + A$. Однако последнее подмножество множества $C + A$ может не быть н.о. Поэтому нам остаётся лишь применить лемму о сранении в.у.м. и его подмножества.
3. Если $B \overset{f}{\cong} [0_C, c)$, то отображение $(a, b) \mapsto (a, f(b))$ даёт $AB \cong A[0_C, c)$. Понятно, что последнее множество есть собственный н.о. AC, если $A \neq \varnothing$
4. Имеем $BA \cong [0_C, c)A$. Последнее подмножество множества CA может не быть н.о.

1.1.25 Вывод аксиомы выбора из теоремы Цермело

Теорема Цермело Для всякого множества X существует бинарное отношение $<$ на X такое, что $(X, <)$ - в.у.м.

Вывод AC из теоремы Цермело Пусть S - данное семейство непустых множеств. По теореме Цермело множество $U = \bigcup S$ может быть вполне упорядочено. Для каждого $x \in S$ имеем $x \subset U$. Пусть $\min(x)$ означает наименьший элемент x в смысле порядка на U. Поскольку $\varnothing \notin S$, соответствие $x \mapsto \min(x)$ является функцией выбора на S.

1.2 Вопросы на хор

1.2.1 Существует и единственно пустое множество. Парадокс Рассела. Не существует множества всех множеств.

Существование пустого множества Существует пустое множество $\varnothing$, т.ч. $x \notin \varnothing$ для всех множеств x.

В самом деле, достаточно в любом множестве выделить подмножество элементов, удовлетворяющих какому-нибудь противоречивому свойству, например,

$$\varnothing = \{x \in \mathbb{N} \mid x = x \wedge x \neq x\}$$

Единственность пустого множества Пустое множество единственно в том смысле, что если N_1 и N_2 два пустых множества, то $N_1 = N_2$.

Действительно, по определению пустого множества, условия $x \in N_1$ и $x \in N_2$ ложны для всех x. Следовательно, $\forall x : \ x \in N_1 \Leftrightarrow x \in N_2$

Парадокс Рассела То, что новое множество состоит из элементов уже опрелённого, существенно. Снятие этого ограничения легко приводит к парадоксу Рассела: действительно, тогда существует множество

$$R = \{x \mid x \notin x\}$$

Не существует множества всех множеств Пусть существует такое множество A, что $\forall x : x \in A$. Тогда зададим множество $B = \{x \in A \mid x \notin x\}$. Заметим, что $x \in A$ всегда истино, значит $x \in B \Leftrightarrow x \notin B$. Противоречие.

1.2.2 Упорядоченные пары и критерий их равенства. Декартово произведение множеств. Натуральная декартова степень множества

Упорядоченные пары и критерий их равенства

Упорядоченные пары Для произвольных множеств a и b символом (a, b) обозначают множество $\{\{a\}, \{a, b\}\}$ называемое упорядоченной парой множеств a и b.

Критерий их равенства Для любых множеств a, b, c, d имеет место

$$(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d$$

Доказательство.

Предположим, что $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$ Тогда $\{a\} \in \{\{c\}, \{c, d\}\}$, т.е. $\{a\} = \{c\}$ или $\{a\} = \{c, d\}$. В первом случае $a \in \{c\}$, т.е. $a = c$. Во втором имеем $c \in \{a\}$, откуда $c = a$. Итак, $a = c$.

Из условия также получаем $\{a, b\} = \{c\}$ или $\{a, b\} = \{c, d\}$.

В первом случае $b \in \{c\}$, откуда $b = c = a$. Поскольку $\{c, d\} = \{a\}$ или $\{c, d\} = \{a, b\}$, получаем $d = a = b$. Значит, $b = d$.

Пусть теперь $\{a, b\} = \{c, d\}$. Если $d = b$, то всё доказано. Иначе $d = a = c$, т.е. $\{a, b\} = \{d\}$, откуда вновь $b = d$

Остаётся проверить обратную импликацию. Пусть $a = c$ и $b = d$. Если $x \in (a, b)$, то $x = \{a\}$ или $x = \{a, b\}$. Очевидно, тогда $x = \{c\} \in (c, d)$ или $x = \{c, d\} \in (c, d)$. Аналогично, $(c, d) \subseteq (a, b)$.

Декартово произведение множеств Декартовым (или прямым) произведением множеств A и B называется множество:

$$A \times B = \{z \in \mathcal{P}(\mathcal{P}(A \cup B)) \mid \exists a \in A \, \exists b \in B \; z = (a, b)\}$$

Натуральная декартова степень множества Как и в случае обычного умножения, декартово произведение позволяет определить натуральные степени - для произвольного множества A и всех натуральных чисел $n \geqslant 2$ мы полагаем:

$$A^0 = \{\varnothing\}$$

$$A^1 = A$$

$$A^n = A \times A \times \cdots \times A$$

1.2.3 Сравнение множеств по мощности (вложение). Невозможность вложения $\mathcal{P}(A)$ в A

Сравнение множеств по мощности (вложение)

Вложение Множество A не превосходит по мощности (или вкладывается во) множество B, если существует инъекция $f: A \to B$. Тогда пишем $A \overset{f}{\lesssim} B$ и $A \lesssim B$

Свойства вложения Для любых A, B, C имеем:

1. $A \lesssim A$
2. $A \lesssim B \wedge B \lesssim C \Rightarrow A \lesssim C$
3. $A \sim B \Rightarrow A \lesssim B \wedge B \lesssim A$
4. $A \lesssim B \Leftrightarrow \exists D \subseteq B: A \sim D$

Доказательство.

В последнем утверждении достаточно положить $D = f[A]$, где $f: A \to B$ есть некоторая инъекция.

Невозможность вложения $\mathcal{P}(A)$ в A Ни для какого множества A невозможно $\mathcal{P}(A) \lesssim A$

Доказательство.

Пусть это не так. Рассмотрим произвольную инъекцию $f: \mathcal{P}(A) \to A$. Положим

$$Y = \{a \in A \mid \forall X \in \mathcal{P}(A)\ (a = f(x) \Rightarrow a \notin X)\}$$

Очевидно, $Y \in \mathcal{P}(A)$. Если $f(Y) \in Y$, то, взяв $X = Y$, получаем $f(Y) \notin Y$. Противоречие показывает, что $f(Y) \notin Y$. Рассмотрим произвольное $X \in \mathcal{P}(A)$, т.ч. $f(Y) = f(X)$. В силу инъективности $X = Y$. Но тогда $f(Y) \notin X$ для всех таких X, значит $f(Y) \in Y$. Противоречие.

1.2.4 Связь между строгими и нестрогими порядками на множестве

Определения Пусть $S(A)$ - множество всех строгих порядков на множестве A.

Пусть $N(A)$ - множество всех нестрогих порядков на множестве A.

Рассмотрим функции $\varphi: S(A) \to \mathcal{P}(A^2)$ и $\psi: N(A) \to \mathcal{P}(A^2)$, т.ч.

$$\varphi(P) = P \cup \mathrm{id}_A;\ \psi(Q) = Q \setminus \mathrm{id}_A$$

О свойствах функций φ, ψ Для любых $P \in S(A)$ и $Q \in N(A)$ верно:

1. $\varphi(P) \in N(A), \psi(\varphi(P)) = P$
2. $\psi(Q) \in S(A), \varphi(\psi(Q)) = Q$

Доказательство.

По определению, $\mathrm{id}_A \subseteq \varphi(P)$, используя транзитивность P, докажем транзитивность $\varphi(P)$

$$\varphi(P) \circ \varphi(P) = (P \cup \mathrm{id}_A) \circ (P \cup \mathrm{id}_A) = (P \circ P) \cup (P \circ \mathrm{id}_A) \cup (\mathrm{id}_A \circ P) \cup (\mathrm{id}_A \circ \mathrm{id}_A) =$$

$$(P \circ P) \cup P \cup \mathrm{id}_A \subseteq P \cup \mathrm{id}_A = \varphi(P)$$

Остаётся проверить антисимметричность $\varphi(P)$. Воспользуемся тем, что P антисимметрично:

$$\varphi(P) \cap (\varphi(P))^{-1} = (P \cup \mathrm{id}_A) \cap (P \cup \mathrm{id}_A)^{-1} = (P \cup \mathrm{id}_A) \cap (P^{-1} \cup \mathrm{id}_A) = (P \cap P^{-1}) \cup \mathrm{id}_A = \mathrm{id}_A$$

Итак, $\varphi(P) \in N(A)$. Далее,

$$\psi(\varphi(P)) = (P \cup \mathrm{id}_A) \cap \overline{\mathrm{id}_A} = (P \cap \overline{\mathrm{id}_A}) \cup (\mathrm{id}_A \cap \overline{\mathrm{id}_A}) = (P \cap \overline{\mathrm{id}_A}) \cup \varnothing =$$

$$(P \cap \overline{\mathrm{id}_A}) \cup (P \cap \mathrm{id}_A) = P \cap (\mathrm{id}_A \cup \overline{\mathrm{id}_A}) = P \cap A^2 = P$$

Докажем второе утверждение. По определению, $\psi(Q) \cap \mathrm{id}_A = \varnothing$, т.е. $\psi(Q)$ иррефлексивно. Пусть $(x, y) \in \psi(Q), (y, z) \in \psi(Q)$. Тогда xQy и yQz, откуда xQz, но также $x \neq y, y \neq z$. Предположим, что $x = z$. Имеем yQx, т.е. $xQ^{-1}y$. Но Q антисимметрично, а значит $x = y$, что не так. Следовательно, $x \neq z$ и $(x, z) \in Q \setminus \mathrm{id}_A = \psi(Q)$. Итак, отношение $\psi(Q)$ транзитивно и $\psi(Q) \in S(A)$. Наконец,

$$\varphi(\psi(Q)) = (Q \cap \overline{\mathrm{id}_A}) \cup \mathrm{id}_A = (Q \cup \mathrm{id}_A) \cap (\mathrm{id}_A \cup \overline{\mathrm{id}_A}) = (Q \cup \mathrm{id}_A) \cap A^2 =$$

$$(Q \cup \mathrm{id}_A) = Q$$

поскольку $\mathrm{id}_A \subseteq Q$.

Следствие теоремы Функция $\varphi : S(A) \to N(A)$ является биекцией, причём $\psi = \varphi^{-1}$.

1.2.5 Связь между отношениями эквивалентности и разбиениями

Определения Пусть $\mathrm{Eq}(A)$ есть множество всех отношений эквивалентности на A, и $\Pi(A)$ есть множество всех разбиений множества A. Рассмотрим функцию $\pi : Eq(A) \to \mathcal{P}(\mathcal{P}(A))$ и $\varepsilon : \Pi(A) \to \mathcal{P}(A^2)$, т.ч.

$$\pi(E) = A/E;\ \varepsilon(\Sigma) = \{(x, y) \in A^2 \mid \exists \sigma \in \Sigma\, (x \in \sigma \wedge y \in \sigma)\}$$

Свойства функций π, ε Для любых $E \in Eq(A), \Sigma \in \Pi(A)$ верно:

1. $\pi(E) \in \Pi(A), \varepsilon(\pi(E)) = E$
2. $\varepsilon(\Sigma) \in Eq(A), \pi(\varepsilon(\Sigma)) = \Sigma$

Доказательство.

$\pi(E)$ есть разбиение A в силу леммы из вопросов на удос. Пусть $(x, y) \in \varepsilon(A/E)$. Тогда существует $\sigma \in A/E$, т.ч. $x, y \in \sigma$, т.е. $x, y \in [z]_E$ для некоторого $z \in A$. Значит zEx, zEy, откуда $(x, y) \in E$. Обратно, пусть xEy, тогда $y \in [y]_E = [x]_E$ и $x, y \in [x]_E \in A/E$. Следовательно, $(x, y) \in \varepsilon(A/E)$. Итак, $\varepsilon(\pi(E)) = E$.

Првоерим теперь что $\varepsilon(\Sigma)$ есть эквивалентность на A. Поскольку $\bigcup \Sigma = A$, для каждого $x \in A$ найдётся $\sigma \in \Sigma$, т.ч. $x \in \sigma$; значит, $(x, x) \in \varepsilon(\Sigma)$. Симметричность $\varepsilon(\Sigma)$ очевидна. Допустим теперь, что $(x, y), (y, z) \in \varepsilon(\Sigma)$. Тогда для некоторых $\sigma, \tau \in \Sigma$ имеем $x \in \sigma, y \in \sigma, y \in \tau, z \in \tau$. Из $\sigma \cap \tau \neq \varnothing$ получаем $\sigma = \tau$, откуда $x, z \in \sigma$ и $(x, z) \in \varepsilon(\Sigma)$

Остаётся проверить, что $\pi(\varepsilon(\Sigma)) = \Sigma$. Докажем сначала, что для всех $\sigma \in \Sigma$ и всех $x \in \sigma$ верно $\sigma = [x]_{\varepsilon(\Sigma)}$. В самом деле, если $y \in \sigma$, получаем $x, y \in \sigma \in \Sigma$, откуда $(x, y) \in \varepsilon(\Sigma)$, т.е. $y \in [x]_{\varepsilon(\Sigma)}$. Имеем $\sigma \subseteq [x]_{\varepsilon(\Sigma)}$. Обратно, пусть $y \in [x]_{\varepsilon(\Sigma)}$. Тогда $x, y \in \sigma'$ для некоторого $\sigma' \in \Sigma$. Из $x \in \sigma \cap \sigma' \neq \varnothing$ следует, что $\sigma' = \sigma$, а значит $y \in \sigma$. получили $[x]_{\varepsilon(\Sigma)} \subseteq \sigma$.

Допустим теперь, что $\tau \in A/\varepsilon(\Sigma)$. Тогда $\tau = [x]_{\varepsilon(\Sigma)}$ для некоторого $x \in A$. С другой стороны, $x \in \sigma$ для некоторого $\sigma \in \Sigma$ в силу $\bigcup \Sigma = A$. По доказанному $\sigma = [x]_{\varepsilon(\Sigma)}$, а значит $\tau = \sigma \in \Sigma$. Таким образом, $\pi(\varepsilon(\Sigma)) \subseteq \Sigma$

Обратно, пусть $\tau \in \Sigma$. Поскольку $\tau \neq \varnothing$, можно выбрать $x \in \tau$. Имеем тогда $\tau = [x]_{\varepsilon(\Sigma)} \in A/\varepsilon(\Sigma)$. Итак, $\Sigma \subseteq \pi(\varepsilon(\Sigma))$.

Следствие Функция $\pi : Eq(A) \to \Pi(A)$ является биекцией, причём $\varepsilon = \pi^{-1}$.

1.2.6 Равносильность принципов математической индукции, порядковой индукции и наименьшего числа

Определения Принцип математической индукции: для всякого множества $X \subseteq \mathbb{N}$ если $0 \in X$ и для каждого $n \in \mathbb{N}$ из $n \in X$ следует $n + 1 \in X$, то $X = \mathbb{N}$

Прогрессивное множество: назовём множество $X \subseteq \mathbb{N}$ прогрессивным, если для каждого $n \in \mathbb{N}$ из $\forall m < n\, m \in X$ следует $n \in X$.

Принцип порядковой индукции: для всякого множества $X \subseteq \mathbb{N}$ если оно прогрессивное, то $X = \mathbb{N}$

Принцип наименьшего числа: для всякого множества $X \subseteq \mathbb{N}$ если $X \neq \varnothing$, то в X существует наименьший элемент $\min X$.

Равносильность принципов Следующие утверждения равносильны:

1. Принцип порядковой индукции
2. Принцип наименьшего числа
3. Принцип математической индукции

Доказательство.

Пусть принцип порядковой индукции выполнен. Тогда убедимся, что в каждом непустом $X \subseteq \mathbb{N}$ есть наименьший элемент. Предположим, что в некотором X нет наименьшего элемента. Покажем, что множество $\overline{X}$ прогрессивно. В самом деле, если $\forall m < nm \notin X$, ибо иначе $n = \min X$, что невозможно. По принципу порядковой индукции $\overline{X} = \mathbb{N} \Rightarrow X = \varnothing$.

Пусть принцип наименьшего числа выполнен. Установим, что для всякого множества $X \subseteq \mathbb{N}$ из предположений $0 \in X, \forall n\ (n \in X \Rightarrow n + 1 \in X)$ вытекает $X = \mathbb{N}$. Рассмотрим множество $\overline{X}$. Допустим, что $\overline{X} \neq \varnothing$. Тогда существует $n = \min \overline{X}$. По предположению, $n \neq 0 \notin \overline{X}$. Значит, $n = m + 1$ для некоторого $m \in \mathbb{N}$. Поскольку $m < n$, имеем $m \in X$. В силу предположения, $n = m + 1 \in X$, что не так. Следовательно, $\overline{X} = \varnothing, X = \mathbb{N}$.

Пусть принцип математической индукции выполнен. Проверим, что для всякого множества $X \subseteq \mathbb{N}$ из предположения $Prog(X)$ следует $X = \mathbb{N}$. Рассмотрим множество

$$Y = \{n \in \mathbb{N} \mid \forall m < n\, m \in X\}$$

Очевидным образом, $0 \in Y$. Допустим, что $n \in Y$. Тогда $\forall m < n\ m \in X$, что, в силу прогрессивности X, влечёт $n \in X$. Если $m < n + 1$, то $m < n \vee m = n$. В каждом из случаев $m \in X$, а значит $n + 1 \in Y$. Для множества Y мы проверили основание и шаг индукции; по принципу математической индукции заключаем $Y = \mathbb{N}$. Для всякого $n \in \mathbb{N}$ имеем $n < n + 1 \in Y$, откуда $n \in X$. Следовательно, $X = \mathbb{N}$.

1.2.7 Принцип Дирихле (с доказательством). Мощность конечного множества: корректность определения

Принцип Дирихле

Вспомогательная лемма Для каждого $n \in \mathbb{N}$, если $f : \underline{n+1} \to \underline{n}$, то f не инъекция.

Доказательство.

Предположим противное: пусть найдётся $n \in \mathbb{N}$, для которого есть инъекция $f : \underline{n+1} \to \underline{n}$. Согласно принципу наименьшего числа, рассмотрим наименьшее такое n. Инъекция $f : \underline{1} \to \underline{0}$ невозможно, т.к. $f(0) \notin \underline{0}$. Значит, $n \neq 0$, т.е. $n = m + 1$ для некоторого $m \in \mathbb{N}$.

Пусть $f(n) = x \in \underline{n}$. Рассмотрим функцию $g : \underline{n} \to \underline{n}$, меняющую m и x местами. Точнее,

$$g(k) = \begin{cases} m, & k = x \\ x, & k = m \\ k & \text{иначе} \end{cases}$$

Ясно, что g - инъекция. Функция $f \restriction \underline{n} : \underline{n} \to \underline{n}$ также является инъекцией. Значит, и $h = g \circ (f \restriction \underline{n})$ есть инъекция $\underline{n} \to \underline{n}$.

Если $h(k) = m$, то $(f \restriction \underline{n})(k) = x$. Но тогда $f(n) = x = f(k)$, хотя $n \neq k$. Это противоречит инъективности функции f. Выходит, h не принимает значения m и $\operatorname{rng} h \subseteq \underline{m}$. Тогда h есть инъекция $\underline{m+1} \to \underline{m}$. Однако такой инъекции нет, поскольку $m < n$, а число n наименьшее возможное. Противоречие.

Прицнип Дирихле Если $m > n$ и $f : \underline{m} \to \underline{n}$, то f не инъекция.

Доказательство.

Допустим, инъекция $f : \underline{m} \to \underline{n}$ существует. Так как $m > n$, имеем $m \geqslant n + 1$, откуда $\underline{n+1} \subseteq \underline{m}$. Следовательно, функция $f \restriction \underline{n+1} : \underline{n+1} \to \underline{n}$ также является инъекцией, что невозможно.

Мощность конечного множества: корректность определения

Корректность 1 Если $m \neq n$, то $\underline{m} \nsim \underline{n}$.

Доказательство.

Если $m \neq n$, то $m > n$ или $m < n$. В первом случае, по принципу Дирихле, невозможно $\underline{m} \lesssim \underline{n}$, а во втором - невозможно $\underline{n} \lesssim \underline{m}$. В каждом из случаев исключается $\underline{n} \sim \underline{m}$.

Корректность 2 Для каждого конечного множества A существует единственное $n \in \mathbb{N}$, т.ч. $A \sim \underline{n}$.

1.2.8 Подмножество счётного множества конечно или счётного

Если $A \subset \mathbb{N}$, то множество A конечно или счётно

Доказательство.

Согласно теореме о рекурсии и принципу наименьшего числа, существует функция $\alpha : \mathbb{N} \to \mathcal{P}(A)$, т.ч. для всех $n \in \mathbb{N}$ верно

$$\alpha(0) = A$$

$$\alpha(n+1) = \begin{cases} \alpha(n) \setminus \{\min \alpha(n)\}, & \alpha(n) \neq \varnothing \\ \varnothing, & \text{иначе} \end{cases}$$

Легко видеть, что для всех $n \in \mathbb{N}$ верно $\alpha(n+1) \subseteq \alpha(n)$, причём $\alpha(n+1) \subset \alpha(n)$, если $\alpha(n) \neq \varnothing$.

Допустим функция α принимает значение $\varnothing$. Рассмотрим наименьшее n_0, т.ч. $\alpha(n_0) = \varnothing$. Тогда, полагая $f(m) = \min \alpha(m)$ при всех $m \in \underline{n_0}$, имеем функцию $f : \underline{n_0} \to A$. Если же $\alpha(n) \neq \varnothing$ при всех n, условие $f(n) = \min \alpha(n)$ определяет функцию $f : \mathbb{N} \to A$.

Проверим, что в каждом из случаев функция f является инъекцией. Ясно, что $f(n+1) > f(n)$, если $n+1 \in \operatorname{dom} f$. По индукции, отсюда легко получить $f(m) > f(n)$ при условии $m > n$. Если $m \neq n$, то б.о.о. $m > n$, а значит $f(m) \neq f(n)$

Теперь проверим, что f сюръективна. Допустим, что найдётся $a \in A \subset \mathbb{N}$, т.ч. $a \notin \operatorname{rng} f$. Индукцией легко показать, что $a \in \alpha(n)$ для всех $n \in \mathbb{N}$. Но тогда $\alpha(n_0) \neq \varnothing$, и в случае $f : \underline{n_0} \to A$ мы получили желаемое противоречие.

Остался случай $f : \mathbb{N} \to A$. Мы утверждаем, что найдётся $k \in \mathbb{N}$, т.ч. $A \leqslant f(k)$. В самом деле, иначе $f : \mathbb{N} \to \underline{a}$, т.е. $\mathbb{N} \lesssim \underline{a}$, что невозможно. Очевидно, что $a \neq f(k) \in \operatorname{rng} f$. Значит $a < f(k) = \min \alpha(k)$. С другой стороны, $a \in \alpha(k)$. Противоречие.

Итак, мы доказали, что f - биекция, причём в случае $\underline{n_0} \overset{f}{\sim} A$ множество A конечно, и счётно в случае $\mathbb{N} \overset{f}{\sim} A$.

1.2.9 Правила суммы и произведения. Мощность объединения конечных множеств. Мощность степени и образа конечного множества.

Правила суммы и произведения

Правило суммы Пусть множества A и B конечны и $A \cap B = \varnothing$. Тогда множество $A \cup B$ тоже конечно, причём $|A \cup B| = |A| + |B|$.

Доказательство.

Допустим, что $A \overset{f}{\sim} \underline{n}, B \overset{g}{\sim} \underline{m}$. Определим биекцию $h : A \cup B \to \underline{n+m}$, полагая

$$h(x) = \begin{cases} f(x), & x \in A \\ n + g(x), & x \in B \end{cases}$$

В силу $A \cap B = \varnothing$, действительно, получается функция, причём, очевидно, $h(x) < n+m$. Пусть $h(x) = h(y)$. Если $x, y \in A$, то $x = y$ по инъективности f. Если же $x, y \in B$, имеем $n + g(x) = n + g(y)$, откуда $g(x) = g(y)$ в силу свойств сложения и $x = y$ по инъективности g. Теперь допустим, то $x \in A, y \in B$. Имеем $h(x) = f(x) < n \leqslant n + g(y) = h(y)$, что противоречит $h(x) = h(y)$. Итак, функция h инъективна.

Установим сюръективность. Пусть $k \in \underline{n+m}$. Тогда $k < n$ или $n \leqslant k < n+m$. В первом случае $k = f(x) = h(x)$ для некоторого $x \in A$ в силу сюръективности f. Во втором - по свойствам сложения замечаем, что $k = n + k'$ для некоторого $k' < m$. По сюръективности g найдётся $y \in B$, т.ч. $k' = g(y)$, но тогда $k = n + g(y) = h(y)$.

Правило произведения Пусть множества A и B конечны. Тогда множество $A \times B$ тоже конечно, причём $|A \times B| = |A| \cdot |B|$.

Доказательство.

Пусть $A \overset{f}{\sim} \underline{n}, B \overset{g}{\sim} \underline{m}$. Если $m = 0$, то $B = \varnothing$ и $A \times B = \varnothing \sim \underline{0}$. Пусть $m \neq 0$. Укажем биекцию $h: A \times B \to \underline{nm}$. Именно, положим

$$h(x, y) = mf(x) + g(y)$$

для всех $x \in A, y \in B$.

Из арифметики известна теорема о делении с остатком, согласно которой, для любых натуральных $u, v \neq 0$ существует единственная пара $(q, r) \in \mathbb{N}^2$, т.ч. $u = vq + r, r < q$.

Проверим сюръективность функции h. Пусть $z \in \underline{nm}$. Тогда $z = mq + r$ для некоторых $q \in \mathbb{N}, r \in \underline{m}$. Значит, найдётся $y \in B$, т.ч. $r = g(y)$. Также $q \in \underline{n}$, поскольку иначе $z \geqslant nm$; поэтому наёдётся и $x \in A$, для которого $q = f(x)$. Итак, $z = mf(x) + g(y) = h(x, y)$

Проверим инъективность. Пусть $mf(x)+g(y) = mf(x')+g(y') = z = mq+r$. Поскольку $g(y), g(y') < m$, по теореме о делении с остатком имеем $g(y) = g(y')$ и, учитывая свойства сложения и умножения, $f(x) = f(x')$. Тогда получаем $x = x', y = y'$ по инъективности f и g.

Мощность объединения конечных множеств

Мощность объединения Если множества A и B конечны, то множество $A \cup B$ тоже конечно, причём $|A \cup B| = |A| + |B| - |A \cap B|$.

Доказательство.

Имеем $A = (A \setminus B) \cup (A \cap B), A \cup B = (A \setminus B) \cup B$. Множества $A \setminus B, A \cap B \subseteq A$ конечны. Множество $A \setminus B$ не пересекается ни с $A \cap B$, ни с B. Поэтому $|A| = |A \setminus B| + |A \cap B|$, и для конечного $A \cup B$ получаем

$$|A \cup B| = |A \setminus B| + |B| = (|A| - |A \cap B|) + |B| = |A| + |B| - |A \cap B|$$

Ограничение мощности объединения конечных множеств Если множества A и B конечны, то $|A \cup B| \leqslant |A| + |B|$

Обобщение на объединение n конечных множеств Результат мощности объединения двух конечных множеств нетрудн обобщить на объединение трёх множеств (представим $A \cup B \cup C = (A \cup B) \cup C$)

Дальнейшее обобщение с помощью индукции по $n \geqslant 2$ даёт для конечных множеств $A_1, \ldots, A_n$ важный принцип включений-исключений:

$$|A_1 \cup \cdots \cup A_n| = \sum_{1 \leqslant i_1 \leqslant n} |A_{i_1}| - \sum_{1 \leqslant i_1 < i_2 \leqslant n} |A_{i_1} \cap A_{i_2}| + \cdots + (-1)^{n-1} |A_1 \cap \cdots \cap A_n|$$

Мощность степени и образа конечного множества

Мощность степени конечного множества Если множество A конечно, то при любом $n \in \mathbb{N}$ множество A^n тоже конечно, причём $|A^n| = |A|^n$

Доказательство.

Индукция по n с учётом $A^{n+1} \sim A^n \times A$ при $n \geqslant 1$.

Мощность образа конечного множества Пусть $f : A \to B$ и множество A конечно. Тогда множество $f[A]$ тоже конечно, причём $|f[A]| \leqslant |A|$.

Доказательство.

Проведём индукцию по $n = |A|$. Если $|A| = 0$, то $A = \varnothing$, откуда $f = \varnothing, f[A] = \varnothing$. Пусть $|A| = n + 1$. Рассмотрим некоторый $x \in A$ и положим $A' = A \setminus \{x\}$. По правилу сложения $|A'| = n$, а значит, по предположению индукции для функции $f' = f \restriction A'$ имеем $|f'[A']| \leqslant |A'|$. С другой стороны $f[A] = f'[A'] \cup \{f(x)\}$, откуда $|f[A]| \leqslant |f'[A']| + |\{x\}| \leqslant n+1$

1.2.10 Множество $\mathbb{N}$ вкладывается в каждое бесконечное множество. (допустимо неформальное доказательство, но применение (некоторой формы) аксиомы выбора нужно чётко обозначить)

Принцип зависимого выбора Пусть множество A непусто и отношение $R \subseteq A^2$ таково, что для всякого $a \in A$ найдётся $b \in A$, т.ч. aRb. Тогда существует функция $f : \mathbb{N} \to A$, т.ч. $f(n)Rf(n+1)$ для всех $n \in \mathbb{N}$

Теорема о вложении $\mathbb{N}$ Если множество A бесконечно, то $\mathbb{N} \leqslant A$.

Неформальное доказательство.

Рассмотрим множество F всех индукций из $\underline{n}$ в A. Определим транизитивное отношение $R \subseteq F^2$, т.ч. gRf, если f продолжает функцию g.

$\varnothing \in F \neq \varnothing$, а также любую функцию $f : \underline{n} \to A$ мы можем продолжить до $g : \underline{n+1} \to A$.

Согласно принципу зависимого выбора, существует $\varphi : \mathbb{N} \to F$, т.ч. $\varphi(n)R\varphi(n+1)$ при всех $n \in \mathbb{N}$. Учтя тразитивность R, индукцией легко показать, что $\varphi(n) \restriction \operatorname{dom} \varphi(m) = \varphi(m)$ при $m \leqslant n$. Также по индукции проверим, что $\underline{n} \subseteq \operatorname{dom} \varphi(m)$.

Положим $h = \bigcup \varphi[\mathbb{N}]$. Нетрудно проверить, что это отношение функционально, тотально и инъективно.

1.2.11 Конечное или счётное объединение конечных или счётных множеств конечно или счётно (допустимо неформальное доказательство, но применение (некоторой формы) аксиомы выбора нужно чётко обозначить)

Пусть множество A конечно или счётно и каждое множество $X \in A$ конечно или счётно. Тогда множество $\bigcup A$ тоже конечно или счётно.

Неформальное доказательство.

Можно занумеровать каждый элемент $a \in \bigcup A = \bigcup\{X_0, X_1, \dots\}$ парой чисел $(m, n) \in \mathbb{N}^2$, где $a = a^m_n \in X_m = \{a^m_0, a^m_1, \dots\}$. Число m берём наименьшим подходящим, но аксиома счётного выбора всё же потребуется, ибо присвоить натуральные номера элементам множества X_m можно по-разному, нам нужно зафиксировать такие нумерации для всех $\mathbb{N}$ сразу.

1.2.12 Фундированные порядки. Принцип индукции. Равносильность условия фундированности, конечности убывающих цепей и принципа индукции.

Пусть $(X, <)$ ч.у.м. Тогда следующие условия равносильны.

1. Порядок $<$ фундирован.
2. Не существует бесконечной убывающей цепи элементов $X: x_0 > x_1 > \cdots > x_n > \ldots$
3. Если $Z \subseteq X$, то $Prog(Z) \to \forall x \in X\ (x \in Z)$ или иначе

$$Prog(Z) \to Z = X$$

Доказательство.

Равносильность первых двух пунктов почти очевидна. Впрочем, вывод существования бесконечной убывающей последовательности из нефундированности, строго говоря, использует принцип зависимого выбора: для каждого элемента, раз он не минимальный в некотором подмножестве, можно выбрать меньший - значит, есть и бесконечная последовательность таких выборов, которая, собственно, определяет нашу цепь.

Покажем, что третий пункт - принцип трансфинитной индукции - равносилен фундированности. Действительно, допустим $Prog(Z)$ и $Z \neq X$. Тогда множество $A = X \setminus Z \subseteq X$ непусто. В нём есть минимальный элемент $x' \in A$, т.ч. $\forall a \in A\ \neg(a < x')$. Значит, для любого $y \in X$ если $y < x'$, то $y \notin A$ и $y \in Z$. Иными словами, $\forall y < x'\ (y \in Z)$. По прогрессивности заключаем, что не так.

Обратно, пусть есть множество $A \subseteq X$, не имеющее минимальных элементов. Возьмём $Z = X \setminus A$. Проверим "индукционный переход т.е. установим $Prog(Z)$. Предположим противное: $\forall y < x\ (y \in X \setminus A)$ и $x \notin X \setminus A$ для некоторого $x \in X$. Получается, что $\forall y < x\, (y \notin A)$ и $x \in A$, т.е. x минимален в A, что не так. Поэтому $Prog(Z)$ и, по принципу трансфинитной индукции, $Z = X$, т.е. $A = \varnothing$.

1.2.13 Теорема о сравнимости в.у.м.

Определение Для в.у.м. $(X, <)$ и $y \in X$ обозначим собственный н.о. $\{z \mid z < y\}$ через X_y.

Теорема о сравнимости Пусть имеются в.у.м. $(A, <_A)$ и $(B, <_B)$. Тогда выполнено ровно одно из трёх:

1. $A \cong B$
2. $A \cong B_y$ для некоторого $y \in B$
3. $B \cong A_x$ для некоторого $x \in A$

Доказательство.

Рассмотрим отношение (являющееся множеством, как подмножество $A \times B$)

$$f = \{(x, y) \in A \times B \mid A_x \cong B_y\}$$

Это отношение является биекцией из какого-то $D \subseteq A$ в $R \subseteq B$. Действительно, возьмём $D = \{x \mid \exists y\ (x, y) \in f\}$. Проверим функциональность. Пусть $(x, y_1), (x, y_2) \in f$. Тогда

$A_x \cong B_{y_1}$ и $A_x \cong B_{y_2}$, откуда $B_{y_1} \cong B_{y_2}$. Но одно из этих множество есть н.о. другого. Согласно лемме, в.у.м. не может быть изоморфным своему н.о., поэтому $y_1 = y_2$. Аналогично проверим инъективность.

Функция f монотонна. Действительно, пусть $A_{x_1} \overset{\psi}{\cong} B_{y_1}, A_{x_2} \overset{\varphi}{\cong} B_{y_2}$ и $x_1 <_A x_2$. Предположим, что $y_1 \geqslant_B y_2$. Образ $\varphi(A_{x_1})$ является собственным н.о. множества B_{y_2}, а, следовательно, и B_{y_1}. Этот н.о. под действием изоморфизма ψ^{-1} переходит в собственный н.о. A_{x_1}. Таким образом, A_{x_1} изоморфно собственному н.о. $\psi^{-1}(\varphi(A_{x_1}))$ множества A_{x_1}, что невозможно по какой-то лемме. Значит $y_1 <_B y_2$.

Итак, мы получили изоморфизм $D \overset{f}{\cong} R$. Если $D = A$ и $R = B$, то $A \cong B$ и всё доказано.

Покажем, что R есть н.о. множества B. В самом деле, пусть $y_1 <_B y_2, y_2 \in R$. Тогда найдётся $x_2 \in A$, т.ч. $f(x_2) = y_2$, т.е. $A_{x_2} \overset{\varphi}{\cong} B_{y_2}$. Образом собственного н.о. B_{y_1} при изоморфизме φ^{-1} будет собственный н.о. $\varphi^{-1}(B_{y_1})$ множества A_{x_2}, который в силу леммы о строении каждого с.н.о., равен A_{x_1} для некоторого $x_1 <_A x_2$. Получаем $A_{x_1} \overset{\varphi}{\cong} B_{y_1}$, т.е. $f(x_1) = y_1, y_1 \in R$. Аналогично доказывается, что D есть н.о. множества A.

Допустим, что $R \neq B$ и $D \neq A$. Тогда по лемме о строении н.о. $R = B_{y'}$ для некоторого $y' \in B$. Равно, $D = A_{x'}$ для какого-то $x' \in A$. Тогда $(x', y') \in f$ и $y' \in R$, что не так.

Поэтому возможен лишь случай, когда R собственный н.о. множества B, а $D = A$, и симметричный ему. Эти случаи соответствуют случаям 2 и 3 из условия.

Остаётся понять, почему случаи 1, 2, 3 попарно несовместимы. Ответ даёт лемма, что в.у.м. не может быть изоморфно своему с.н.о.

1.2.14 Теоремы о вычитании и о делении с остатком в.у.м.

Теорема о вычитании в.у.м. Пусть $A \geqslant B$. Тогда существует единственное с точностью до изоморфизма множество C, т.ч. $B + C \cong A$

Доказательство.

Имеем $B \overset{f}{\cong} [0_A, a)$ для $a \in A$. Рассмотрим в.у.м. $C = \{x \in A \mid x \geqslant a\}$. Отображение $(b, 0) \mapsto f(b)$ для $b \in B, (c, 1) \mapsto c$ для $c \in C$, очевидно, осуществляет искомый изоморфизм.

Пусть найдутся C_1, C_2, т.ч. $C + C_1 \cong B + C_2$, причём $C_1 \ncong C_2$. Тогда множества C_1, C_2 сравнимы. Пусть, б.о.о. $C_1 < C_2$. Тогда по лемме о свойствах сложения в.у.м. $B + C_1 < B + C_2$. Противоречие.

Теорема о делении с остатком в.у.м. Пусть в.у.м. $B \neq \varnothing$ (эквивалентно, $B \geqslant 1$). Тогда для любого в.у.м. A существует единственные с точностью до изоморфизма в.у.м. C и $R < B$, т.ч. $BC + R \cong A$.

Доказательство.

Рассмотрим в.у.м. $X = B(A + 1)$. В силлу леммы о свойствах умножения в.у.м. имеем $A < A + 1 \leqslant B(A + 1)$. Поэтому $A \cong [0_X, (b, \alpha))$, где $b \in B$. По определению произведения в.у.м. $(b', \alpha') <_X (b, \alpha) \Leftrightarrow (\alpha' < \alpha) \vee (\alpha' = \alpha \wedge b' <_B b)$. Поэтому, как легко видеть,

$$[0_X, (b, \alpha)) \cong B[0_{A+1}, \alpha) + [0_B, b)$$

Остаётся положить $C = [0_{A+1}, \alpha), R = [0_B, b) < B$

Проверим однозначность. Пусть $BC_1 + R_1 \cong BC_2 + R_2$. Если $C_1 \cong C_2$, то $R_1 \cong R_2$. В противном случае, б.о.о., $C_1 < C_2$. Тогда найдётся D, т.ч. $C_2 \cong C_1 + D$. Ясно, что $D \neq \varnothing$, т.е. $D \geqslant 1$. Имеем

$$BC_1 + R_1 \cong BC_1 + BD + R_2$$

По лемме о левом сокращении, $BD + R_2 \cong R_1$. Но $R_1 < B$, а $BD + R_2 \geqslant B + R_2 \geqslant B$. Противоречие.

1.2.15 Теорема о сравнении множеств по мощности. Мощность объединения двух бесконечных множеств.

Теорема о сравнении множеств по мощности Если A бесконечно, то множество $A \times \mathbb{N}$ равномощно A.

Доказательство.

Вполне упорядочим множество A. Всякий элемент A однозначно представим в виде $z+n$, где z - предельный элемент, а n - натуральное число. Это означает, что A равномощно $B \times \mathbb{N}$.

Теперь утверждение теоремы очевидно: $A \times \mathbb{N} \sim (B \times \mathbb{N}) \times \mathbb{N} \sim A \times (\mathbb{N} \times \mathbb{N}) \sim A \times \mathbb{N}$.

По теореме Кантора-Берштейна отсюда следует, что промежуточные мощности (любое произведение A и конечного множества) совпадают с $|A|$

Мощность объединения двух бесконечных множеств Сумма двух бесконечных мощностей равна их максимуму.

Доказательство.

Пусть, скажем $|A| \leqslant |B|$. Тогда $|B| \leqslant |A| + |B| \leqslant |B| + |B| \leqslant |B \times \mathbb{N}| = |B|$. Остаётся воспользоваться теоремой Кантора-Берштейна и заключить, что $|B| = |A + B|$.

2 Логика

2.1 Вопросы на удос

2.1.1 Структуры и сигнатуры. Нормальные структуры. Изоморфизм структур

Структуры и сигнатуры

Структура Структура $\mathcal{M} := (M, \mathcal{R}, \mathcal{F}, \mathcal{C})$, где

- $M \neq 0$ - носитель структуры
- $\forall f \in \mathcal{F}\ \exists n \in \mathbb{N}\ f:\ M^n \to M$
- $\forall R \in \mathcal{R}\ \exists n \in \mathbb{N}\ R \subseteq M^n$
- $\forall c \in \mathcal{C}\ c \in M$

Пример: $(\mathbb{N}, \{=, <\}, \{+, \cdot\}, \{0, 1\})$

Сигнатуры $\sigma = (Rel_\sigma, Func_\sigma, Const_\sigma)$, причём $Rel_\sigma \neq \varnothing$ и все они не пересекаются.

- Каждому $R \in Rel_\sigma$ и каждому $f \in Func_\sigma$ поставлено в соответствие натуральное число, оно называется валентностью символа R (или f). Пишем $R^{(n)}$, $f^{(n)}$

Интерпретация структуры Интерпретация сигнатуры σ - это пара $(\mathcal{M}, \mathcal{S})$, где

- $\mathcal{M}$ - структура $(M, \mathcal{R}, \mathcal{F}, \mathcal{C})$
- $\mathcal{S}: \; Rel_\sigma \cup Fnc_\sigma \cup Const_\sigma \to \mathcal{R} \cup \mathcal{F} \cup \mathcal{C}$, причём
  1. $\forall R^{(n)} \in Rel_\sigma \; \mathcal{S}(R) \in \mathcal{R} \wedge \mathcal{S}(R) \subseteq M^n$
  2. $\forall f^{(n)} \in Fnc_\sigma \; \mathcal{S}(f) \in \mathcal{F} \wedge \mathcal{S}(f): \; M^n \to M$
  3. $\forall c \in Const_\sigma \; \mathcal{S}(c) \in \mathcal{C}$

Нормальные структуры Если сигнатура включает в себя символ равенства, то среди её интерпретаций выделяют нормальные интерпретации, в которых символ равенства интерпретируется, как совпадение элементов.

Изоморфизм структур Пусть M_1 и M_2 - две интерпретации сигнатуры σ. Биекция (взаимно однозначное отображение) $\alpha: \; M_1 \to M_2$ называется изоморфизмом этих интерпретаций, если она сохраняет все функции и предикаты структуры. Это означает, если P_1 и P_2 - два k-местных предиката в M_1 и M_2, соответствующих одному предикатному символу сигнатуры, то для всех $a_1, \ldots, a_k \in M_1$:

$$P_1(a_1, \ldots, a_k) = P_2(\alpha(a_1), \ldots, \alpha(a_k))$$

Аналогичное утверждение для функций: если k-местные функции f_1 и f_2 соответствуют одному функциональному символу, то для всех $a_1, \ldots, a_k \in M_1$:

$$\alpha(f_1(a_1, \ldots, a_k)) = f_2(\alpha(a_1), \ldots, \alpha(a_k))$$

2.1.2 Формулы первого порядка данной сигнатуры. Параметры (свободные переменные) формулы. Предложения

Формулы первого порядка данной сигнатуры

Множество переменных Мы считаем, что задано счётное множество индивидных, или предметных переменных

$$Var = \{x_0, x_1, \ldots, x_n, \ldots\}$$

Множество термов Правила построения множества термов Tm_σ над сигнатурой σ:

1. $x \in Var \Rightarrow x \in Tm_\sigma$
2. $c \in Const_\sigma \Rightarrow c \in Tm_\sigma$
3. $f^{(n)} \in Fnc_\sigma \Rightarrow ft_1 \ldots t_n \in Tm_\sigma$, где $t_1, \ldots, t_n \in Tm_\sigma$

Множество формул Правила построения множества формул Fm_σ над сигнатурой σ:

1. $R^{(n)} \in Rel_\sigma \wedge t_1, \ldots, t_n \in Tm_\sigma \Rightarrow Rt_1 \ldots t_n \in Fm_\sigma$ - такие формулы называются атомарными
2. $\varphi, \psi \in Fm_\sigma \Rightarrow \neg\varphi \in Fm_\sigma, (\varphi \wedge \psi) \in Fm_\sigma, (\varphi \vee \psi) \in Fm_\sigma, (\varphi \to \psi) \in Fm_\sigma, \ldots$
3. $x \in Var \wedge \varphi \in Fm_\sigma \Rightarrow \forall x\varphi \in Fm_\sigma, \exists x\varphi \in Fm_\sigma$

Параметры (свободные переменные) формулы

Переменные формулы или терма Пусть $V: Tm_\sigma \cup Fm_\sigma \to \mathcal{P}(Var)$, причём

1. $x \in Var \Rightarrow V(x) = \{x\}$
2. $c \in Cnst_\sigma \Rightarrow V(c) = \varnothing$
3. $V(ft_1 \dots t_n) = \bigcup\limits_{i=1}^{n} V(t_i)$
4. $V(Rt_1 \dots t_n) = \bigcup\limits_{i=1}^{n} V(t_i)$
5. $V(\varphi \wedge \psi) = V(\varphi) \cup V(\psi)$
6. $V(\forall x \varphi) = V(\varphi) \cup \{x\}$

Свободные переменные формулы Пусть $FV: Fm_\sigma \to \mathcal{P}(Var)$, причём

1. $FV(Rt_1 \dots t_n) = V(Rt_1 \dots t_n)$
2. $FV(\varphi \vee (\wedge)(\to)\psi) = FV(\varphi) \cup FV(\psi)$
3. $FV(\forall(\exists)x\, \varphi) = FV(\varphi) \setminus \{x\}$

Предложения $St_\sigma = \{\varphi \in Fm_\sigma \mid FV(\varphi) = \varnothing\}$

2.1.3 Оценка переменных. Значение терма и формулы в данной структуре при данной оценке. Независимость значения формулы от значения переменных, не являющихся её параметрами.

Оценка переменных Оценка переменных (в $\mathcal{M}$) - это любая функция $\pi: Var \to M$

Значение терма и формулы в данной структуре при данной оценке

Значение терма $t \in Tm_\sigma, \pi$ - оценка. Тогда $[t]_{\mathcal{M}}(\pi) \in M$ - значение t в $\mathcal{M}$ при оценке π, причём

1. $x \in Tm_\sigma \Rightarrow [x](\pi) = \pi(x)$
2. $c \in Cnst_\sigma \Rightarrow [c](\pi) = c^{\mathcal{M}}$
3. $[ft_1 \dots t_n](\pi) = f^{\mathcal{M}}([t_1](\pi), \dots, [t_n](\pi))$

Значение формулы $\varphi \in Fm_\sigma, \pi$ - оценка. $\{0,1\} \ni [\varphi]_{\mathcal{M}}(\pi)$ - значение формулы φ в $\mathcal{M}$ при оценке π, причём

1. $[Rt_1 \dots t_n](\pi) = 1 \Leftrightarrow ([t_1](\pi), \dots, [t_n](\pi)) \in R^{\mathcal{M}}$
2. $[\varphi \to (\dots)\psi](\pi) = 1 \Leftrightarrow [\varphi](\pi) \to (\dots)[\psi](\pi)$
3. $[\forall x\, \varphi](\pi) = 1 \Leftrightarrow \forall a \in M\ [\varphi](\pi^a_x) = 1$, где
$$\pi^a_x(y) = \begin{cases} a, & y = x \\ \pi(y), & y \neq x \end{cases}$$
4. $[\exists x\, \varphi](\pi) = 1 \Leftrightarrow \exists a \in M\ [\varphi](\pi^a_x) = 1$

Независимость значения формулы от значений переменных, не являющихся её параметрами Пусть π_1 и $\pi_2 : Var \to M$

1. $(\forall x \in V(t)\ \pi_1(x) = \pi_2(x)) \Rightarrow [t](\pi_1) = [t](\pi_2)$
2. $(\forall x \in FV(\varphi)\ \pi_1(x) = \pi_2(x)) \Rightarrow [\varphi](\pi_1) = [\varphi](\pi_2)$

Доказательство.

1. Индуккция по построению t.
   - $t := x \in Var\ [x](\pi_1) = \pi_1(x) \overset{x \in V(t)}{=} \pi_2(x) = [x](\pi_2)$
   - $t := c \in Cnst_\sigma\ [c](\pi_1) = C^{\mathcal{M}} = [c](\pi_2)$
   - $t := ft_1 \dots t_n\ [ft_1 \dots t_n](\pi) = f^{\mathcal{M}}([t_1](\pi_1), \dots, [t_n](\pi_1)) \overset{\text{по индукции}}{=} f^{\mathcal{M}}([t_1](\pi_2), \dots, [t_n](\pi_2)) = [ft_1 \dots t_n](\pi_2)$
2. Индукция по построению φ
   - $\varphi = Rt_1 \dots t_n\ [Rt_1 \dots t_n](\pi_1) = 1 \Leftrightarrow ([t_1](\pi_1), \dots, [t_n](\pi_1)) \in R^{\mathcal{M}} \overset{\text{по п.1}}{\Leftrightarrow} ([t_1](\pi_2), \dots, [t_n](\pi_2)) \in R^{\mathcal{M}} \Leftrightarrow [Rt_1 \dots t_n](\pi_2) = 1$
   - $\varphi = \psi \wedge \theta, FV(\varphi) = FV(\psi) \cup FV(\theta)\ [\psi \wedge \theta](\pi_1) = [\psi](\pi_1) \wedge [\theta](\pi_1) \overset{\text{ПИ}}{=} [\psi](\pi_2) \wedge [\theta](\pi_2) = [\psi \wedge \theta](\pi_2)$
   - $[\forall x \psi](\pi_1) = 1 \Leftrightarrow \forall a \in M\ [\psi](\pi^a_{1\,x}) = 1 \Leftrightarrow \forall a \in M\ [\psi](\pi^a_{2\,x}) = 1 \Leftrightarrow [\forall x\, \psi](\pi_2) = 1$

2.1.4 Значение терма и формулы на наборе элементов структуры. Выразимые в структуре множества (отношения, функции, элементы). Примеры выразимых множеств.

Значение терма и формулы на наборе элементов структуры

Определения

$$Fm_\sigma(x_1, \dots, x_n) = \{\varphi \in Fm_\sigma \mid FV(\varphi) \subseteq \{x_1, \dots, x_n\}\}$$

$$Tm_\sigma(x_1, \dots, x_n) = \{t \in Tm_\sigma \mid V(t) \subseteq \{x_1, \dots, x_n\}\}$$

Человеческое обозначение значения терма и формулы Пусть $t \in Tm_\sigma(x_1, \ldots, x_n), \vec{a} = (a_1, \ldots, a_n) \in M^n$. Тогда $[t]_\mathcal{M}(\vec{a}) := [t]_\mathcal{M}(\pi^{a_1 a_2 \ldots a_n}_{x_1 x_2 \ldots x_n})$.

Аналогично, $[\varphi]_\mathcal{M}(\vec{a}) := [\varphi]_\mathcal{M}(\pi^{a_1 \ldots a_n}_{x_1 \ldots x_n})$

Выразимые в структуре множества (отношения, функции, элементы)

Выразимые отношения Отношение $X \subseteq M^n$ выразимо в σ-структуре $\mathcal{M} \Leftrightarrow \exists X \in Fm_\sigma(x_1, \ldots, x_n)\ \varphi^\mathcal{M} = X$

Выразимые функции Функция $f : M^n \to M$ выразима в σ- структуре $\mathcal{M} \Leftrightarrow \exists t \in Tm_\sigma(x_1, \ldots, x_n)\ t^\mathcal{M} = f$

Выразимое множество Множество $X \subseteq M$ выразимо в σ-структуре $\mathcal{M}$, если существует выразимое отношение $Y \subseteq M$, т.ч. $\forall x\ x \in X \Leftrightarrow x \in Y^\mathcal{M}$

Пример выразимых множеств $\mathcal{M} = (\mathbb{Z}, =, +)$, выразим $X =$ все чётные числа. a чётно $\Leftrightarrow [\varphi]_\mathcal{M}(a) = 1$, где $\varphi(x) := \exists y\ x = y + y$.

2.1.5 Значение формулы при изоморфизме структур. Элементарная эквивалентность структур. Изоморфные структуры элементарно эквивалентны.

Значение формулы при изоморфизме структур Пусть $\mathcal{M}, \mathcal{N}$ - σ-структуры и $\mathcal{M} \overset{\alpha}{\cong} \mathcal{N}$. Пусть $t \in Tm_\sigma(\vec{x}), \varphi \in Fm_\sigma(\vec{x})$. Тогда

1. $\forall \vec{a}\ ([t]_\mathcal{M}(\vec{a})) = [t]_\mathcal{N}(\alpha\vec{a})$
2. $\forall \vec{a}\ [\varphi]_\mathcal{M}(\vec{a}) = [\varphi]_\mathcal{N}(\alpha\vec{a})$

Доказательство.

1. Индукция по построению t
   - $t := x_i \in Var\ \alpha([x_i]_\mathcal{M}(\vec{a})) = \alpha a_i = [x_i]_\mathcal{N}(\alpha\vec{a})$
   - $t := c \in Cnst_\sigma\ \alpha([c]_\mathcal{M}(\vec{a})) = \alpha c^\mathcal{M} = c^\mathcal{N} = [c]_\mathcal{N}(\alpha\vec{a})$
   - $t := ft_1 \ldots t_n\ \alpha([ft_1 \ldots t_n]_\mathcal{M}(\vec{a})) = \alpha(f^\mathcal{M}([t_1]_\mathcal{M}(\vec{a}), \ldots, [t_n]_\mathcal{M}(\vec{a})))$
     $= f^\mathcal{N}(\alpha([t_1]_\mathcal{M}(\vec{a})), \ldots, \alpha([t_n]_\mathcal{M}(\vec{a})) \overset{\text{ПИ}}{=} f^\mathcal{N}([t_1]_\mathcal{N}(\alpha\vec{a}), \ldots, [t_n]_\mathcal{N}(\alpha\vec{a})) = [ft_1 \ldots t_k]_\mathcal{N}(\alpha\vec{a})$
2. Индукция по построению φ
   - $\varphi := Rt_1 \ldots t_n\ [Rt_1 \ldots t_n](\alpha\vec{a}) = 1 \Leftrightarrow ([t_1]_\mathcal{N}(\alpha\vec{a}), \ldots, [t_n]_\mathcal{N}(\vec{a})) \in R^\mathcal{N} \Leftrightarrow$
     $(\alpha([t_1]_\mathcal{M}(\vec{a})), \ldots, \alpha([t_n]_\mathcal{M}(\vec{a}))) \in R^\mathcal{N} \Leftrightarrow ([t_1]_\mathcal{M}(\vec{a}), \ldots, [t_n]_\mathcal{M}(\vec{a})) \in R^\mathcal{M} \Leftrightarrow [Rt_1 \ldots t_n]_\mathcal{M}(\vec{a}) = 1$
   - $\varphi := \psi \to \theta\ [\psi \to \theta]_\mathcal{N}(\alpha\vec{a}) = [\psi]_\mathcal{N}(\alpha\vec{a}) \to [\theta]_\mathcal{N}(\alpha\vec{a}) = [\psi]_\mathcal{M}(\vec{a}) \to [\theta]_\mathcal{M}(\vec{a}) = [\psi \to \theta]_\mathcal{M}(\vec{a})$
   - $\varphi := \exists x\ \psi\ [\exists x\ \psi]_\mathcal{M}(\vec{a}) = 1 \Leftrightarrow \exists b \in M\ [\psi]_\mathcal{M}(\vec{a}, \overset{x}{b}) = 1 \Leftrightarrow \exists b \in M\ [\psi]_\mathcal{N}(\alpha\vec{a}, \overset{x}{\alpha b}) \Rightarrow$
     $[\exists x\ \psi]_\mathcal{N}(\alpha\vec{a}) = 1 \Rightarrow \exists c \in N\ [\psi]_\mathcal{N}(\alpha\vec{a}, \overset{x}{c}) = 1 \overset{\alpha\ \text{сюр.}}{\Rightarrow} (\exists b \in M\ c = \alpha b)\ [\psi]_\mathcal{N}(\alpha\vec{a}, \alpha\vec{b}) =$
     $1 \Rightarrow [\exists x\ \psi]_\mathcal{M}(\vec{a}) = 1$

Элементарная эквивалентность структур Две σ-структуры $\mathcal{M}, \mathcal{N}$ элементарно эквивалентны $\Leftrightarrow \forall \varphi \in St_\sigma$

$$\mathcal{M} \vDash \varphi \Leftrightarrow \mathcal{N} \vDash \varphi$$

Обозначение $\mathcal{M} \equiv \mathcal{N}$

Изоморфные структуры элементарно эквивалентны $\mathcal{M} \cong \mathcal{N} \Rightarrow \mathcal{M} \equiv \mathcal{N}$

Доказательство.

Пусть $\mathcal{M} \overset{\alpha}{\cong} \mathcal{N}, \varphi \in St_\sigma$.

$$\mathcal{M} \vDash \varphi \Leftrightarrow [\varphi]_{\mathcal{M}}(\varnothing) = 1 \Leftrightarrow [\varphi]_{\mathcal{N}}(\alpha\varnothing) = 1 \Leftrightarrow \mathcal{N} \vDash \varphi$$

2.1.6 Значение формулы при изоморфизме структур. Сохранение выразимых множеств автоморфизмами структуры. Примеры невыразимых множеств.

Сохранение выразимых множеств автоморфизмами структур

Определение $Aut(\mathcal{M}) = \{\alpha \mid \mathcal{M} \overset{\alpha}{\cong} \mathcal{M}\}$

Сохранение выразимости автоморфизмами Если X выразимо в $\mathcal{M}$, то $\forall \alpha \in Aut(\mathcal{M})\, \forall \vec{a} \in M^n\ (\vec{a} \in X \Leftrightarrow \alpha\vec{a} \in X)$

Доказательство.

Пусть $\varphi(\vec{x})$ выражает X в $\mathcal{M}$, т.е. $\vec{a} \in X \Leftrightarrow [\varphi]_{\mathcal{M}}(\vec{a}) = 1 \Leftrightarrow [\varphi]_{\mathcal{M}}(\alpha\vec{a}) = 1 \Leftrightarrow \alpha\vec{a} \in X$

Примеры невыразимых множеств Пусть $\mathcal{M} = (\mathbb{Z}, =, +)$, в $\mathcal{M}$ НЕвыразимо $\mathbb{Z}_+$, т.к. существует автоморфизм $\alpha:\ n \mapsto -n$.

2.1.7 Эквивалентность формул первого порядка. Лемма о фиктивном кванторе. Общезначиивые и выполнимые формулы. Квантор всеобщности и общезначимость.

Эквивалентность формул первого порядка.

Определение Формулы φ и ψ называются эквивалентными (обозначение: $\varphi \equiv \psi$), если их значения совпадают в любой интерпретации при любой оценке. Или иначе, если общезначима формула $\varphi \leftrightarrow \psi$, т.е. $\varphi \to \psi \vee \psi \to \varphi$.

Отношение эквивалентности

1. $\varphi \equiv \varphi$
2. $\varphi \equiv \theta \vee \theta \equiv \psi \to \varphi \equiv \psi$
3. $\varphi \equiv \psi \to \psi \equiv \varphi$

Таким образом, $\equiv$ действительно определяет некоторое отношение эквивалентности на множестве Fm_σ.

Лемма о фиктивном кванторе Пусть $x \in FV(\varphi)$. Тогда $\varphi \equiv \forall x\, \varphi$.

Доказательство.

Имеем $[\forall x\, \varphi](\pi) = \forall a \in M\, [\varphi](\pi_x^a)$. Поскольку $x \notin FV(\varphi)$, для всех $a \in M$ для всех $y \in FV(\varphi)$ выполнено $\pi_x^a(y) = \pi(y)$. Применяя лемму о значении формулы при изоморфизме структур, заключаем $[\varphi](\pi_x^a) = [\varphi](\pi)$ для всех $a \in M$. Отсюда

$$[\forall x\, \varphi](\pi) = \forall a \in M\, [\varphi](\pi_x^a) = \forall a \in M\, [\varphi](\pi) = [\varphi](\pi)$$

Общезначимые и выполнимые формулы Формула, значение которой равно единице (т.е. она истинна) в любой интерпретации при любой оценке, называется общезначимой. Формула, для которой существует интерпретация и оценка такие, что значение этой формулы равно единице, называется выполнимой.

Квантор всеобщности и общезначимости Формула φ общезначима $\Leftrightarrow$ общезначима формула $\forall y\, \varphi$.

Доказательство.

Рассмотрим произвольную интерпретацию. Если формула φ общезначима, то $[\varphi](\pi) = 1$ для всех оценок π, в частности, для всех оценок вида $\pi_y^{'a}$ для произвольного $a \in M$. Поэтому $[\forall y\, \varphi](\pi') = 1$ для всех π'.

Обратно, пусть общезначима $\forall y \varphi$. Тогда для всех π' и для всех $a \in M$ верно $[\varphi](\pi_y^{'a}) = 1$. Однако, для любой π имеем $\pi = \pi_y^{\pi(y)}$. Поэтому $[\varphi](\pi) = 1$ для всех π.

2.1.8 Булевы комбинации формул. Тавтологии первого порядка.

Булевы комбинации формул Пусть имеется пропозициональная формула $A(p_1, \ldots, p_n)$, не содержащая иных переменных, кроме указанных. Пусть также $\varphi_1, \ldots, \varphi_n$ суть некоторые формулы первого порядка. Тогда формула первого порядка, получаемая заменой p_i на φ_i всюду в формуле $A(p_1, \ldots, p_n)$, обозначается $A(\varphi_1, \ldots, \varphi_n)$. Если $A(p_1, \ldots, p_n)$ тавтология, то формула $A(\varphi_1, \ldots, \varphi_n)$ также называется тавтологией.

Тавтологии первого порядка Всякая тавтология общезначима.

Доказательство.

Напомним, что всякой пропозициональной формуле мы ставили в соответствие булеву функцию, возвращаемую истинностное значение формулы по значению её переменных. Пусть для $A(p_1, \ldots, p_n)$ это функция $f_A : \mathbb{B}^n \to \mathbb{B}$. Индукция по построению формулы $A(p_1, \ldots, p_n)$ показывает, что для любой оценки π

$$[A(\varphi_1, \ldots, \varphi_n)](\pi) = f_A([\varphi_1](\pi), \ldots, [\varphi_n](\pi))$$

Например, в случае $A(p_1, \ldots, p_n) = B_1(p_1, \ldots, p_n) \to B_2(p_1, \ldots, p_n)$ имеем, используя предположение индукции,

$$[A(\varphi_1, \ldots, \varphi_n)](\pi) = [B_1(\varphi_1, \ldots, \varphi_n)](\pi) \to [B_2(\varphi_1, \ldots, \varphi_n)](\pi) =$$

$$f_{B_1}([\varphi_1](\pi), \ldots, [\varphi_n](\pi)) \to f_{B_2}([\varphi_1](\pi), \ldots, [\varphi_n](\pi)) = f_A([\varphi_1](\pi), \ldots, [\varphi_n](\pi))$$

2.1.9 Основные эквивалентности логики первого порядка. Замена подформулы на эквивалентную.

Основные эквивалентности логики первого порядка Для произвольных формул φ и ψ выполнено нижеследующее.

1. Пусть $x \notin FV(\psi)$. Тогда
   (a) $\forall x\,(\varphi \wedge \psi) \equiv \forall x\,\varphi \wedge \psi$
   (b) $\exists x\,(\varphi \wedge \psi) \equiv \exists x\,\varphi \wedge \psi$
   (c) $\exists x\,(\varphi \vee \psi) \equiv \exists x\,\varphi \vee \psi$
   (d) $\forall x\,(\varphi \vee \psi) \equiv \forall\,\varphi \vee \psi$
2. $\forall x\,(\varphi \wedge \psi) \equiv \forall x\,\varphi \wedge \forall x\,\psi$
3. $\exists x\,(\varphi \vee \psi) \equiv \exists x\,\varphi \vee \exists x\,\psi$
4. $\neg\forall x\,\varphi \equiv \exists x\,\neg\varphi$
5. $\neg\exists x\,\varphi \equiv \forall x\,\neg\varphi$

Докажем некоторые из этих эквивалентностей.

П.1a. Предполагаем $x \notin FV(\psi)$. По определению в произвольной интерпретации при всякой оценке π имеем

$$[\forall x\,(\varphi \wedge \psi)](\pi) = \forall a \in M\,[\varphi](\pi^a_x) \wedge [\psi](\pi^a_x)$$

$$[\forall x\,\varphi \wedge \psi](\pi) = (\forall a \in M\,[\varphi](\pi^a_x)) \wedge [\psi](\pi)$$

Поскольку $x \notin FV(\psi)$, то для всех $w \in FV(\psi)$ имеем $\pi(w) = \pi^a_x(w)$, и можем применить лемму о значении формулы на наборе элементов структуры, получая для любых $a \in M$:

$$[\psi](\pi^a_x) = [\psi](\pi)$$

$$[\forall x\,(\varphi \wedge \psi)](\pi) = \forall a \in M\,[\varphi](\pi^a_x) \wedge [\psi](\pi)$$

Разберём возможные случаи. Если $[\psi](\pi) = 0$, то, очевидно,

$$[\forall x\,(\varphi \wedge \psi)](\pi) = 0 = [\forall x\,\varphi \wedge \psi](\pi)$$

Если же $[\psi](\pi) = 1$, то

$$[\forall x\,(\varphi \wedge \psi)](\pi) = \forall a \in M\,[\varphi](\pi^a_x) = [\forall x\,\varphi \wedge \psi](\pi)$$

Мы, таким образом, в произвольной интерпретации для всех оценок π установили $[\forall x\,(\varphi \wedge \psi)](\pi) = [\forall x\,\varphi \wedge \psi](\pi)$

Аналогично доказываются остальные пункты.

Замена подформулы на эквивалентную

Замены в простейших формулах Пусть φ произвольная формула, а $\psi \equiv \psi'$. Тогда выполнено нижеследующее

1. $(\varphi \wedge \psi) \equiv (\varphi \wedge \psi')$
2. $(\varphi \vee \psi) \equiv (\varphi \vee \psi')$
3. $(\varphi \to \psi) \equiv (\varphi \to \psi')$
4. $(\psi \to \varphi) \equiv (\psi' \to \varphi)$
5. $(\varphi \leftrightarrow \psi) \equiv (\varphi \leftrightarrow \psi')$
6. $\neg\psi \equiv \neg\psi'$
7. $\forall x\, \psi \equiv \forall x\, \psi'$
8. $\exists x\, \psi \equiv \exists x\, \psi'$

Доказательство.

Проверка первых шести пунктов тривиальна. Разберём пункт 7 (пункт 8 аналогичен). Рассмотрим произвольную интерпретацию. Имеем, что для всех оценок π' верно $[\psi](\pi') = [\psi'](\pi')$. В частности, для любой оценки π и любого $a \in M$ имеем

$$[\psi](\pi_x^a) = [\psi'](\pi_x^a) \Rightarrow$$

$$[\forall x\, \psi](\pi) = \forall a \in M\ [\psi](\pi_x^a) = \forall a \in M\ [\psi'](\pi_x^a) = [\forall x\, \psi'](\pi)$$

Замена всех вхождений на эквивалентные Пусть $\psi \equiv \psi'$ и формула φ' получена из φ заменой некоторых вхождений подформулы ψ на ψ'. Тогда $\varphi \equiv \varphi'$.

Доказательство.

Очевидно, достаточно рассмотреть случай замены, когда хотя бы одно вхождение есть. Проведём индукцию по построению φ. Рассмотрим лишь один из случаев. Пусть $\varphi := \theta_1 \to \theta_2$. Тогда подформула ψ либо совпадает с φ, и всё доказано, либо рассматриваемое вхождение будет вхождением либо в θ_1, либо в θ_2. Применим к соответствующему θ_i предположение индукции, получив, например $\varphi' := \theta_1' \to \theta_2, \theta_1 \equiv \theta_1'$. Далее используем подходящее утверждение из предыдущей леммы и заключаем $\varphi \equiv \varphi'$.

2.1.10 Переименование связанной переменной (без доказательства). Теорема о предварённой нормальной форме

Переименование связанной переменной Пусть $y \notin V(\varphi)$. Тогда

$$\forall x\, \varphi \equiv \forall y\, \varphi(y/x)$$

где выражение $\varphi(y/x)$ означает результат замены всех свободных вхождений переменной x в формулу φ на y.

Теорема о предварённой нормальной форме

Определени ПНФ Говорят, что формула φ предварённая или пренексная, если

$$\varphi := Q_1 y_1 \dots Q_n y_n \psi$$

где каждый Q_i есть некоторый квантор, а в формуле ψ кванторы отсутствуют вовсе.

Сама теорема Для всякой формулы φ найдётся предварённая формула φ', такая что $\varphi \equiv \varphi'$.

Доказательство.

Проводится индукция по построению формулы φ. Если φ атомарная, то она предварённая. Если φ начинается с квантора, то по предположению индукции заменяем формулу под этим квантором на эквивалентную предварённую. Если φ начинается с отрицания, то по предположению индукции заменяем формулу под отрицанием на эквивалентную предварённую. Затем проносим отрицание вовнутрь, переменяя кванторы. Если в φ главная связка бинарная, то по предположению индукции заменяем каждую из формул под этой связкой на эквивалентную предварённую. Затем переименовываем связанные переменные так, чтобы можно было вынести все кванторы наружу. Выносим их.

2.1.11 Понятие теории первого порядка. Примеры содержательных теорий. Модель теории. Логическое следование

Понятие теории первого порядка Если $T \subseteq St_\sigma$, то T - теория в сигнатуре σ.

Если T - теория и $\varphi \in St_\sigma$, то

$$T \vDash \varphi \Leftrightarrow \forall \mathcal{M}\, (\mathcal{M} \vDash T \Rightarrow \mathcal{M} \vDash \varphi)$$

Примеры содержательных теорий $T_{\text{групп}} = \{\forall x \forall y \forall z\ (x+y)+z = x+(y+z), \forall x\ (0+x = x \wedge x+0 = x), \forall x\ (x+(-x) = 0 \wedge (-x)+x = 0)\}$

$\sigma = (=^{(1)};\ +^{(2)}, -^{(1)};\ 0)$

Нормальная σ-структура $\mathcal{M}$ является группой $\Leftrightarrow \mathcal{M} \vDash T_{\text{групп}}$

Модель теории Модель теории T - это σ-структура, в которой выполняется эта теория.

Логическое следование Формула φ семантически следует из T, если она истинна в любой модели теории T (обозначение $T \vDash \varphi$). Семантическое следование равносильно выводимости. Взяв в качестве φ тождественно ложную формулу $\bot$, приходим к понятиям противоречивости ($T \vdash \bot$) и несовместимости ($T \vDash$, T не имеет моделей). В противоречивой теории выводима любая формула.

2.1.12 Исчисление предикатов с равенством в форме натурального вывода: основные и производные правила. Пример вывода. Выводимость в теории

Исчисление предикатов с равенством в форме натурального вывода: основные и производные правила Отношение $\vdash \subseteq \mathcal{F}\Updownarrow_\sigma \times Fm_\sigma$ определим индуктивно

1. Правило аксиомы (Ax) $\Gamma, \varphi \vdash \varphi$

2. Правило ослабления (W) $\dfrac{\Gamma \vdash \varphi}{\Gamma, \Delta \vdash \varphi}$

3. Правило введения конъюнкции ($\wedge$ I) $\dfrac{\Gamma \vdash \varphi \quad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi}$

4. Правило удаления конъюнкции ($\wedge$ E) $\dfrac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \varphi}$

5. Правило введения дизъюнкции ($\vee$ I) $\dfrac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi}$

6. Правило удаления дизъюнкции ($\vee$ E) $\dfrac{\Gamma, \varphi \vdash \theta \quad \Gamma, \psi \vdash \theta \quad \Gamma \vdash \varphi \vee \psi}{\Gamma \vdash \theta}$

7. Правило введения импликации ($\to$ I) $\dfrac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}$

8. Правило удаления импликации ($\to$ E) $\dfrac{\Gamma \vdash \varphi \quad \Gamma \vdash \varphi \to \psi}{\Gamma \vdash \psi}$

9. Правило удаления отрицания ($\neg$ E) $\dfrac{\Gamma, \neg\varphi \vdash \bot}{\Gamma \vdash \varphi}$

10. Правило введения всеобщности ($\forall$ I) $\dfrac{\Gamma \vdash \varphi(y/x), \text{ где } y \notin FV(\Gamma) \text{ и } (y := x \vee y \notin V(\varphi))}{\Gamma \vdash \forall x\, \varphi}$

11. Правило удаления всеобщности ($\forall$ E) $\dfrac{\Gamma \vdash \forall x\, \varphi, \text{ где } t \text{ -- } x \text{ -- } \varphi}{\Gamma \vdash \varphi(t/x)}$

12. Правило введения существования ($\exists$ I) $\dfrac{\Gamma \vdash \varphi(t/x), \text{ где } t \text{ -- } x \text{ -- } \varphi}{\Gamma \vdash \exists x\, \varphi}$

13. Правило удаления существования
($\exists$ E) $\dfrac{\Gamma \vdash \exists x\, \varphi \quad \Gamma, \varphi(y/x) \vdash \psi, \text{ если } y \notin FV(\Gamma) \cup FV(\psi) \text{ и } (y := x \vee y \notin V(\varphi))}{\Gamma \vdash \psi}$

14. Аксиома рефлексивности $\Gamma \vdash \forall x\, x = x$

15. Правило конкгруентности (congr) $\dfrac{\Gamma \vdash t = s \quad \Gamma \vdash \varphi(t/x), \text{ если } t \text{ -- } x \text{ -- } \varphi \wedge s \text{ -- } x \text{ -- } \varphi}{\Gamma \vdash \varphi(s/x)}$

16. Правило удаления лжи ($\bot$ E) $\dfrac{\Gamma \vdash \bot}{\Gamma \vdash \varphi}$

17. Приведение к абсурду (ra) $\dfrac{\Gamma \vdash \neg\varphi \quad \Gamma \vdash \varphi}{\Gamma \vdash \bot}$

18. Закон исключённого третьего (tnd) $\dfrac{\Gamma, \neg\varphi \vdash \psi \quad \Gamma, \varphi \vdash \psi}{\Gamma \vdash \psi}$

19. Правило симметрии (sym) $\dfrac{\Gamma \vdash t = s}{\Gamma \vdash s = t}$

2.1.13 Теорема о полноте и корректности исчисления предикатов с равенством: без доказательства. Теорема о компактности в двух равносильных формах.

Теорема о полноте и корректности исчисления предикатов с равенством

Теорема о корректности исчисления предикатов с равенством $\Gamma \vdash \varphi \Rightarrow \Gamma \vDash \varphi$

Теорема о полноте исчисления предикатов с равенством $\Gamma \vDash \varphi \Rightarrow \Gamma \vdash \varphi$

Теорема о компактности в двух равносильных формах

Первая форма теоремы о компактности Если $\Gamma \vdash \varphi$, то $\exists$ конечная $\Gamma' \subseteq \Gamma$, т.ч. $\Gamma' \vdash \varphi$.

Доказательство.

Формально - индукция по выводам. Рассмотрим для примера удаление существования.

$$\frac{\Gamma \vdash \exists x\,\varphi \quad \Gamma, \varphi(y/x) \vdash \psi}{\Gamma \vdash \psi} \text{ пи } \Rightarrow \frac{\dfrac{\Gamma' \vdash \exists x\,\varphi \quad \Gamma'', \varphi(y/x) \vdash \psi}{\Gamma' \cup \Gamma'' \vdash \exists x\,\varphi \quad \Gamma'' \cup \Gamma', \varphi(y/x) \vdash \psi}}{\Gamma' \cup \Gamma'' \vdash \psi}$$

Вторая форма Если $\forall$ конечного $\Gamma' \subseteq \Gamma$ Γ' выполнима, то Γ выполнима (причём есть модель мощности $\leqslant \max(|\sigma|, |\mathbb{N}|)$)

Доказательство.

От противного. Допустим Γ невыполнима. Тогда $\Gamma \vDash \bot \Rightarrow \exists \Gamma'$ конечная $\subseteq \Gamma$ $\Gamma' \vDash \bot$, противоречие.

2.2 Вопросы на хор

2.2.1 Любые два счётных плотных линейных порядка без наименьшего и наибольшего элемента изоморфны.

Любые два счётных плотных линейно упорядоченных множества без наибольшего и наименьшего элемента изоморфны.

Доказательство.

Пусть X и Y - данные нам множества. Требуемый изоморфизм строится по шагам. После n шагов у нас есть два n-элементных подмножества $X_n \subset X, Y_n \subset Y$, элементы которых мы будем называть "охваченными и взаимно однозначное соответствие между ними, сохраняющее порядок. На очередном шаге мы берём какой-либо неохваченный элемент одного из множеств (скажем, множества X) и сравниваем его со всеми охваченными элементами X. Он может оказаться либо меньше всех, либо больше, либо попасть между какими-то двумя. В каждом из случаев мы можем найти неохваченный элемент в Y, находящийся в том же положении (больше всех, между первым и вторым охваченным сверху, между вторым и третьем охваченным сверху и т.д.). При этом мы пользуемся тем, что в Y нет наименьшего элемента, нет наибольшего и нет соседних элементов, - в зависимости от того, какой из трёх случаев имеет место. После этого мы добавляем выбранные элементы к X_n и Y_n, считая их соответствующими друг другу.

Чтобы в пределе получить изоморфизм между множествами X и Y, мы должны позаботиться о том, чтобы все элементы обоих множеств были рано или поздно охвачены. Это

можно сделать так: поскольку каждое из множеств счётно, пронумеруем его элементы и будем выбирать неохваченный элемент с наименьшим номером (на нечётных шагах - из X, на нечётных - из Y).

2.2.2 Лемма о корректной подстановке. Переименование связанной переменной

Лемма о корректной подстановке В любой интерпретации при любой оценке π для всех $\varphi \in Fm_\sigma, t, s \in Tm_\sigma$, и $x \in Var$, если $t\ -\ x\ -\ \varphi$, то

$$[s(t/x)](\pi) = [s](\pi_x^{[t](\pi)}) \wedge [\varphi(t/x)](\pi) = [\varphi](\pi_x^{[t](\pi)})$$

Доказательство.

Доказывается индукцией по построению s и φ. Рассмотрим лишь принципиальный случай, когда $\varphi = \forall z\psi, z \neq x$. Из условия $t{-}x{-}\varphi$ вытекает $(z \notin V(t) \wedge t{-}x{-}\psi) \vee x \notin FV(\varphi)$. В первом случае имеем

$$[\varphi(t/x)](\pi) = [\forall z\ (\psi(t/x))][\pi] = \forall a \in M\ [\psi(t/x)](\pi_z^a) = \forall a \in M\ [\psi](\pi_{zx}^{a[t](\pi_z^a)}) =$$

$$\forall a \in M\ [\psi](\pi_{zx}^{a[t](\pi)}) = [\forall z\ \psi](\pi_x^{[t](\pi)})$$

Во втором случае те же равенства выполняются вследствие $x \notin FV(\psi)$: применяем предположение индукции для ψ, т.к. $t\ -\ x\ -\ \varphi$.

Переименование связанной переменной Пусть $y \notin V(\varphi)$. Тогда

$$\forall x\ \varphi \equiv \forall y\ \varphi(y/x)$$

где $\varphi(y/x)$ означает результат замены всех свободных вхождений переменной x в формулу φ на y.

Доказательство.

Для доказательства прежде всего уточним смысл выражения $\varphi(y/x)$. Именно, дадим индуктивное определение такой подстановки для термов и формул...

Вспомогательная лемма Для любого терма t и любой формулы φ, если $y \notin V(\varphi)$, то для всякой оценки π верно

$$[t(y/x)](\pi) = [t](\pi_x^{\pi(y)}) \wedge [\varphi(y/x)](\pi_x^{\pi(y)})$$

Доказывается также индукцией по построению терма t и формулы φ.

Теперь мы можем завершить доказательство предыдущей леммы. Действительно, в любой интерпретации и при произвольной оценке π имеем

$$[\forall y\ \varphi(y/x)](\pi) = \forall a \in M\ [\varphi(y/x)](\pi_y^a) = \forall a \in M\ [\varphi](\pi_{yx}^{a\pi_y^a(y)}) =$$

$$\forall a \in M\ [\varphi](\pi_{yx}^{aa}) = \forall a \in M\ [\varphi](\pi_x^a) = [\forall x\ \varphi](\pi)$$

2.2.3 Вывод производных правил в исчислении предикатов

1. Правило удаления лжи $\dfrac{\dfrac{\Gamma \vdash \bot}{\Gamma, \neg\varphi \vdash \bot}}{\Gamma \vdash \varphi}$

2. Приведение к абсурду (просто частный случай удаления импликации, т.к. $\neg\varphi = \varphi \to \bot$)

3. Третьего не дано: Нужно свести к удалению дизъюнкции, а для этого нужно доказать $\Gamma \vdash \neg\varphi \vee \varphi$.

4. Правило симметрии (см. картинки)

2.2.4 Теорема о корректности исчисления предикатов

Доказываем, индуктивно рассматривая все правила.

2.2.5 Пример применения теоремы о компактности

Утверждение: не существует теории конечных множеств.

Доказательство.

Для начала заметим, что теория бесконечных множеств существует. Рекурсивно определим $Diff_2 = \neg(x_1 = x_2), Diff_{n+1} = Diff_n \wedge \bigwedge\limits_{i=1}^{n} \neg(x_i = x_{n+1})$. Тогда определим теорию бесконечных множеств, как $T^{\text{inf}} = \{\exists x_1, \ldots, x_n\, Diff_n(\vec{x}) \mid n \geqslant 2\}$

Предположим противное - T из условия существует. Тогда положим $T^0 = T \cup T^{\text{inf}}$. Очевидно, что T^0 невыполнима.

Положим T' - конечная, причём $T' \subseteq T^0$. Тогда $\exists k \in \mathbb{N}$, т.ч. $T' \subseteq T \cup \{\exists \vec{x}\, Diff_n(\vec{x}) \mid 2 \leqslant n \leqslant k\}$ и возьмём интерпретацию M, которая содержит k элементов. С одной стороны имеем $M \vDash T$, а сдругой $M \vDash \{\exists \vec{x}\, Diff_n(\vec{x}) \mid 2 \leqslant n \leqslant k\}$. Тогда $M \vDash T'$.

Получили, что любое конечное подмножество T^0 выполнима $\Rightarrow$ по теореме о компактности T^0 выполнима, что невозможно.

3 Алгоритмы

3.1 Вопросы на удос

3.1.1 Вычислимые функции(при интуитивном понимании алгоритма). Разрешимые и перечислимые множества. Связь конечности, разрешимости и перечислимости. Разрешимые множества под действием операций алгебры множеств и декартова произведения.

Вычислимые функции Функция $f : A \xrightarrow{p} B$ вычислима, если существует алгоритм, который на любом входе $x \in \operatorname{dom} f$ выписывает $f(x)$ и завершается, а на любом входе $x \in A \setminus \operatorname{dom} f$ не завершается ни за какое конечное количество шагов.

Разрешимые и перечислимые множества

Разрешимое множество Множество A разрешимо, если его характеристическая функция χ_A вычислима. Иными словами, если есть алгоритм, по входу определяющий, принадлежит ли этот вход множеству A;

Перечислимое множество Множество A перечислимо, если есть алгоритм, на пустом входе последовательно выписывающий все элементы A и только их.

Связь конечности, разрешимости и перечислимости

Связь конечности и разрешимости Каждое конечное множество разрешимо, т.к. мы можем просто перебрать все его элементы за конечное время, и определить, принадлежит ли наш вход ему.

Связь разрешимости и перечислимости Каждое разрешимое множество перечислимо, т.к. мы можем подставлять в его характеристическую функцию поочерёдно все числа из $\mathbb{N}$ и печатать их, если функция вернула 1.

Разрешимые множества под действием операций алгебры множеств и декартова произведения Если A, B разрешимы, то разрешимы $A \cup B, A \cap B, A \times B$ и $\overline{A}$.

Доказательство.

Покажем, например, что множество $A \times B$ перечислимо, если перечислимы A и B. Станем попеременно выполнять по шагу перечисляющих алгоритмов для A и для B, раздельно выписывая куда-либо всякий получаемый элемент каждого из этих множеств. Как только получен очередной элемент $a \in A$, выдадим на выход пары (a, b_i) для всех накопленных к этому моменту элементов $b_1, \ldots, b_k \in B$. Аналогично поступим с очередным элементом множества B. Если $(a, b) \in A \times B$, то элементы a, b попадут в наш накопитель, причём один из них попадёт в него позже другого. Пусть, без ограничения общности, это будет a. Тогда b уже содержится в накопителе, и мы выпишем пару (a, b). Также очевидно, что никаких лишних пар мы не выписываем.

3.1.2 Перечислимые множества под действием операций алгебры множеств, декартова произведения и проекции. Теорема Поста.

Перечислимые множества под действием операций алгебры множеств, декартова произведения и проекции. Если A, B перечислимы, то перечислимы $A \cup B, A \cap B, A \times B$ и $pr^i A$.

Теорема Поста Множество A разрешимо $\Leftrightarrow$ A и $\overline{A}$ перечислимы.

Доказательство.

Импликация слево направо следует из леммы об операциях с разрешимыми множествами. Допустим, что A и $\overline{A}$ перечислимы. Как мог бы работать разрешающий A алгоритм? Ясно, что, получив на вход $n \in \mathbb{N}$, достаточно попеременно выполнять по шагу перечисляющих алгоритмов для A и $\overline{A}$, ожидая, пока n не будет выписан тем или другим. Поскольку $n \in A \vee n \in \overline{A}$, описанная процедура завершится.

3.1.3 Теорема о графике вычислимой функции. Перечислимость образа и прообраза множества под действием вычислмой функции.

1. Функция $f : \mathbb{N} \xrightarrow{p} \mathbb{N}$ вычислима тогда и только тогда, когда её график $\Gamma_f = \{(x, f(x)) \mid x \in \text{dom } f\}$ перечислим.

2. Пусть $A \subseteq \mathbb{N}$ перечислимо, а функция $f : \mathbb{N} \xrightarrow{p} \mathbb{N}$ вычислима. Тогда $f(A)$ и $f^{-1}(A)$ перечислимы.

Доказательство.

Установим первое утверждение. Пусть график Γ_f перечислим. Тогда, чтобы вычислить значение $f(n)$, достаточно выписывать элементы Γ_f и проверять, совпадает ли первая координата пары с n. Если совпадает, выдавать вторую координату. Этот процесс завершается тогда и только тогда, когда $n \in \text{dom } f$.

Обратно, пусть f вычислима. Но тогда перечислимо множество dom f и, следовательно, есть вычислимая функция g, т.ч. rng $g =$ dom f. Рассмотрим функцию $h : \mathbb{N} \xrightarrow{p} \mathbb{N} \times \mathbb{N}$, т.ч. $h(n) \simeq (g(n), f(g(n)))$ для всех $n \in \mathbb{N}$. Она вычислима $\Rightarrow$ rng h перечислим, причём

$$(x, y) \in \text{rng } h \Leftrightarrow (x \in \text{rng } g \wedge f(x) = y) \Leftrightarrow (x \in \text{dom } f \wedge f(x) = y) \Leftrightarrow (x, y) \in \Gamma_f$$

для всех $x, y \in \mathbb{N}$. Значит $\Gamma_f =$ rng h и график функции f перечислим.

Теперь легко получить второе утверждение. Имеем

$$f(A) = pr^2 \left(\Gamma_f \cap A \times \mathbb{N}\right)$$

$$f^{-1}(A) = pr^1 \left(\Gamma_f \cap \mathbb{N} \times A\right)$$

3.1.4 Перечислимые множества суть, в точности, области определения вычислимых функций

3.1.5 Непустые перечислимые суть, в точности, области значений вычислимых тотальных функций

3.1.6 Перечислимые множества суть, в точности, проекции разрешимых

Пусть $A \subseteq \mathbb{N}$. Тогда равносильны условия

1. A перечислимо
2. существует вычислимая $f : \mathbb{N} \xrightarrow{p} \mathbb{N}$, т.ч. $A =$ dom f
3. существует вычислимая $f : \mathbb{N} \xrightarrow{p} \mathbb{N}$, т.ч. $A =$ rng f
4. $A = \varnothing$ или существует вычислимая тотальная $f : \mathbb{N} \to \mathbb{N}$, т.ч. $A =$ rng f.
5. существует разрешимое $B \subseteq \mathbb{N}^2$, т.ч. $A = pr^1 B$.

Доказательство.

Рассмотрим пункт 2 леммы, чтобы продмонстрировать важный приём. Очевидно, для перечислимого A вычислима полухактеристическая функция $\overline{\chi}_A$ для которой dom $\overline{\chi}_A = A$. Обратно, пусть f вычислима. Перечислим dom f.

Мы считаем, что у нас имеется вычислимое тотальное биективное кодирование пар натуральных чисел $\langle \cdot, \cdot \rangle : \mathbb{N}^2 \to \mathbb{N}$. Его нетрудно предъявить, вспомнив про обход диагоналей в построении биекции $\mathbb{N}$ и $\mathbb{N}^2$:

$$\langle n, m \rangle = \frac{(n+m)(n+m+1)}{2} + n$$

В силу биективности, вычислимыми тотальными будут и обратные функции $\pi^i : \langle x_1, x_2 \rangle \mapsto x_i$ для $i \in \{1, 2\}$.

Исполним следующую программу. В бесконечном цикле по $n \in \mathbb{N}$ станем вычислять $x = \pi^1(n)$ и $k = \pi^2(n)$, а затем выполнять k шагов программы для f на входе x. Если при этом мы обнаружим, что вычисление $f(x)$ закончилось не более, чем за k шагов, выпишем x. Вследствие биективности кодирования пар, мы обязательно обнаружим все пары (x, k) соответствующие заканчивающимся вычислениям f.

Равносильность п.3. и п.1. устанавливается с помощью той же конструкции. П.4. был, по существу, нами рассмотрен выше.

Также мы видим, как найти B для п.5. Можно взять вычислимую функцию f, т.ч. $A = \operatorname{dom} f$, и рассмотреть множество

$$B = \{(x, k) \mid \text{ программа для f на входе x завершается за k шагов } \}$$

Разрешающая процедура для B должна просто выполнить k (или менее, если останов случится раньше) шагов программы для f на x.

3.1.7 Универсальная вычислимая функция. Т-предикат.

Универсальная вычислимая функция Функция $U : \mathbb{N}^2 \xrightarrow{p} \mathbb{N}$ называется универсальной вычислимой, если она вычислима и для всякой вычислимой функции $f : \mathbb{N} \xrightarrow{p} \mathbb{N}$ найдётся число $n \in \mathbb{N}$, называемое индексом функции f относительно U, т.ч. $U_n = f$

Т-предикат Для каждой у.в.ф. U разрешимы множества

$T' = \{(n, x, y, k) \mid \text{ алгоритм U останавливается на входе (n,x) за k шагов и оставляет на выходе y}\}$

$$T = \{n, x, k \mid \text{ алгоритм U останавливается на вхоже (n,x) ровно за k шагов}\}$$

Доказательство.

Неформально, нужно просто остановить алгоритм $\mathcal{U}$ на входе (n, x) после k шагов и посмотреть, завершился ли он и, если завершился, что подал на выход. Или констатировать, что $\mathcal{U}$ остановился раньше, чем за k шагов.

3.1.8 Неразрешимость проблемы самоприменимости и остановки. Примеры перечислимого неразрешимого и неперечислимого множеств.

Пример неразрешимого перечислимого множества Пусть U - у.в.ф. Тогда множество $K = \{n \in \mathbb{N} \mid \exists k \in \mathbb{N}\, T(n, n, k)\}$ неразрешимо, но перечислимо.

Пример неразрешимого неперичслимого множества Пусть U - у.в.ф. Тогда множество $S = \{(n, x) \in \mathbb{N}^2 \mid \exists k \in \mathbb{N}\, T(n, x, k)\}$

Доказательство.

Допустим K разрешимо. Рассмотрим f, т.ч. $f(n) \simeq \begin{cases} 1, & n \notin K \\ \text{undef}, & n \in K \end{cases}$. f вычислима, т.к. K разрешимо по предположению.

$\exists m \in \mathbb{N}\ f = U_m$, в частности $f(m) \simeq U(m, m)$

$m \in K \Rightarrow f(m)$ undef $\Rightarrow U(m, m)$ undef $\Rightarrow m \notin K$

$m \notin K \Rightarrow f(m) = 1 \Rightarrow U(m, m) = 1 \Rightarrow m \in K$

Противоречие, значит K неразрешимо. Но $K = \text{dom}\ d(x)$, где $d(x) = U(x, x)$. d вычислима, а значит её домен перечислим.

В свою очередь, $\overline{K}$ неперечислимо, т.к. иначе было бы, что $K, \overline{K}$ перечислимы, что влекло бы по теореме Поста разрешимость K.

3.1.9 Пример вычислимой функции, неимеющей вычислимого тотального продолжения

Функция d не имеет вычислимого тотального продолжения.

Доказательство.

Допустим $d \subseteq g$ и g тотальная. Рассмотрим $h : \mathbb{N} \to \mathbb{N}$, т.ч. $h = g + 1$.

$x \in \text{dom}\ d \Rightarrow d(x) = g(x) \neq g(x) + 1 = h(x)$

$x \notin \text{dom}\ d \Rightarrow d(x)$ undef $\not\simeq h(x)$ def $\Rightarrow \forall x\ d(x) \not\simeq h(x) \Rightarrow h(x)$ невычислима $\Rightarrow g(x)$ невычислима.

3.1.10 Область определения вычислимой функции, не имеющей вычислимого тотального продолжения, перечислима, но не разрешима

Если функция f вычислима, но не имеет вычислимого тотального продолжения, то dom f - неразрешимое перечислимое множество.

Доказательство.

Предположим противное: пусть dom f разрешимо. Рассмотрим

$$g(x) = \begin{cases} f(x), & x \in \text{dom}\ f \\ 1, & x \notin \text{dom}\ f \end{cases} = \chi_{\text{dom}\ f}(x) \cdot f(x) + (1 - \chi_{\text{dom}\ f}(x))$$

Получили тотальное вычислимое продолжение функции f. Противоречие.

3.1.11 Теорема о рекурсии как следствие теоремы Клини. Пример применения теоремы о рекурсии.

Теорема о рекурсии как следствие теоремы Клини Пусть U - г.у.в.ф., а функция $V : \mathbb{N}^2 \to \mathbb{N}$. Тогда $\exists n \in \mathbb{N} : U_n = V_n$.

Доказательство.

Ввиду главности U существует вычислимая тотальная $S : \forall k \in \mathbb{N}\, U_{S(k)} = V_k$, а по теореме Клини $\exists n : U_{S(n)} = U_n$. Следовательно, $U_n = V_n$.

Пример применения теоремы о рекурсии Существует программа, выводящая свой текст, т.е. $\exists n \in \mathbb{N}\, \forall x \in \mathbb{N}\, U(n,x) = n$.

Доказательство.

Функция $V(k,x) = k$ вычислима. По теореме о рекурсии $\exists k \in \mathbb{N} : V(n,x) \simeq U(n,x) = n$

3.1.12 m-сводимость и её свойства

Определение Пусть $A, B \subseteq \mathbb{N}$. A m-сводится к B тогда и только тогда, когда существует вычислимая тотальная функция $f : \mathbb{N} \to \mathbb{N} : \forall n\ (n \in A \Leftrightarrow f(n) \in B)$. Обозначается, как $A \leqslant_m B$ или $A \leqslant_B^f B$, если необходимо уточнить сводящую функцию.

Свойства

1. Рефлексивность $A \leqslant_m^{\mathrm{id}\,\mathbb{N}} A$
2. Транзитивность $A \leqslant_m B \wedge B \leqslant_m C \Rightarrow A \leqslant_m C$
3. $A \leqslant_m^f B \Rightarrow \overline{A} \leqslant_m^f \overline{B} : n \in \overline{A} \Leftrightarrow n \notin A \Leftrightarrow f(n) \notin B \Leftrightarrow f(n) \in \overline{B}$
4. Сравнение множеств по алгоритмической сложности: если $A \leqslant_m B$ и B разрешимо (перечислимо), то разрешимо (перечислимо) и A.

   Доказательство.

   $\forall n\ n \in A \Leftrightarrow f(n) \in B \Leftrightarrow \chi_B(f(n)) = 1 \Rightarrow \chi_A = \chi_B \circ f \Rightarrow \chi_A$ вычислима $\Rightarrow A$ разрешимо (аналогично с полухарактеристической функцией).
5. Если $A \leqslant_m B$ и A неразрешимо (неперечислимо), то B неразрешимо (неперечислимо)
6. Если A разрешимо и B нетривиально ($\varnothing \neq B \neq \mathbb{N}$), то $A \leqslant_m B$.

   Доказательство.

   Пусть $b \in B, a \in \overline{B}$, зададим вычислимую $f(n) := \begin{cases} b, & n \in A \\ a, & n \notin A \end{cases} \Rightarrow A \leqslant_m^f B$
7. $\exists A : A \not\leqslant_m \overline{A}$. Возьмём $A := \overline{K}, \overline{A} = K$, не могут сходится по предыдущим свойствам.
8. $\nexists A : \forall B \subseteq \mathbb{N}\ B \leqslant_m A$. Одна функция может сводить к A лишь одно множество, но вычислимых функций счётно, а подмножеств $\mathbb{N}$ континуальное количество.

3.2 Вопросы на хор

3.2.1 Главная универсальная вычислимая функция. Вычислимое биективное кодирование пар натуральных чисел. Построение главной у.в.ф. с помощью произвольной у.в.ф.

Главная универсальная вычислимая функция Вычислимая функция $U : \mathbb{N}^2 \xrightarrow{p} \mathbb{N}$ называется главной у.в.ф., если для любой вычислимой функции $V : \mathbb{N}^2 \xrightarrow{p} \mathbb{N}$ найдётся вычислимая тотальная функция $S : \mathbb{N} \to \mathbb{N}$, т.ч. $\forall n \in \mathbb{N} : U_{S(n)} = V_n$

Вычислимое биективное кодирование пар натуральных чисел Мы считаем, что у нас имеется вычислимое тотальное биективное кодирование пар натуральных чисел $\langle \cdot, \cdot \rangle : \mathbb{N}^2 \to \mathbb{N}$. Его нетрудно предъявить, вспомнив про обход диагоналей в построении биекции $\mathbb{N}$ и $\mathbb{N}^2$:

$$\langle n, m \rangle = \frac{(n+m)(n+m+1)}{2} + n$$

В силу биективности, вычислимыми тотальными будут и обратные функции $\pi^i : \langle x_1, x_2 \rangle \mapsto x_i$ для $i \in \{1, 2\}$.

Построение главной у.в.ф. с помощью произвольной у.в.ф. Существует главная универсальная вычислимая функция.

Доказательство.

Пусть U какая-либо у.в.ф. Рассмотрим функцию $W : \mathbb{N}^2 \xrightarrow{p} \mathbb{N}$, т.ч.

$$W(n, x) \simeq U(\pi^1(n), \langle \pi^2(n), x \rangle)$$

для всех $n, x \in \mathbb{N}$. Очевидно, W вычислима.

Проверим теперь, что W является г.у.в.ф. Пусть $V : \mathbb{N}^2 \xrightarrow{p} \mathbb{N}$ произвольная вычислимая функция. Функция $V'(x) \simeq V(\pi^1(x), \pi^2(x))$ очевидно, тоже вычислимая. Имеем $V' = U_l$ для некоторого l.

Мы положим $S(n) = \langle l, n \rangle$ для всех $n \in \mathbb{N}$. Ясно, что функция S вычислимая и тотальная. Далее, для любых n, x имеем:

$$W(s(n), x) \simeq W(\langle l, n \rangle, x) \simeq U(l, \langle n, x \rangle) \simeq V'(\langle n, x \rangle) \simeq V(n, x)$$

3.2.2 Невозможность универсальной вычислимой тотальной функции

Не существует вычислимой всюду определённой функции двух аргументов, универсальной для класса всех вычислимых всюду определённых функций одного аргумента.

Доказательство.

Пусть U - произвольная вычислимая всюду определённая функция двух аргументов. Рассмотрим диагональную функцию $u(n) = U(n, n)$. Очевидно, на аргументе n функция u совпадает с функцией U_n, а функция $d(n) = u(n) + 1$ отличается от U_n. Таким образом, вычислимая всюду определённая функция $d(n)$ отличается от всех U_n, и потому функция U не является универсальной.

3.2.3 Теорема Клини о неподвижной точке

Пусть U - г.у.в.ф., и вычислимая функция $f : \mathbb{N} \to \mathbb{N}$ тотальна. Тогда существует $n \in \mathbb{N}$, т.ч. $U_n = U_{f(n)}$.

Доказательство.

Рассмотрим функцию $V : \mathbb{N}^2 \xrightarrow{p} \mathbb{N}$, т.ч.

$$V(k, x) \simeq U(U(k, k), x)$$

Она, очевидно, вычислима. Вследствие главности U, найдётся вычисслимая тотальная функция $S : \mathbb{N} \to \mathbb{N}$, для которой при любых $k, x \in \mathbb{N}$ верно

$$U(S(k), x) \simeq V(k, x) \simeq U(U(k, k), x)$$

Функция $f \circ S$ также вычислимая тотальная. Существует $t \in \mathbb{N}$, т.ч. $U_t = f \circ S$. Для любых $x \in \mathbb{N}$ имеем

$$U(S(t), x) \simeq U(U(t, t), x) \simeq U((f \circ S)(t), x) \simeq U(f(S(t)), x)$$

Взяв $n := S(t)$, имеем $U_n = U_{f(n)}$, что и требовалось.

3.2.4 Индексные множества. Теорема Райса-Успенского: вывод из теоремы Клини. Пример применения.

Индексные множества Здесь и далее U - г.у.в.ф. Индексными называются множества вида $\{n \in \mathbb{N} \mid U_n$ обладает каким-то свойством$\}$

Теорема Райса-Успенского: вывод из теоремы Клини Если семейство $\mathcal{F}$ вычислимых функций нетривиально (то есть $\varnothing \neq \mathcal{F} \neq \mathbb{N}$), то его индексное множество F относительно любой ГУВФ неразрешимо.

Доказательство.

Предположим противное: пусть F разрешимо, тогда вычислима тотальная функция

$$h(k) = \begin{cases} m, & k \in F \\ n, & k \notin F \end{cases}$$

В таком случае можно применить теорему Клини: $\exists t : \ U_t = U_{h(t)}$. Рассмотрим два случая:

- $t \in F \Rightarrow U_t = U_{h(t)} \in \mathcal{F} \Rightarrow h(t) = m \Rightarrow U_m = g \in \mathcal{F}$ - противоречие
- $t \notin \mathcal{F} \Rightarrow U_t = U_{h(t)} \in \mathcal{F} \Rightarrow h(t) = n \Rightarrow U_n = f \notin \mathcal{F}$ - противоречие

Следовательно, множество F неразрешимо.

Пример применения Пусть U - г.у.в.ф. Разрешимо ли множество $X = \{n \in \mathbb{N} \mid$ не все значения функции U_n просты$\}$?

3.2.5 Индексные множества. Теорема Райса-Успенского: доказательство с помощью сведения. Пример применения.

Если семейство $\mathcal{F}$ вычислимых функций нетривиально (то есть $\varnothing \neq \mathcal{F} \neq \mathbb{N}$), то его индексное множество F относительно любой ГУВФ неразрешимо.

Доказательство.

Пусть $\xi \notin \mathcal{F} \Rightarrow \exists f \in \mathcal{F} : \ f \neq \xi$. Рассмотрим любое перечислимое неразрешимое K и вычислимую $V(n, x) \simeq f(x) \cdot \omega_K(n)$. Из главности U следует существование вычислимой тотальной $S : \ U_{S(n)} = V_n$. Рассмотрим два случая

- $n \in K \Rightarrow V_n = f \in \mathcal{F} \Rightarrow U_{S(n)} \in \mathcal{F} \Rightarrow S(n) \in F$
- $n \notin K \Rightarrow V_n = \xi \notin \mathcal{F} \Rightarrow U_{S(n)} \notin \mathcal{F} \Rightarrow S(n) \notin F$

Получили, что $n \in K \Leftrightarrow S(n) \in F \Rightarrow K \leqslant_m^S F$, причём K неразрешимо, поэтому неразрешимо и F.

Пусть теперь $\xi \in \mathcal{F}$. Тогда просто применим такое же рассуждение к множеству $\overline{F}$ и получим такой же результат.

3.2.6 Пример неперечислимого множества с неперечислимым дополнением

Пусть U - г.у.в.ф. Докажем, что множество $Z = \{n \in \mathbb{N} \mid \text{dom } U_n = 2\mathbb{N}\}$ и $\overline{Z}$ неперечислимы.

Введём две функции:

$$V(n,x) \simeq \begin{cases} 1, & n \in K \cap (x \vdots 2) \\ \text{undef}, & \text{else} \end{cases}$$

вычислима, т.к. это $\overline{\chi}_K$ с дополнительной проверкой чётности.

Тогда из главности U $\exists S : \forall n \in \mathbb{N}\ U_{S(n)} = V_n \Rightarrow n \in K \Leftrightarrow \text{dom } V_n = 2\mathbb{N} \Leftrightarrow \text{dom } U_{S(n)} = 2\mathbb{N} \Leftrightarrow S(n) \in Z \Rightarrow K \leqslant_m^S Z \Rightarrow \overline{K} \leqslant_m^S \overline{Z} \Rightarrow \overline{Z}$ неперечислимо по свойствам сводимости.

$$V'(n,x) \simeq \begin{cases} 1, & n \in K \cup (x \vdots 2) \\ \text{undef}, & \text{else} \end{cases}$$

аналогично $\exists S' : \forall n \in \mathbb{N}\ U_{S'(n)} = V'_n \Rightarrow n \in K \Leftrightarrow \text{dom } V'_n \neq 2\mathbb{N} \Leftrightarrow \text{dom } U_{S'(n)} \neq 2\mathbb{N} \Leftrightarrow S'(n) \notin Z \Rightarrow K \leqslant_m^{S'} \overline{Z} \Rightarrow \overline{K} \leqslant_m^{S'} Z \Rightarrow Z$ неперечислимо по свойствам m-сводимости.