

Содержание

1. Математическая логика	3
1.1. Включение и равенство множеств. Основные способы задания множеств. Операции и основные тождества алгебры множеств. Упорядоченные пары и декартово произведение.	3
1.2. Бинарные отношения; композиция и обращение. Функции. Равномощность и вложение. Теорема Кантора; тождества в смысле равномощности для множеств $\mathbb{N} \times \mathbb{N}$, $(A \times B)^C$ и C^{B^A} . Теорема Кантора–Бернштейна–Шрёдера (без доказательства) с примером применения.	5
1.3. Частичные порядки. Связь строгих и нестрогих порядков. Максимальные и минимальные, наибольшие и наименьшие элементы, верхние и нижние грани, супремум и инфимум. Изоморфизм порядков. Отношения эквивалентности, фактор-множество. Разбиения и отношения эквивалентности.	8
1.4. Принципы математической индукции, «сильной» индукции и наименьшего числа. Их равносильность. Теорема о рекурсии в различных формах (без доказательства). Принцип Дирихле (с доказательством). Основные теоремы о мощностях конечных и счетных множеств (про подмножество, объединение, произведение, степень и пр.; доказательства как доп. вопросы).	11
1.5. Вполне упорядоченные множества (ВУМ). Теорема о строении элементов ВУМ. Начальные отрезки ВУМ и их свойства; теорема о сравнении ВУМ (доказательство как доп. вопрос). Сложение и умножение ВУМ; свойства этих операций..	15
1.6. Аксиома выбора (с любой мотивировочной задачей — например, о существовании правой обратной у сюръекции). Лемма Цорна и теорема Цермело (без доказательства). Любой пример применения. Теоремы о мощностях бесконечных множеств, вытекающие из них (доказательства как дополнительные вопросы) .	17
1.7. Структуры и сигнатуры. Изоморфизм структур. Термы и формулы первого порядка. Их значения. Значение формулы при изоморфизме структур. Выразимые отношения и автоморфизмы структуры.	18
1.8. Эквивалентность, общезначимость и выполнимость формул первого порядка. Приведение булевой комбинации к дизъюнктивной и конъюнктивной нормальным формам. Корректные подстановки. Приведение формулы к предваренной нормальной форме.	21
1.9. Теорема об играх Эрэнфойхта (без доказательства). Пример элементарно эквивалентных неизоморфных структур. Теорема о компактности (для логики первого порядка — без доказательства). Пример ее применения.	23
1.10. Вычислимые функции (на основе интуитивного понятия об алгоритме). Разрешимые и перечислимые множества; их свойства. Универсальные вычислимые функции и Т-предикаты. Неразрешимость проблем самоприменимости и остановки. Теорема Клини о неподвижной точке (без доказательства). Теорема о рекурсии. Теорема Райса–Успенского	24
2. Дискретные структуры	27
2.1. Основные правила комбинаторики: правило сложения, правило умножения. Принцип Дирихле. Формула включения-исключения: формулировка, применение для вывода формулы для числа беспорядков (перестановок без неподвижных точек). Базовые комбинаторные конфигурации: размещения, перестановки и соче-	

тания. Формулы для количеств размещений, перестановок и сочетаний (конфигурации с повторениями и без). Формула Стирлинга (б/д).	27
2.2. Формула бинома Ньютона, полиномиальная формула. Свойства биномиальных коэффициентов: симметричность, унимодальность, рекуррентная формула треугольника Паскаля. Знакопеременная сумма биномиальных коэффициентов. Оценки для биномиальных коэффициентов при n : асимптотика C_n^k в случае $j = \text{const} \cdot n$ и в случае $k = o(\sqrt{n})$	29

ДМ Гос (ИВТ: Матлог + ДС)

Disclaymer: доверять этому конспекту или нет выбирайте сами

1. Математическая логика

1.1. Включение и равенство множеств. Основные способы задания множеств. Операции и основные тождества алгебры множеств. Упорядоченные пары и декартово произведение.

Определение 1.1.1: Множество A **включено** \subseteq в множество $B \Leftrightarrow$

$$x \in A \Rightarrow x \in B$$

Определение 1.1.2: Множество A **равно** множеству $B \Leftrightarrow$

$$x \in A \Leftrightarrow x \in B$$

Лемма 1.1.1 (Свойства включения):

- $A \subseteq A$
- $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$
- $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$

Лемма 1.1.2 (Свойства равенства):

- $A = A$
- $A = B \wedge B = C \Rightarrow A = C$
- $A = B \Rightarrow B = A$

Замечание 1.1.1 (Основные способы задания множеств):

- Назвать все его элементы, когда число этих элементов конечно и все они уже определены
- Выделение всех элементов какого-нибудь уже определённого множества A , обладающих некоторым точно определённым свойством φ
- Рассмотреть **множество всех подмножеств** множества A . Такое множество обозначают выражением $\mathcal{P}(A)$
- Располагая каким-нибудь множеством X , рассмотреть его объединение, обозначаемое $\cup X$ и состоящее из всевозможных элементов множеств, принадлежащих X

Определение 1.1.3: Объединением множеств A и B называется множество $A \cup B$:

$$x \in A \cup B \Leftrightarrow x \in A \vee x \in B$$

Определение 1.1.4: Пересечением множеств A и B называется множество $A \cap B$:

$$x \in A \cap B \Leftrightarrow x \in A \wedge x \in B$$

Определение 1.1.5: Разностью множеств A и B называется множество $A \setminus B$:

$$x \in A \setminus B \Leftrightarrow x \in A \wedge x \notin B$$

Определение 1.1.6: Нередко все рассматриваемые множества оказываются подмножествами какого-нибудь множества U .

Такое U называют тогда **универсумом**.

Для каждого подмножества A заданного универсума U определено **дополнение**

$$\bar{A} = U \setminus A$$

Теорема 1.1.1 (Основные тождества алгебры множеств): $\forall A, B, C$ и любого включающего их универсума U верно:

- $A \cap B = B \cap A; A \cup B = B \cup A$
- $(A \cap B) \cap C = A \cap (B \cap C); (A \cup B) \cup C = A \cup (B \cup C)$
- $A \cap A = A; A \cup A = A$
- $\overline{A \cap (A \cup B)} = A; A \cup (A \cap B) = A$
- $\overline{\bar{A}} = A$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C); A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $\overline{A \cap B} = \bar{A} \cup \bar{B}; \overline{A \cup B} = \bar{A} \cap \bar{B}$
- $A \cap \emptyset = \emptyset; A \cup \emptyset = A; A \cap U = A; A \cup U = U; \bar{\emptyset} = U; \bar{U} = \emptyset$
- $A \cap \bar{A} = \emptyset; A \cup \bar{A} = U$

Определение 1.1.7: Для произвольных множеств a и b символом (a, b) обозначают множество $\{\{a\}, \{a, b\}\}$, называемое **упорядоченной парой** множеств a и b

Определение 1.1.8: Декартовым (или прямым) произведением множеств A и B называется множество

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

1.2. Бинарные отношения; композиция и обращение. Функции. Равномощность и вложение. Теорема Кантора; тождества в смысле равномощности для множеств $\mathbb{N} \times \mathbb{N}$, $(A \times B)^C$ и C^{B^A} . Теорема Кантора–Бернштейна–Шрёдера (без доказательства) с примером применения.

Определение 1.2.1: Множество R называется **бинарным отношением**, если каждый его элемент является упорядоченной парой множеств.

Определение 1.2.2: Назовём **областью определения** отношения R множество

$$\text{dom } R = \{a \in \cup \cup R \mid \exists b : (a, b) \in R\}$$

и **областью значений** отношения R – множество

$$\text{rng } R = \{b \in \cup \cup R \mid \exists a : (a, b) \in R\}$$

Определение 1.2.3: Для любых отношений P и Q определена **композиция** отношений P и Q :

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

Определение 1.2.4: Пусть R – бинарное отношение. **Обратным отношением** к R называется отношение

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

Определение 1.2.5: Пусть R – бинарное отношение и X – некоторое множество.

Мы называем **образом под действием отношения R множества X** множество

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

Определение 1.2.6: Бинарное отношение R называется:

- **Функциональным**, если $\forall x : \forall y : \forall z : xRy \wedge xRz \Rightarrow y = z$
- **Инъективным**, если $\forall x : \forall y : \forall z : xRy \wedge zRy \Rightarrow x = z$
- **Тотальным** для множества Z , если $\forall x \in Z : \exists y : (x, y) \in R$
- **Сюръективным** для множества Z , если $\forall y \in Z : \exists x : (x, y) \in R$

Определение 1.2.7: Функциональное отношение $f \subseteq A \times B$ называется **частичной функцией на множестве A во множество B** . В таком случае пишем $f : A \xrightarrow{p} B$.

Если, помимо того, отношение является тотальным для множества A , то оно называется **функцией на множестве A во множество B** . В таком случае пишем $f : A \rightarrow B$.

Определение 1.2.8: Множество

$$\{f \in \mathcal{P}(A \times B) \mid f : A \rightarrow B\}$$

всех функций из A в B обозначается символом B^A

Определение 1.2.9: Если функция $f : A \rightarrow B$ инъективна, она называется **инъекцией из A в B** .

Определение 1.2.10: Если функция $f : A \rightarrow B$ сюръективна, она называется **сюръекцией из A в B** .

Определение 1.2.11: Если функция $f : A \rightarrow B$ инъективна и сюръективна, она называется **биекцией из A в B** .

Определение 1.2.12: Будем писать $A \overset{f}{\sim} B$, если $f : A \rightarrow B$ есть биекция.

Скажем, что множество A **равномощно** множеству B , если существует f , такая что $A \overset{f}{\sim} B$. Тогда пишем $A \sim B$.

Определение 1.2.13: Множество A не превосходит по мощности (вкладывается во) множество B , если существует инъекция $f : A \rightarrow B$. Тогда пишем $A \overset{f}{\lesssim} B$ и $A \lesssim B$

Теорема 1.2.1 (Кантора): Ни для какого множества A невозможно $\mathcal{P}(A) \lesssim A$

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

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

Очевидно, $Y \in \mathcal{P}(A)$. По определению Y следует, что $f(Y) \notin Y$.

Рассмотрим произвольное $X \in \mathcal{P}(A) : f(Y) = f(X)$. В силу инъективности f имеем $X = Y$. Но тогда $f(Y) \notin X$ для всех таких X .

По определению множества Y получаем $f(Y) \in Y$. Противоречие. \square

Утверждение 1.2.1: Убедимся, что

$$\mathbb{N}^2 \sim \mathbb{N}$$

Доказательство: Положим

$$\forall (m, n) \in \mathbb{N}^2 : f(m, n) = 2^m(2n + 1) - 1$$

Докажем инъективность, если $f(m, n) = f(m', n')$, то

$$2^m(2n + 1) = 2^{m'}(2n' + 1)$$

Допустим, что $m \neq m'$ и БОО $m < m'$. Тогда

$$2n + 1 = 2^{m'-m}(2n' + 1)$$

Причём второе число чётно, а первое – нет. Противоречие показывает, что $m = m'$, но тогда $2n + 1 = 2n' + 1 \Rightarrow n' = n$. Инъективность доказана.

Докажем 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 $k = 2k'$. Но $k' < k$, а, значит,

$$k' = 2^{m'}(2n' + 1) \text{ для некоторых } m', n' \in \mathbb{N}.$$

Но тогда $k = 2^{m'+1}(2n' + 1)$ – противоречие. Сюръективность, а значит и биективность доказана \square

Утверждение 1.2.2:

$$(A \times B)^C \sim A^C \times B^C$$

Доказательство: Рассмотрим функции-проекторы $\pi_1 : A \times B \rightarrow A$ и $\pi_2 : A \times B \rightarrow B$.

Положим теперь $\psi : f \mapsto (\pi_1 \circ f, \pi_2 \circ f)$ для всех $f \in (A \times B)^C$.

Это отображения является биекцией, доказывается очевидной проверкой инъективности и сюръективности. \square

Утверждение 1.2.3:

$$C^{B^A} \sim C^{A \times B}$$

Доказательство: Для всех $f \in C^{B^A}$ и $z \in A \times B$ положим

$$\psi(f) : z \mapsto (f(\pi_1(z)))(\pi_2(z))$$

Это отображения является биекцией, доказывается очевидной проверкой инъективности и сюръективности. \square

Теорема 1.2.2 (Кантора-Шрёдера-Бернштейна): Для любых множеств A и B , если $A \lesssim B$ и $B \lesssim A$, то $A \sim B$.

Пример: Очевидно, что $\mathbb{N} \lesssim \mathbb{Q}$.

С другой стороны, $\mathbb{Q} \lesssim \mathbb{N}^3$: каждое положительное рациональное число q однозначно представляется несократимой дробью $\frac{m}{n}$, где $m, n \in \mathbb{N}$. Тогда отображение

$$f(q) = \begin{cases} (0,1,0), & q=0 \\ (m,n,0), & q>0 \\ (m,n,1), & q<0 \end{cases}$$

является искомой инъекцией. Осталось вспомнить, что $\mathbb{N}^3 = \mathbb{N}^2 \times \mathbb{N} \sim \mathbb{N} \times \mathbb{N} \sim \mathbb{N}$.

Показали инъекцию в обе стороны, а значит по КШБ $\mathbb{Q} \sim \mathbb{N}$.

1.3. Частичные порядки. Связь строгих и нестрогих порядков. Максимальные и минимальные, наибольшие и наименьшие элементы, верхние и нижние грани, супремум и инфимум. Изоморфизм порядков. Отношения эквивалентности, фактор-множество. Разбиения и отношения эквивалентности.

Определение 1.3.1: Бинарное отношение R называется

- **Рефлексивным** для множества Z , если $\forall x \in Z : (x, x) \in R$
- **Иррефлексивным**, если $\forall x : (x, x) \notin R$
- **Симметричным**, если $\forall x : \forall y : xRy \Rightarrow yRx$
- **Антисимметричным**, если $\forall x : \forall y : xRy \wedge yRx \Rightarrow x = y$
- **Транзитивным**, если $\forall x : \forall y : \forall z : xRy \wedge yRz \Rightarrow xRz$

Лемма 1.3.1: Отношение $R \subseteq A^2$:

- Рефлексивно $\Leftrightarrow \text{id}_A \subseteq R$
- Иррефлексивно $\Leftrightarrow \text{id}_A \cap R = \emptyset$
- Симметрично $\Leftrightarrow R \subseteq R^{-1} \Leftrightarrow R = R^{-1} \Leftrightarrow R^{-1} \subseteq R$
- Антисимметрично $\Leftrightarrow R \cap R^{-1} \subseteq \text{id}_A$
- Транзитивно $\Leftrightarrow R \circ R \subseteq R$

Определение 1.3.2: Отношение R на каком-либо множестве называется **строгим частичным порядком** на этом множестве, если R иррефлексивно и транзитивно.

Определение 1.3.3: Отношение R на каком-либо множестве называется **нестрогим частичным порядком** на этом множестве, если R рефлексивно, транзитивно и антисимметрично.

Утверждение 1.3.1: Пусть $P \subseteq A \times B, Q, R$ – бинарные отношения, тогда

- $(P^{-1})^{-1} = P$
- $(P \cup Q)^{-1} = P^{-1} \cup Q^{-1}$
- $\overline{P^{-1}} = \overline{P}^{-1}$
- $(P \cup Q) \circ R = (P \circ R) \cup (Q \circ R)$
- $(P \cap Q) \circ R \subseteq (P \circ R) \cap (Q \circ R)$

Теорема 1.3.1 (Связь строгих и нестрогих порядков): Положим

$$S(A) = \{R \in \mathcal{P}(A^2) \mid R \text{ строгий порядок}\}$$

и аналогично выделим множество $N(A)$ всех нестрогих порядков на A .

Рассмотрим функции $\varphi : S(A) \rightarrow \mathcal{P}(A^2)$ и $\psi : N(A) \rightarrow \mathcal{P}(A^2)$:

$$\varphi(P) = P \cup \text{id}_A \quad \psi(Q) = Q \setminus \text{id}_A$$

Тогда утверждается, что

- $\varphi(P) \in N(A) \wedge \psi(\varphi(P)) = P$
- $\psi(Q) \in S(A) \wedge \varphi(\psi(Q)) = Q$

Доказательство: Проверим нестрогость $\varphi(P)$:

- Рефлексивно, так как $\text{id}_A \subseteq \varphi(P)$
- Транзитивно, так как

$$\begin{aligned} \varphi(P) \circ \varphi(P) &= (P \cup \text{id}_A) \circ (P \cup \text{id}_A) = \\ &= (P \circ P) \cup (P \circ \text{id}_A) \cup (\text{id}_A \circ P) \cup (\text{id}_A \circ \text{id}_A) = \\ &= (P \circ P) \cup P \cup \text{id}_A \subseteq P \cup \text{id}_A = \varphi(P) \end{aligned}$$

- Антисимметрично, так как

$$\begin{aligned} \varphi(P) \cap (\varphi(P))^{-1} &= (P \cup \text{id}_A) \cap (P \cup \text{id}_A)^{-1} = \\ &= (P \cup \text{id}_A) \cap (P^{-1} \cup \text{id}_A) = (P \cap P^{-1}) \cup \text{id}_A = \text{id}_A \end{aligned}$$

Итак, $\varphi(P) \in N(A)$. Далее,

$$\begin{aligned} \psi(\varphi(P)) &= (P \cup \text{id}_A) \cap \overline{\text{id}_A} = \\ &= (P \cap \overline{\text{id}_A}) \cup \emptyset = (P \cap \overline{\text{id}_A}) \cup (P \cap \text{id}_A) = P \cap (\text{id}_A \cup \overline{\text{id}_A}) = P \cap A^2 = P \end{aligned}$$

Проверим нестрогость $\psi(Q)$:

- Ирефлексивно, так как $\text{id}_A \cap \psi(Q) = \emptyset$
- Транзитивно, так как пусть $xQy \wedge yQz$, где $x \neq y \wedge y \neq z$. Если $x = z$, то $zQy \wedge yQz \Rightarrow z = y$ – противоречие.

Итак, $\psi(Q) \in S(A)$. Далее,

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

□

Определение 1.3.4: Если на множестве A задан строгий частичный порядок P , элемент $x \in A$ называется **максимальным**, если

$$\forall y \in A : \neg(xPy)$$

В случае нестрогого порядка Q определяется, как

$$\forall y \in A : xQy \Rightarrow y = x$$

Определение 1.3.5: Если на множестве A задан строгий частичный порядок P , элемент $x \in A$ называется **минимальным**, если

$$\forall y \in A : \neg(yPx)$$

В случае нестрогого порядка Q определяется, как

$$\forall y \in A : yQx \Rightarrow y = x$$

Определение 1.3.6: Если R есть строгий или нестрогий частичный порядок на множестве A , пара (A, R) называется **частично упорядоченным множеством (ч.у.м.)**

Определение 1.3.7: Элемент $x \in B$ называется **наибольшим** в подмножестве B ч.у.м. $(A, <)$, если

$$\forall y \in B : y < x$$

и **наименьшим**, если

$$\forall y \in B : x < y$$

Определение 1.3.8: Пусть $(A, <)$ ч.у.м. и $B \subseteq A$. Элемент $x \in A$ назовём **верхней гранью** множества B , если

$$\forall y \in B : y \leq x$$

Аналогично определяются **нижние грани**.

Определим B^Δ – множество всех верхних граней, а также B^∇ – нижних граней.

Определение 1.3.9: Мы говорим, что $x \in A$ есть **точная верхняя грань (супремум)** множества B , если x есть наименьший элемент множества B^Δ .

Аналогично определяется **точная нижняя грань (инфимум)**.

Определение 1.3.10: Структуры $\mathcal{A} = (A, R); \mathcal{B} = (B, Q)$ **изоморфны**, если существует функция $\alpha : A \rightarrow B$, т.ч. $A \simeq B$ и

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

Определение 1.3.11: Отношение $R \subseteq A^2$ называется **отношением эквивалентности (эквивалентностью)** на A , если R рефлексивно, симметрично и транзитивно.

Определение 1.3.12: 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 .

Определение 1.3.13: 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 .

Определение 1.3.14: Назовём множество $\Sigma \subseteq \mathcal{P}(A)$ **разбиением** множества A , если

$$\emptyset \notin \Sigma \wedge \bigcup \Sigma = A \wedge (\forall \sigma, \tau \in \Sigma : \sigma \cap \tau \neq \emptyset \Leftrightarrow \sigma = \tau)$$

1.4. Принципы математической индукции, «сильной» индукции и наименьшего числа. Их равносильность. Теорема о рекурсии в различных формах (без доказательства). Принцип Дирихле (с доказательством). Основные теоремы о мощностях конечных и счетных множеств (про подмножество, объединение, произведение, степень и пр.; доказательства как доп. вопросы).

Определение 1.4.1: Принцип математической индукции:

$$\forall X \subseteq \mathbb{N} : (0 \in X \wedge (\forall n \in \mathbb{N} : n \in X \Rightarrow n + 1 \in X)) \Rightarrow X = \mathbb{N}$$

Определение 1.4.2: Назовём множество $X \subseteq \mathbb{N}$ **прогрессивным**, если

$$\forall n \in \mathbb{N} : \forall m < n : (m \in X \Rightarrow n \in X)$$

Принцип порядковой индукции:

$$\forall X \subseteq \mathbb{N} : X \text{ — прогрессивное} \Rightarrow X = \mathbb{N}$$

Определение 1.4.3: Принцип наименьшего числа:

$$\forall X \subseteq \mathbb{N} : X \neq \emptyset \Rightarrow \exists \min X$$

Теорема 1.4.1: Следующие утверждения равносильны:

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

Доказательство: $(1 \Rightarrow 2)$. Предположим, что в некотором X нет наименьшего элемента. Покажем, что \bar{X} прогрессивно:

$$\forall m < n : m \notin X \Rightarrow n \notin X$$

ибо иначе $n = \min X$, что невозможно.

По принципу порядковой индукции $\bar{X} = \mathbb{N} \Rightarrow X = \emptyset$.

$(2 \Rightarrow 3)$. Рассмотрим множество \bar{X} . Допустим, что $\bar{X} \neq \emptyset$. Тогда $\exists n = \min \bar{X}$.

По предположению, $n \neq 0$ (так как $0 \in X$). Значит, $n = m + 1$ для некоторого $m \in \mathbb{N}$. Поскольку $m < n$, имеем $m \in X$, но по предположению должно было быть, что $m + 1 = n \in X$, что не так. Следовательно $\bar{X} = \emptyset$, $X = \mathbb{N}$.

$(3 \Rightarrow 1)$. Рассмотрим множество

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

Очевидно, $0 \in Y$.

Допустим, что $n \in Y$. Тогда $\forall m < n : m \in X$, что, в силу прогрессивности, влечёт $n \in X$, а значит и $n + 1 \in Y$.

Для множества Y мы проверили базу и шаг индукции, а значит $Y = \mathbb{N}$.

Наконец, для всякого $n \in \mathbb{N}$ имеем $n < n + 1 \in Y \Rightarrow n \in X$. Следовательно, и $X = \mathbb{N}$. \square

Теорема 1.4.2 (О рекурсии): Пусть U – некоторое множество, $u_0 \in U$ и $h : U \rightarrow U$.

Тогда существует единственная функция $f : \mathbb{N} \rightarrow U$:

$$f(0) = u_0 \wedge \forall n \in \mathbb{N} : f(n + 1) = h(f(n))$$

Теорема 1.4.3 (О рекурсии, знающей шаг): Пусть U – некоторое множество, $u_0 \in U$ и $h : \mathbb{N} \times U \rightarrow U$.

Тогда существует единственная функция $f : \mathbb{N} \rightarrow U$:

$$f(0) = u_0 \wedge \forall n \in \mathbb{N} : f(n + 1) = h(n, f(n))$$

Теорема 1.4.4 (О примитивной рекурсии): Пусть U, V – некоторые множества, $g : V \rightarrow U$ и $h : \mathbb{N} \times V \times U \rightarrow U$.

Тогда существует единственная функция $f : \mathbb{N} \times V \rightarrow U$:

$$\forall v \in V : f(0, v) = g(v) \wedge \forall n \in \mathbb{N} : f(n + 1, v) = h(n, v, f(n))$$

Определение 1.4.4: Пусть $n \in \mathbb{N}$, тогда определим множество

$$\underline{n} = \{m \in \mathbb{N} \mid m < n\} = \{0, \dots, n-1\}$$

Определение 1.4.5: Множество A **конечно**, если $\exists n \in \mathbb{N} : A \sim \underline{n}$

Определение 1.4.6: Множество A **счётно**, если $A \sim \mathbb{N}$

Лемма 1.4.1: Для каждого $n \in \mathbb{N}$, если $f : \underline{n+1} \rightarrow \underline{n}$, то f не инъекция

Доказательство: Предположим противное, пусть найдётся $n \in \mathbb{N}$, для которого есть инъекция $f : \underline{n+1} \rightarrow \underline{n}$.

Согласно принципу наименьшего числа, рассмотрим наименьшее такое n .

Заметим, что инъекция $f : \underline{1} \rightarrow \underline{0} = \emptyset$ невозможна. Значит $n \neq 0 \Rightarrow \exists m \in \mathbb{N} : n = m + 1$.

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

Ясно, что g — биекция, а ограничение инъекции $f|_{\underline{n}}$ также является инъекцией. Тогда и $h = g \circ f|_{\underline{n}}$ также инъекция.

Заметим, если $h(k) = m$, то $f|_{\underline{n}} = x$, но f принимала x только на n , так что текущая ситуация невозможна из-за инъективности.

Значит $\text{rng } h \subseteq \underline{m} \Rightarrow h : \underline{m+1} \rightarrow \underline{m}$ — инъекция для $m < n$ — противоречие. \square

Теорема 1.4.5 (Принцип Дирихле): Если $m > n$ и $f : \underline{m} \rightarrow \underline{n}$, то f не инъекция

Доказательство: Допустим, $\exists m > n : f : \underline{m} \rightarrow \underline{n}$ — инъекция.

Но тогда $f|_{\underline{n+1}} : \underline{n+1} \rightarrow \underline{n}$ — тоже инъекция, что противоречит предыдущей лемме. \square

Теорема 1.4.6 (Правило подмножеств): Если $A \subseteq \mathbb{N}$, то множество A конечно или счётно.

Доказательство: Согласно теореме о рекурсии, существует функция $\alpha : \mathbb{N} \rightarrow \mathcal{P}(A)$

$$\alpha(0) := A \wedge \alpha(n+1) := \begin{cases} \alpha(n) \setminus \{\min \alpha(n)\}, & \alpha(n) \neq \emptyset \\ \emptyset, & \text{else} \end{cases}$$

Определим $f(m) := \min \alpha(m)$, тогда будут два случая

- $\exists n_0 : \alpha(n_0) = \emptyset$, выберем из таких n_0 наименьшее и докажем, что $f : \overline{n_0} \rightarrow A$ – биекция
- Иначе $f : \mathbb{N} \rightarrow A$, также является биекцией.

□

Теорема 1.4.7 (Правило суммы): Пусть множества A и B конечны и $A \cap B = \emptyset$.

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 функцию $h : A \cup B \rightarrow \underline{n+m}$:

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

Доказательство её биективности тривиально.

□

Теорема 1.4.8 (Правило произведения): Пусть множества A и B конечны.

Тогда множество $A \times B$ тоже конечно, причём

$$|A \times B| = |A| \cdot |B|$$

Доказательство: Допустим, что $A \overset{f}{\sim} \underline{n}, B \overset{g}{\sim} \underline{m}$. Если $m = 0 \vee n = 0$, то $A \times B = \emptyset$ – тривиальный случай.

Определим функцию $h : A \times B \rightarrow \underline{nm}$:

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

Доказательство её биективности тривиально.

□

Теорема 1.4.9 (Правило объединения): Пусть множества A и B конечны.

Тогда множество $A \times B$ тоже конечно, причём

$$|A \times B| = |A| + |B| - |A \cap B|$$

Доказательство: Заметим, что $A \cup B = (A \setminus B) \cup B$, причём $(A \setminus B) \cap B = \emptyset$.

Тогда по правилу суммы

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

□

Теорема 1.4.10 (Правило степени): 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 $A^{n+1} = A^n \times A$.

□

1.5. Вполне упорядоченные множества (ВУМ). Теорема о строении элементов ВУМ. Начальные отрезки ВУМ и их свойства; теорема о сравнении ВУМ (доказательство как доп. вопрос). Сложение и умножение ВУМ; свойства этих операций.

Определение 1.5.1: Порядок $<$ на множестве A называется **линейным**, если любые два элемента A сравнимы.

Мы говорим, что ч.у.м. $(A, <)$ есть **линейно упорядоченное множество (л.у.м.)**, если порядок $<$ линейный.

Определение 1.5.2: Порядок $<$ на множестве X **фундирован**, если во всяком непустом $Y \subseteq X$ существует минимальный элемент.

Множество **вполне упорядоченно (в.у.м.)**, если оно линейно и фундировано.

Определение 1.5.3: Для элемента x в.у.м. $(X, <)$ введём обозначение

$$[0, x) := \{y \mid y < x\}$$

Элемент x называется **предельным**, если

$$x \in \lim \Leftrightarrow x = \sup[0, x) \wedge x \neq 0$$

Наименьший элемент в.у.м. 0 тоже иногда считают предельным, поскольку $0 = \sup \emptyset = \sup[0, 0)$, мы не станем этого делать, но обозначим

$$\lim^* = \lim \cup \{0\}$$

Утверждение 1.5.1 (Свойства предельных элементов): Следующие условия эквивалентны:

- $x \in \lim^*$
- $\forall y : \neg(y + 1 = x)$
- $\forall y < x : y + 1 < x$

Теорема 1.5.1 (О строении элементов в.у.м.): Всякий элемент $x \in X$ однозначно однозначно представим в виде $x = y + n$, где $y \in \lim^*$

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 $C = \emptyset$, то $\forall z \in X : z + 1 \neq x \Rightarrow x$ — предельный. (по свойствам выше)

Иначе $C \neq \emptyset \Rightarrow \exists z' := \min C$ и для некоторого $k' > 0 : x = z' + k'$.

Если $z' = 0$, то $y = 0, n = k'$. Если же $z' \notin \text{lim}$, то по свойствам $\exists z'' : z' = z'' + 1$, что противоречит минимальности $z' \Rightarrow z' \in \text{lim}$. Значит можно брать $y = z', n = k'$.

Пусть $x = y_1 + n_1 = y_2 + n_2$. Если БОО $n_1 < n_2$, то $y_1 = y_2 + (n_2 - n_1)$, что противоречит предельности $y_1 \Rightarrow n_1 = n_2 \Rightarrow y_1 = y_2$, всё доказали. \square

Определение 1.5.4: 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**.

Утверждение 1.5.2 (Свойства начальных отрезков в.у.м.): Пусть $(X, <)$ в.у.м. Тогда

1. X есть свой начальный отрезок
2. Пусть I_a – н.о. X при всех $a \in A$. Тогда $\cup_{a \in A} I_a$ тоже н.о.
3. Если $x \in X$, то $[0, x)$ есть н.о. X
4. Если I собственный н.о. X , то существует и единственен такой $x \in X : I = [0, x)$
5. Пусть $\mathcal{J} = \{I \mid I \text{ — начальный отрезок } X\}$. Тогда (\mathcal{J}, \subseteq) есть в.у.м.
6. $(\mathcal{J}, \subseteq) \simeq X + 1; (\mathcal{J} \setminus X, \subseteq) \simeq X$

Доказательство:

2. Пусть $x \in \cup_{a \in A} I_a \wedge y < x$. Тогда найдётся $I_a \ni x \Rightarrow y \in I_a \subseteq \cup_{a \in A} I_a$
4. Имеем $X \setminus I \neq \emptyset$. Возьмём наименьший x элемент этого множества. Очевидно $y < x \Rightarrow y \in I$. Причём если $x \leq y \Rightarrow x \in I$ – не может быть.
5. Порядок (\mathcal{J}, \subseteq) линейен: все собственные н.о. вложены в X и сравнимы между собой по предыдущему пункту. Выделим в произвольном подмножестве $\mathcal{J} \subseteq \mathcal{J}$ 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' .
6. Изоморфизм строится как $[0, x) \mapsto x$, а X переходит в наибольший элемент множества $X + 1$.

\square

Определение 1.5.5 (Сравнение в.у.м.):

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

Лемма 1.5.1: Пусть $(X, <)$ – в.у.м. и функция $f : X \rightarrow X$ монотонна. Тогда $\forall x \in X : f(x) \geq x$

Доказательство: От противного. Тогда подмножество

$$C := \{x \mid f(x) < x\} \neq \emptyset$$

Пусть x' его наименьший элемент. Имеем $f(x') < x'$ по монотонности, но тогда $f(f(x')) < f(x') \Rightarrow f(x') \in C$, т.е. x' не наименьший. \square

Теорема 1.5.2 (О сравнении в.у.м.): Пусть C – в.у.м. и $B \subseteq C$. Тогда $B \leq C$.

Доказательство: Допустим $B > C$. Тогда, по определению

$$\exists b \in B : C \stackrel{f}{\simeq} [0_B, b) \subset B$$

Поскольку $b \in C$, то $f(b) < b$, но f монотонна, как изоморфизм, а значит $f(b) \geq b$ (по предыдущей лемме) – противоречие. \square

Определение 1.5.6: Произведением AB в.у.м. $(A, <_A)$ и $(B, <_B)$ называется $(A \times B, <)$:

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

Определение 1.5.7: Сумма в.у.м. $A + B$ есть $(A \times \{0\} \cup B \times \{1\}, <)$:

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

Лемма 1.5.2 (Свойства операций над в.у.м.):

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

1.6. Аксиома выбора (с любой мотивировочной задачей — например, о существовании правой обратной у сюръекции). Лемма Цорна и теорема Цермело (без доказательства). Любой пример применения. Теоремы о мощностях бесконечных множеств, вытекающие из них (доказательства как дополнительные вопросы)

Определение 1.6.1 (Аксиома выбора): Пусть множество A таково, что $\emptyset \notin A$.

Тогда существует функция $f : A \rightarrow \cup A$, т.ч. $f(a) \in a$ для всех $a \in A$.

Пример: Пусть $f : A \rightarrow B$. Правая обратная функция $g : B \rightarrow A$ существует тогда и только тогда, когда f есть сюръекция.

\Rightarrow . Тогда $f \circ g = \text{id}_B \Rightarrow \forall b \in B : (b, b) \in f \circ g$, а значит найдётся $a \in A$, для которого $(a, b) \in f$, что и есть сюръективность.

\Leftarrow . Ясно теперь, что множества $f^{-1}[\{b\}]$ непусты для все $b \in B$. Определим функцию $g : B \rightarrow A$, полагая

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

Теперь очевидно, что $f(g(b)) = b$.

Определение 1.6.2: Пусть $(A, <)$ – ч.у.м. Множество $C \subseteq A$ называется **цепью** в A , если

$$\forall x, y \in C : x \leq y \vee y \leq x$$

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

Лемма 1.6.1 (Цорна): Пусть $(X, <)$ – частично упорядоченное множество, в котором любая цепь $C \subset X$ имеет верхнюю грань. Тогда в $(X, <)$ найдётся максимальный элемент.

Теорема 1.6.1 (Цермело): Для всякого множества X существует бинарное отношение $<$ на X такое, что $(X, <)$ – в.у.м.

Теорема 1.6.2: Любые два множества сравнимы по мощности, то есть для любых множеств A, B найдётся инъекция из A в B или из B в A .

Доказательство: Вполне упорядочим эти множества по теореме Цермело. Тогда одно из них вложено в другое, как начальный отрезок. \square

1.7. Структуры и сигнатуры. Изоморфизм структур. Термы и формулы первого порядка. Их значения. Значение формулы при изоморфизме структур. Выразимые отношения и автоморфизмы структуры.

Определение 1.7.1: Структурой \mathcal{M} называется кортеж $(M, \mathcal{R}, \mathcal{F}, \mathcal{C})$:

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

Пример: Пример структуры натуральных чисел

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

Определение 1.7.2: Сигнатурой σ называется кортеж $(\text{rel}_\sigma, \text{func}_\sigma, \text{const}_\sigma)$, причём $\text{rel}_\sigma \neq \emptyset$ и все элементы кортежа не пересекаются.

Каждому $R \in \text{rel}_\sigma$ и каждому $f \in \text{func}_\sigma$ поставлено в соответствие натуральное число, оно называется **валентностью** символа. Пишем $R^{(n)}, f^{(n)}$.

Определение 1.7.3: Интерпретация сигнатуры σ – пара $(\mathcal{M}, \mathcal{S})$, где

- \mathcal{M} – структура $(M, \mathcal{R}, \mathcal{F}, \mathcal{C})$
- $\mathcal{S} : \text{rel}_\sigma \cup \text{func}_\sigma \cup \text{const}_\sigma \rightarrow \mathcal{R} \cup \mathcal{F} \cup \mathcal{C}$, причём
 - $\forall R^{(n)} \in \text{rel}_\sigma : \mathcal{S}(R) \in \mathcal{R} \wedge \mathcal{S}(R) \subseteq M^n$
 - $\forall f^{(n)} \in \text{func}_\sigma : \mathcal{S}(f) \in \mathcal{F} \wedge \mathcal{S}(f) \in M^{M^n}$
 - $\forall c \in \text{const}_\sigma : \mathcal{S}(c) \in \mathcal{C}$

Определение 1.7.4: Пусть M_1 и M_2 – две Интерпретации сигнатуры σ .

Биекция $\alpha : M_1 \rightarrow M_2$ 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

$$\forall a_1, \dots, a_k \in M_1 : P_1(a_1, \dots, a_k) = P_2(\alpha(a_1), \dots, \alpha(a_k))$$

Аналогично для k -местных функций f_1 и f_2 соответствующих одному функциональному символу, то

$$\forall a_1, \dots, a_k \in M_1 : \alpha(f_1(a_1, \dots, a_k)) = f_2(\alpha(a_1), \dots, \alpha(a_k))$$

Определение 1.7.5: Мы считаем, что задано счётное множество **индивидуальных (предметных)** переменных

$$\text{var} = \{x_0, x_1, \dots, x_n, \dots\}$$

Определение 1.7.6: Правила построения множества **термов** tm_σ над сигнатурой σ :

- $x \in \text{var} \Rightarrow x \in \text{tm}_\sigma$
- $c \in \text{const}_\sigma \Rightarrow c \in \text{tm}_\sigma$
- $f^{(n)} \in \text{func}_\sigma \Rightarrow \forall t_1, \dots, t_n \in \text{tm}_\sigma : f(t_1, \dots, t_n) \in \text{tm}_\sigma$

Определение 1.7.7: Правила построения множества **формул** fm_σ над сигнатурой σ (булевы операции и кванторы рассматриваются как формальные символы):

- $R^{(n)} \in \text{rel}_\sigma \Rightarrow \forall t_1, \dots, t_n \in \text{tm}_\sigma : R(t_1, \dots, t_n) \in \text{fm}_\sigma$
- $\varphi, \psi \in \text{fm}_\sigma \Rightarrow \neg\varphi \in \text{fm}_\sigma, \varphi \wedge \psi \in \text{fm}_\sigma, \varphi \vee \psi \in \text{fm}_\sigma, \varphi \rightarrow \psi \in \text{fm}_\sigma$
- $x \in \text{var}, \varphi \in \text{fm}_\sigma \Rightarrow \forall x : \varphi \in \text{fm}_\sigma, \exists x : \varphi \in \text{fm}_\sigma$

Определение 1.7.8: Оценка переменных – это любая функция $\pi : \text{var} \rightarrow M$

Определение 1.7.9: Пусть $t \in \text{tm}_\sigma$, π – оценка.

Тогда $[t]_{\mathcal{M}}(\pi) \in M$ – значение t в \mathcal{M} при оценке π , причём

- $x \in \text{var} \Rightarrow [x](\pi) = \pi(x)$
- $c \in \text{const}_\sigma \Rightarrow [c](\pi) = c^{\mathcal{M}}$
- $[f(t_1, \dots, t_n)](\pi) = f^{\mathcal{M}}([t_1](\pi), \dots, [t_n](\pi))$

Определение 1.7.10: Пусть $\varphi \in \text{fm}_\sigma$, π – оценка.

Тогда $[\varphi]_{\mathcal{M}}(\pi) \in \{0, 1\}$ – значение формулы φ в \mathcal{M} при оценке π , причём

- $[R(t_1, \dots, t_n)](\pi) = 1 \Leftrightarrow ([t_1](\pi), \dots, [t_n](\pi)) \in R^{\mathcal{M}}$
- $[\varphi \rightarrow \psi](\pi) = 1 \Leftrightarrow [\varphi](\pi) \rightarrow [\psi](\pi)$
- $[\forall x : \varphi](\pi) = 1 \Leftrightarrow \forall a \in M : [\varphi](\pi_x^a) = 1$, где

$$\pi_x^a(y) = \begin{cases} a, & y=x \\ \pi(y), & \text{else} \end{cases}$$
- $[\exists x : \varphi](\pi) = 1 \Leftrightarrow \exists a \in M : [\varphi](\pi_x^a) = 1$

Определение 1.7.11: Определим функцию, возвращающую переменные формулы или терма.

Пусть $V : \text{tm}_\sigma \cup \text{fm}_\sigma \rightarrow \mathcal{P}(\text{var})$, причём

- $x \in \text{var} \Rightarrow V(x) = \{x\}$
- $c \in \text{const}_\sigma \Rightarrow V(c) = \emptyset$
- $V(f(t_1, \dots, t_n)) = \bigcup_{i=1}^n V(t_i)$
- $V(R(t_1, \dots, t_n)) = \bigcup_{i=1}^n V(t_i)$
- $V(\varphi \wedge \psi) = V(\varphi) \cup V(\psi)$
- $V(\forall x : \varphi) = V(\varphi) \cup \{x\}$

Определение 1.7.12: Определим функцию, возвращающую свободные переменные формулы

Пусть $FV : \text{fm}_\sigma \rightarrow \mathcal{P}(\text{var})$, причём:

- $FV(R(t_1, \dots, t_n)) = V(R(t_1, \dots, t_n))$
- $FV(\varphi \vee \psi) = FV(\varphi) \cup FV(\psi)$
- $FV(\forall x : \varphi) = FV(\varphi) \setminus \{x\}$

Теорема 1.7.1: Значение терма $t \in \text{tm}_\sigma$ зависит лишь от значения оценки на $V(t)$.

Значение формулы $\varphi \in \text{fm}_\sigma$ зависит лишь от значения оценки на $FV(\varphi)$.

Определение 1.7.13: Пусть

- $\text{fm}_\sigma(x_1, \dots, x_n) := \{\varphi \in \text{fm}_\sigma \mid FV(\varphi) \subseteq \{x_1, \dots, x_n\}\}$
- $\text{tm}_\sigma(x_1, \dots, x_n) := \{t \in \text{tm}_\sigma \mid V(t) \subseteq \{x_1, \dots, x_n\}\}$

Следствие 1.7.1.1: Переопределим значения термов и формул, независимо от оценки.

Пусть $t \in \text{tm}_\sigma(x_1, \dots, x_n), \varphi \in \text{fm}_\sigma(x_1, \dots, x_n)$:

- $[t]_{\mathcal{M}}(\vec{a}) := [t]_{\mathcal{M}}(\pi_{x_1 \dots x_n}^{a_1 \dots a_n})$
- $[\varphi]_{\mathcal{M}}(\vec{a}) := [\varphi]_{\mathcal{M}}(\pi_{x_1 \dots x_n}^{a_1 \dots a_n})$

Теорема 1.7.2 (Значение формулы при изоморфизме): Пусть \mathcal{M}, \mathcal{N} – σ -структуры и $\mathcal{M} \stackrel{\alpha}{\simeq} \mathcal{N}$. Пусть $t \in \text{tm}_\sigma(\vec{x}), \varphi \in \text{fm}_\sigma(\vec{x})$.

Тогда

- $\forall \vec{a} : [t]_{\mathcal{M}}(\vec{a}) = [t]_{\mathcal{N}}(\alpha \vec{a})$
- $\forall \vec{a} : [\varphi]_{\mathcal{M}}(\vec{a}) = [\varphi]_{\mathcal{N}}(\alpha \vec{a})$

Доказательство: Доказывается очевидной индукцией по построению термов и функций. \square

Определение 1.7.14: Отношение $X \subseteq M^n$ выразимо в σ -структуре $\mathcal{M} \Leftrightarrow \exists X \in \text{fm}_\sigma(x_1, \dots, x_n) : \varphi^{\mathcal{M}} = X$

Определение 1.7.15: Функция $f : M^n \rightarrow M$ выразима в σ -структуре $\mathcal{M} \Leftrightarrow \exists t \in \text{tm}_\sigma(x_1, \dots, x_n) : t^{\mathcal{M}} = f$

Определение 1.7.16: Автоморфизмами структуры \mathcal{M} называют множество

$$\text{Aut}(\mathcal{M}) = \{\alpha \mid \mathcal{M} \stackrel{\alpha}{\simeq} \mathcal{M}\}$$

1.8. Эквивалентность, общезначимость и выполнимость формул первого порядка. Приведение булевой комбинации к дизъюнктивной и конъюнктивной нормальной формам. Корректные подстановки. Приведение формулы к предваренной нормальной форме.

Определение 1.8.1: Формула, значение которой равно единице в любой интерпретации при любой оценке, называется **общезначимой**

Определение 1.8.2: Формула, для которой существует интерпретация и оценка такие, что значение этой формулы равно единице, называется **выполнимой**

Определение 1.8.3: Формулы φ и ψ называются **эквивалентными** ($\psi \equiv \varphi$), если общезначима формула $\varphi \Leftrightarrow \psi$.

Теорема 1.8.1 (О переименовании 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 x в формулу φ на y .

Замечание 1.8.1 (Построение ДНФ и КНФ):

1. Избавляемся от всех логических операций, содержащихся в формуле, выразив их через конъюнкцию, дизъюнкцию и отрицание.
2. Заменить знаки отрицания, относящиеся ко всему выражению, знаками отрицания, относящимся к отдельным высказываниям
3. Избавиться от двойного отрицания
4. Раскрываем скобки по дистрибутивности
5. Избавляемся от одинаковых литералов

Определение 1.8.4: 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

Теорема 1.8.2: 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 во внутрь, перемещая кванторы.

Если в φ главная связка бинарная, то по предположению индукции, заменим каждую из формул под этой связкой на эквивалентную предварённую. Затем переименоваем связанные переменные так, чтобы можно было вынести все кванторы наружу. \square

1.9. Теорема об играх Эренфойхта (без доказательства).

Пример элементарно эквивалентных неизоморфных структур. Теорема о компактности (для логики первого порядка — без доказательства). Пример ее применения.

Определение 1.9.1: Предложениями в сигнатуре σ st_σ назовём все формулы без свободных переменных.

Определение 1.9.2: σ -структуры \mathcal{M} и \mathcal{N} элементарно эквивалентны \Leftrightarrow в них истинны одни и те же предположения.

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

Пример (Элементарно эквивалентные, но не эквивалентные структуры):
 $(\mathbb{R}, <) \simeq (\mathbb{Q}, <)$

Предложениями являются неравенства всех констант из \mathbb{Q} , которые, очевидно, будут выполняться и в \mathbb{R} .

Однако мы знаем, что $\mathbb{R} \neq \mathbb{Q} \Rightarrow (\mathbb{R}, <) \not\simeq (\mathbb{Q}, <)$

Определение 1.9.3: Если $T \subseteq \text{st}_\sigma$, то T — теория в сигнатуре σ .

Если T — теория и $\varphi \in \text{st}_\sigma$, то

$$T \models \varphi \Leftrightarrow \forall \mathcal{M} : \mathcal{M} \models T \Rightarrow \mathcal{M} \models \varphi$$

Теорема 1.9.1 (О компактности): Если любое конечное подмножество теории Γ' выполнимо, то Γ выполнима.

Пример (Применения теоремы о компактности): Не существует теории конечных множеств.

Для начала заметим, что теория бесконечных множеств существует.

Рекурсивно определим вспомогательную формулу

$$d_2 = \neg(x_1 = x_2) \quad d_{n+1} = d_n \wedge \left(\bigwedge_{i=1}^n \neg(x_i = x_{n+1}) \right)$$

Тогда определим теорию бесконечных множеств, как

$$T^\infty = \{ \exists x_1, \dots, x_n : d_n(\vec{x}) \mid n \geq 2 \}$$

Предположим противное — T из условия существует. Тогда, очевидно $T^0 = T^\infty \cup T$ невыполнима.

Положим T' — произвольное конечное подмножество T^0 . Тогда

$$\exists k \in \mathbb{N} : T' \subseteq T \cup \{ \exists x_1, \dots, x_n : d_n(\vec{x}) \mid 2 \leq n \leq k \}$$

И возьмём интерпретацию M , которая содержит k элементов. Получили $M \models T'$.

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

1.10. Вычислимые функции (на основе интуитивного понятия об алгоритме). Разрешимые и перечислимые множества; их свойства. Универсальные вычислимые функции и Т-предикаты. Неразрешимость проблем самоприменимости и остановки. Теорема Клини о неподвижной точке (без доказательства). Теорема о рекурсии. Теорема Райса–Успенского

Определение 1.10.1: Частичная функция $f: A \xrightarrow{p} B$ **вычислима**, если существует алгоритм, который на любом входе $x \in \text{dom } f$ выписывает $f(x)$ и завершается, а на любом входе $x \in A \setminus \text{dom } f$ не завершается ни за какое конечное количество шагов.

Определение 1.10.2: Множество A **разрешимо**, если его характеристическая функция χ_A вычислима.

Определение 1.10.3: Множество A **перечисливо**, если есть алгоритм, на пустом входе последовательно выписывающий все элементы A и только их.

Утверждение 1.10.1: Каждое конечное множество разрешимо

Доказательство: Переберём все его элементы за конечное время и определим, принадлежит ли вход ему □

Утверждение 1.10.2: Каждое разрешимое множество перечисливо

Доказательство: Поочерёдно будем считать результат характеристической функции на всех числах из \mathbb{N} и печатать, если функция вернула 1. □

Утверждение 1.10.3: Если A, B разрешимы, то разрешимы

- $A \cup B$
- $A \cap B$
- $A \times B$
- \overline{A}

Доказательство: Выразим характеристические функции полученных множеств через характеристические функции A и B □

Утверждение 1.10.4: Если A, B перечислимы, то перечислимы

- $A \cup B$
- $A \cap B$
- $A \times B$
- $\text{pr}^i A$

Доказательство: Будем запускать перечисляющие алгоритмы «параллельно» – чередовать их по одному шагу и потоки вывода:

- Сливать в один
- Если число, выведенное одним из потоком выводилось другим, то выводим его
- При получении нового числа из первого потока, декартово умножаем его на все числа из второго потока и выводим пары

□

Определение 1.10.4: Частичная 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 , такое что $U_n = f$.

Определение 1.10.5: Для каждой у.в.ф. U разрешимы множества (**Т-предикаты**):

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

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

Утверждение 1.10.5: 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

Доказательство: Допустим K разрешимо.

Рассмотрим f :

$$f(n) \simeq \begin{cases} 1, n \notin K \\ \text{undef}, n \in K \end{cases}$$

Она вычислима, так как K разрешимо.

Значит $\exists m \in \mathbb{N} : f = U_m$. В частности $f(m) \simeq U(m, m)$. Но

- $m \in K \Rightarrow f(m) \text{ undef} \Rightarrow U(m, m) \text{ undef} \Rightarrow m \notin K$
- $m \notin K \Rightarrow f(m) = 1 \Rightarrow U(m, m) = 1 \Rightarrow m \in K$

Противоречие! □

Определение 1.10.6: 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 $S : \mathbb{N} \rightarrow \mathbb{N}$, такая, что

$$\forall n \in \mathbb{N} : U_{S(n)} = V_n$$

Теорема 1.10.1 (Клини): Пусть U – г.у.в.ф. и вычислимая функция $f : \mathbb{N} \rightarrow \mathbb{N}$ тотальна.

Тогда существует $n \in \mathbb{N}$, такая что $U_n = U_{f(n)}$

Теорема 1.10.2 (О рекурсии): Пусть U – г.у.в.ф., а $V : \mathbb{N}^2 \rightarrow \mathbb{N}$ – вычислима. 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 $\exists n : U_{S(n)} = U_n = V_n$ □

Теорема 1.10.3 (Райса-Успенского): Если семейство \mathcal{F} вычислимых функций нетривиально, то есть $\emptyset \neq \mathcal{F} \neq \mathbb{N}$, то его индексное множество

$$F = \{n \in \mathbb{N} \mid U_n \in \mathcal{F}\}$$

относительно любой г.у.в.ф. неразрешимо.

Доказательство: Предположим противное: пусть F разрешимо, тогда вычислима тотальная функция

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

где по аксиоме выбора m – индекс функции, которая не принадлежит \mathcal{F} , а n – той, которая принадлежит.

В таком случае можно применить теорему Клини:

$$\exists t : U_t = U_{h(t)}$$

Рассмотрим два случая

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

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

□

2. Дискретные структуры

2.1. Основные правила комбинаторики: правило сложения, правило умножения. Принцип Дирихле. Формула включения-исключения: формулировка, применение для вывода формулы для числа беспорядков (перестановок без неподвижных точек). Базовые комбинаторные конфигурации: размещения, перестановки и сочетания. Формулы для количеств размещений, перестановок и сочетаний (конфигурации с повторениями и без). Формула Стирлинга (б/д).

Замечание 2.1.1 (Основные правила комбинаторики): Предположим, что у нас имеются 2 множества $A = \{a_1, \dots, a_n\}; B = \{b_1, \dots, b_m\}$:

1. **Правило суммы** – количество способов выбрать один объект из A или B равно $n + m$
- **Правило произведения** – количество способов выбрать один объект из A и к нему в пару один объект из B равно nm

Замечание 2.1.2 (Принцип Дирихле): Если $nk + 1$ различных элементов разбить на n множеств, то хотя бы в одном множестве содержится $k + 1$ элемент.

Теорема 2.1.1 (Формула включения-исключения): Пусть имеется множество из N объектов и некоторые свойства $\alpha_1, \dots, \alpha_n$.

Обозначим α'_k отрицанием свойства α_k .

Пусть $N(\alpha_i)$ обозначает количество объектов удовлетворяющих свойству α_i , аналогично введём количества объектов, удовлетворяющим произвольному m числу свойств.

Тогда справедливо следующая формула, называемая формулой включений и исключений:

$$\begin{aligned} N(\alpha'_1, \dots, \alpha'_n) = & N - N(\alpha_1) - \dots - N(\alpha_n) + \\ & N(\alpha_1, \alpha_2) + \dots + N(\alpha_{n-1}, \alpha_n) - \dots \\ & + (-1)^n N(\alpha_1, \dots, \alpha_n) \end{aligned}$$

Пример (Формула для числа беспорядков): Сколько способов рассадить n человек по n местам в аудитории, чтобы никто не сидел на своём месте?

Рассмотрим $n!$ перестановок людей. Пусть α_i означает, что i -й человек сидит на своём месте. Тогда

$$N(\alpha'_1, \dots, \alpha'_n) = n! - C_n^1(n-1)! - \dots + (-1)^n C_n^n =$$

$$n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \dots + (-1)^n \frac{1}{n!} \right) \xrightarrow{n \rightarrow \infty} \frac{n!}{e}$$

Определение 2.1.1: Произвольный упорядоченный набор из k элементов данного множества, среди которых могут быть повторяющиеся, называется **размещением из n элементов по k с повторением**.

Соответственно, если элементы не могут повторяться, то набор называется **размещением без повторений**, или просто размещением из n по k .

Обозначения – \overline{A}_n^k, A_n^k соответственно.

Определение 2.1.2: Сочетанием из n элементов по k называется набор k элементов этого множества.

Наборы, отличающиеся только порядком следования элементов считаются одинаковыми.

Соответственно, сочетания **бывают с повторениями и без**.

Обозначения – \overline{C}_n^k и C_n^k соответственно.

Лемма 2.1.1:

- $\overline{A}_n^k = n^k$
- $A_n^k = \frac{n!}{(n-k)!}$
- $\overline{C}_n^k = \frac{n!}{k!(n-k)!}$
- $\overline{C}_n^k = C_{n+k-1}^k$

Доказательство:

- На каждую из k позиций независимо выбираем n элементов, применяем правило умножения
- Первый элемент можно выбрать n способами, второй – $n - 1$ и так далее
- Так как нам не важен порядок, делим количество размещений на количество перестановок из k элементов
- Заметим, что по произвольному сочетанию с повторениями мы можем построить последовательность из 0 и 1 по следующему правилу:
 - Напишем столько 1, сколько раз встречается первый элемент изначального набора, потом напишем 0, потом столько 1, сколько встречается второй элемент набора и т.д.
 - В конце ставить 0 не будем, заметим, что наше сочетание с повторением – это количество способов выбрать позиции для k единиц в последовательности длины $n + k - 1$.

□

Теорема 2.1.2 (Формула Стирлинга):

$$n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$$

2.2. Формула бинома Ньютона, полиномиальная формула. Свойства биномиальных коэффициентов: симметричность, унимодальность, рекуррентная формула треугольника Паскаля. Знакопеременная сумма биномиальных коэффициентов. Оценки для биномиальных коэффициентов при n : асимптотика C_n^k в случае $j = \text{const} \cdot n$ и в случае $k = o(\sqrt{n})$

Теорема 2.2.1 (Бином Ньютона): **Биномом Ньютона** называется выражение

$$(a + b)^n = \sum_{k=0}^n C_n^k a^k b^{n-k}$$

Доказательство: n -ю степень суммы можно записать в виде

$$(a + b)^n = \underbrace{(a + b)(a + b) \dots (a + b)}_{n \text{ раз}}$$

Чтобы получить слагаемое в сумме, мы должны последовательно выбрать из каждой скобки a или b , причём любое слагаемое имеет вид $a^k b^{n-k}$.

Более того, чтобы определить слагаемое, нам необходимо и достаточно знать, сколько a мы выбрали.

А это для каждого слагаемого можно сделать C_n^k способами. \square

Определение 2.2.1: Пусть $n = \sum_{i=1}^t n_i$.

Для каждого $i \in \{1, \dots, t\}$ мы хотим забрать в a_i группу ровно n_i элементов из изначального набора n элементов.

Количество способов это сделать равно

$$\begin{aligned} P(n_1, \dots, n_t) &= C_n^{n_1} C_{n-n_1}^{n_2} \dots C_{n-n_1-\dots-n_{t-1}}^{n_t} = \\ &= \frac{n!}{n_1!(n-n_1)!} \frac{(n-n_1)!}{n_2!(n-n_1-n_2)!} \dots \frac{(n-n_1-\dots-n_{t-1})!}{n_t!(n-n_1-\dots-n_t)!} = \\ &= \frac{n!}{n_1!n_2!\dots n_t!} \end{aligned}$$

Оно называется **полиномиальный коэффициентом**

Теорема 2.2.2 (Полиномиальная формула): **Полиномиальной формулой** называется выражение

$$(x_1 + \dots + x_t)^n = \sum_{n_1 + \dots + n_t = n} P(n_1, \dots, n_t) x_1^{n_1} \dots x_t^{n_t}$$

Доказательство: Рассуждения аналогичны доказательству бинома Ньютона
□

Теорема 2.2.3 (Свойства биномиальных коэффициентов):

- **Симметричность:** $C_n^k = C_n^{n-k}$
- **Унимодальность:** коэффициенты возрастают до $k = \frac{n}{2}$, а потом убывают
- **Треугольник Паскаля:** $C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$
- $\sum_{k=0}^n (-1)^k C_n^k = 0$

Доказательство:

- Выбрать k объектов из n – это то же самое, что оставить $n - k$ объектов из n
- Отношение $\frac{C_n^k}{C_n^{k-1}} = \frac{n-k+1}{k} = \frac{n+1}{k} - 1 > 1 \Leftrightarrow \frac{n+1}{k} > 2 \Leftrightarrow k \leq \frac{n}{2}$
- Заметим, что все наборы можно разбить на две группы:
 - Содержат n -й элемент, но помимо него нужно выбрать $k - 1$ элемент из $n - 1$ штук.
 - Не содержат n -й элемент, а значит нужно выбрать k из $n - 1$ штук
- Применим Бином Ньютона для $(1 - 1)^n$

□

Теорема 2.2.4: Пусть $a \in (0, 1)$.

Тогда

$$C_n^{[an]} = \left(\frac{1}{a^a(1-a)^{1-a}} + o(1) \right)^n, n \rightarrow \infty$$

Доказательство: Будем пользоваться формулой Стирлинга $n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$:

$$C_n^{[an]} = \frac{n!}{[an]!(n-[an])!} \sim \frac{\sqrt{2\pi n} \left(\frac{n}{e}\right)^n}{\sqrt{2\pi [an]} \left(\frac{[an]}{e}\right)^{[an]} \sqrt{2\pi (n-[an])} \left(\frac{n-[an]}{e}\right)^{n-[an]}} \sim$$

$$\Theta\left(\frac{1}{\sqrt{n}}\right) \frac{\left(\frac{n}{e}\right)^n}{\left(\frac{[an]}{e}\right)^{[an]} \left(\frac{n-[an]}{e}\right)^{n-[an]}} = \Theta\left(\frac{1}{\sqrt{n}}\right) \frac{n^n}{[an]^{[an]} (n-[an])^{n-[an]}}; \quad n \rightarrow \infty$$

Теперь предположим, что $an \in \mathbb{N}$, тогда получим

$$C_n^{[an]} \sim \frac{\Theta\left(\frac{1}{\sqrt{n}}\right)}{a^{an}(1-a)^{n-an}} = \Theta\left(\frac{1}{\sqrt{n}}\right) \left(\frac{1}{a^a(1-a)^{1-a}}\right)^n = \left(\frac{1}{a^a(1-a)^{1-a}} + o(1)\right)^n; \quad n \rightarrow \infty$$

□

Теорема 2.2.5: Если $k = o(\sqrt{n})$, то $C_n^k \sim \frac{n^k}{k!}$

Доказательство: Распишем биномиальный коэффициент:

$$C_n^k = \frac{n(n-1)\dots(n-k+1)}{k!} = \frac{n^k}{k!} \left(1 - \frac{1}{n}\right) \dots \left(1 - \frac{k-1}{n}\right) = \frac{n^k}{k!} e^{\ln(1-\frac{1}{n}) + \dots + \ln(1-\frac{k-1}{n})}$$

Используем разложение логарифма $\ln(1-x) = -x + O(x^2), x \rightarrow 0$:

$$C_n^k = \frac{n^k}{k!} e^{-\frac{k(k-1)}{n} + O\left(\frac{k^3}{n^2}\right)} \xrightarrow{k=o(\sqrt{n}), n \rightarrow \infty} \frac{n^k}{k!}$$

□