Содержание

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):
- $A \subseteq A$
- $A \subseteq B \land B \subseteq C \Rightarrow A \subseteq C$
- $A = B \Leftrightarrow A \subseteq B \land B \subseteq A$

Лемма 1.1.2 (Свойства равенства):
- $A = A$
- $A = B \land B = C \Rightarrow A = C$
- $A = B \Rightarrow B = A$

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: Нередвко все рассматриваемые множества оказываются подмножествами какого-нибудь множества U.

Такое U называют тогда **универсумом**.

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

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

Теорема 1.1.1 (Основные тождества алгебры множеств): $\forall A, B, C$ и любого включающего их универсума U верно:
- $A \cap B = B \cap A; A \cup B = B \cup A$
- $(A \cap B) \cap C = A \cap (B \cap C); (A \cup B) \cup C = A \cup (B \cup C)$
- $A \cap A = A; A \cup A = A$
- $A \cap (A \cup B) = A; A \cup (A \cap B) = A$
- $\overline{\overline{A}} = A$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C); A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $\overline{A \cap B} = \overline{A} \cup \overline{B}; \overline{A \cup B} = \overline{A} \cap \overline{B}$
- $A \cap \emptyset = \emptyset; A \cup \emptyset = A; A \cap U = A; A \cup U = U; \overline{\emptyset} = U; \overline{U} = \emptyset$
- $A \cap \overline{A} = \emptyset; A \cup \overline{A} = U$

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

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

и **областью значений** отношения R – множество

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

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

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

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

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

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

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

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

Определение 1.2.6: Бинарное отношение R называется:
- **Функциональным**, если $\forall x : \forall y : \forall z : xRy \land xRz \Rightarrow y = z$
- **Инъективным**, если $\forall x : \forall y : \forall z : xRy \land zRy \Rightarrow x = z$
- **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 $f : A \overset{p}{\to} B$.

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

Определение 1.2.8: Множество
$$\{f \in \mathcal{P}(A \times B) \mid f : A \to B\}$$
всех функций из A в B обозначается символом B^A

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

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

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

Определение 1.2.12: Будем писать $A \overset{f}{\sim} B$, если $f : A \to B$ 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 $f : A \to B$. 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 $f : \mathcal{P}(A) \to A$. Положим
$$Y = \{a \in A \mid \forall X \in \mathcal{P}(A) : a = f(X) \Rightarrow a \notin X\}$$
Очевидно, $Y \in \mathcal{P}(A)$. 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. □

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 □

Утверждение 1.2.2:
$$(A \times B)^C \sim A^C \times B^C$$

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

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. □

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

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

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 $\forall x : \forall y : xRy \land yRx \Rightarrow x = y$
- **Транзитивным**, если $\forall x : \forall y : \forall z : xRy \land yRz \Rightarrow xRz$

Лемма 1.3.1: Отношение $R \subseteq A^2$:
- Рефлексивно $\Leftrightarrow \mathrm{id}_A \subseteq R$
- Иррефлексивно $\Leftrightarrow \mathrm{id}_A \cap R = \emptyset$
- Симметрично $\Leftrightarrow R \subseteq R^{-1} \Leftrightarrow R = R^{-1} \Leftrightarrow R^{-1} \subseteq R$
- Антисимметрично $\Leftrightarrow R \cap R^{-1} \subseteq \mathrm{id}_A$
- 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
- $\left(P^{-1}\right)^{-1} = P$
- $(P \cup Q)^{-1} = P^{-1} \cup Q^{-1}$
- $\overline{P}^{-1} = \overline{P^{-1}}$
- $(P \cup Q) \circ R = (P \circ R) \cup (Q \circ R)$
- $(P \cap Q) \circ R \subseteq (P \circ R) \cap (Q \circ R)$

Теорема 1.3.1 (Связь строгих и нестрогих порядков): Положим
$$S(A) = \left\{R \in \mathcal{P}(A^2) \mid R \text{ строгий порядок}\right\}$$
и аналогично выделим множество $N(A)$ всех нестрогих порядков на A.
Рассмотрим функции $\varphi : S(A) \to \mathcal{P}(A^2)$ и $\psi : N(A) \to \mathcal{P}(A^2)$:
$$\varphi(P) = P \cup \mathrm{id}_A \quad \psi(Q) = Q \setminus \mathrm{id}_A$$
Тогда утверждается, что
- $\varphi(P) \in N(A) \land \psi(\varphi(P)) = P$
- $\psi(Q) \in S(A) \land \varphi(\psi(Q)) = Q$

Доказательство: Проверим нестрогость $\varphi(P)$:
- Рефлексивно, так как $\mathrm{id}_A \subseteq \varphi(P)$
- Транзитивно, так как
$$\varphi(P) \circ \varphi(P) = (P \cup \mathrm{id}_A) \circ (P \cup \mathrm{id}_A) =$$
$$(P \circ P) \cup (P \circ \mathrm{id}_A) \cup (\mathrm{id}_A \circ P) \cup (\mathrm{id}_A \circ \mathrm{id}_A) =$$
$$(P \circ P) \cup P \cup \mathrm{id}_A \subseteq P \cup \mathrm{id}_A = \varphi(P)$$
- Антисимметрично, так как
$$\varphi(P) \cap (\varphi(P))^{-1} = (P \cup \mathrm{id}_A) \cap (P \cup \mathrm{id}_A)^{-1} =$$
$$(P \cup \mathrm{id}_A) \cap \left(P^{-1} \cup \mathrm{id}_A\right) = \left(P \cap P^{-1}\right) \cup \mathrm{id}_A = \mathrm{id}_A$$

Итак, $\varphi(P) \in N(A)$. Далее,
$$\psi(\varphi(P)) = (P \cup \mathrm{id}_A) \cap \overline{\mathrm{id}_A} =$$
$$\left(P \cap \overline{\mathrm{id}_A}\right) \cup \emptyset = \left(P \cap \overline{\mathrm{id}_A}\right) \cup (P \cap \mathrm{id}_A) = P \cap \left(\mathrm{id}_A \cup \overline{\mathrm{id}_A}\right) = P \cap A^2 = P$$

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

Итак, $\psi(Q) \in S(A)$. Далее,
$$\varphi(\psi(Q)) = \left(Q \cap \overline{\mathrm{id}_A}\right) \cup \mathrm{id}_A = (Q \cup \mathrm{id}_A) \cap \left(\mathrm{id}_A \cup \overline{\mathrm{id}_A}\right) = Q \cap A^2 = Q$$

$\square$

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 $B^{\triangle}$ – множество всех верхних граней, а также $B^{\triangledown}$ – 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 $B^{\triangle}$.

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

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

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

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 $\overline{X}$ прогрессивно:

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

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

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

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

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 $\overline{X} = \emptyset, X = \mathbb{N}$.

$(3 \Rightarrow 1)$. 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 $X = \mathbb{N}$. □

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

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

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

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

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

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

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

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

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

Определение 1.4.4: Пусть $n \in \mathbb{N}$, тогда определим множество
$$\underline{n} = \{m \in \mathbb{N} \mid m < n\} = \{0, ..., n-1\}$$

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 $f : \underline{n+1} \to \underline{n}$, 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, расммотрим наименьшее такое n.

Заметим, что инъекция $f : \underline{1} \to \underline{0} = \emptyset$ 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 $\operatorname{rng} h \subseteq \underline{m} \Rightarrow h : \underline{m+1} \to \underline{m}$ – инъекция для $m < n$ – противоречие.

□

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

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

Но тогда $f|_{\underline{n+1}} : \underline{n+1} \to \underline{n}$ – тоже инъекция, что противоречит предыдущей лемме. □

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

Доказательство: Согласно теореме о рекурсии, существует функция $\alpha : \mathbb{N} \to \mathcal{P}(A)$
$$\alpha(0) := A \land \alpha(n+1) := \begin{cases} \alpha(n) \setminus \{\min \alpha(n)\}, \alpha(n) \neq \emptyset \\ \emptyset, \text{ else} \end{cases}$$

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 $f : \overline{n_0} \to A$ – биекция
- Иначе $f : \mathbb{N} \to A$, также является биекцией.

$\square$

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

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

Доказательство её биективности тривиально. $\square$

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

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

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

Доказательство её биективности тривиально. $\square$

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

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

$\square$

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 $A^{n+1} = A^n \times A$. $\square$

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

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

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

Если $z' = 0$, то $y = 0, n = k'$. Если же $z' \notin \lim$, то по свойствам $\exists z'' : z' = z'' + 1$, что противоречит минимальности $z' \Rightarrow z' \in \lim$. 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. □

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 $\mathcal{I} = \{I \mid I -$ начальный отрезок $X\}$. Тогда $(\mathcal{I}, \subseteq)$ есть в.у.м.
6. $(\mathcal{I}, \subseteq) \simeq X + 1; (\mathcal{I} \setminus X, \subseteq) \simeq X$

Доказательство:

2. Пусть $x \in \cup_{a \in A} \wedge y < x$. 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 $(\mathcal{I}, \subseteq)$ линеен: все собственные н.о. вложены в X и сравнимы между собой по предыдущему пункту. Выделим в произвольном подмножестве $\mathcal{J} \subseteq \mathcal{I}$ 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'.
6. Изоморфизм строится как $[0, x) \mapsto x$, а X переходит в наибольший элемент множества $X + 1$.

□

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 $f : X \to X$ монотонна. Тогда $\forall x \in X : f(x) \geq x$

Доказательство: От противного. Тогда подмножество

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

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. □

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

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

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

Определение 1.5.6: **Произведением** AB в.у.м. $\left(A, \underset{A}{<}\right)$ и $\left(B, \underset{B}{<}\right)$ называется $(A \times B, <)$:

$$(a_1, b_1) < (a_2, b_2) \coloneqq \left(b_1 \underset{B}{<} b_2\right) \vee \left((b_1 = b_2) \wedge \left(a_1 \underset{A}{<} a_2\right)\right)$$

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

$$(x, \varepsilon) < (y, \delta) \coloneqq (\varepsilon < \delta) \vee \left((\varepsilon = \delta = 0) \wedge \left(x \underset{A}{<} y\right)\right) \vee \left((\varepsilon = \delta = 1) \wedge \left(x \underset{B}{<} y\right)\right)$$

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 $f : A \to \cup A$, т.ч. $f(a) \in a$ для всех $a \in A$.

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

$\Rightarrow$. Тогда $f \circ g = \mathrm{id}_B \Rightarrow \forall b \in B : (b, b) \in f \circ g$, 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 $g : B \to A$, 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. □

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 $(\mathrm{rel}_\sigma, \mathrm{func}_\sigma, \mathrm{const}_\sigma)$, причём $\mathrm{rel}_\sigma \neq \emptyset$ и все элементы кортежа не пересекаются.

Каждому $R \in \mathrm{rel}_\sigma$ и каждому $f \in \mathrm{func}_\sigma$ 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 $(M, \mathcal{R}, \mathcal{R}, \mathcal{F}, \mathcal{C})$
- $\mathcal{S} : \mathrm{rel}_\sigma \cup \mathrm{func}_\sigma \cup \mathrm{const}_\sigma \to \mathcal{R} \cup \mathcal{F} \cup \mathcal{C}$, причём
  - $\forall R^{(n)} \in \mathrm{rel}_\sigma : \mathcal{S}(R) \in \mathcal{R} \land \mathcal{S}(R) \subseteq M^n$
  - $\forall f^{(n)} \in \mathrm{func}_\sigma : \mathcal{S}(f) \in \mathcal{F} \land \mathcal{S}(f) \in M^{M^n}$
  - $\forall c \in \mathrm{const}_\sigma : \mathcal{S}(c) \in \mathcal{C}$

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

Биекция $\alpha : M_1 \to M_2$ называется **изомофизмом 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 предикатому символу сигнатуры, то

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

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

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

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

$$\mathrm{var} = \{x_0, x_1, ..., x_n, ...\}$$

Определение 1.7.6: Правила построения множества **термов** tm_σ над сигнатурой σ:
- $x \in \mathrm{var} \Rightarrow x \in \mathrm{tm}_\sigma$
- $c \in \mathrm{const}_\sigma \Rightarrow c \in \mathrm{tm}_\sigma$
- $f^{(n)} \in \mathrm{func}_\sigma \Rightarrow \forall t_1, ..., t_n \in \mathrm{tm}_\sigma : f(t_1, ..., t_n) \in \mathrm{tm}_\sigma$

Определение 1.7.7: Правила построения множества **формул** fm_σ над сигнатурой σ (булевые операции и кванторы рассматриваются как формальные символы):
- $R^{(n)} \in \mathrm{rel}_\sigma \Rightarrow \forall t_1, ..., t_n \in \mathrm{tm}_\sigma : R(t_1, ..., t_n) \in \mathrm{fm}_\sigma$
- $\varphi, \psi \in \mathrm{fm}_\sigma \Rightarrow \neg\varphi \in \mathrm{fm}_\sigma, \varphi \land \psi \in \mathrm{fm}_\sigma, \varphi \lor \psi \in \mathrm{fm}_\sigma, \varphi \to \psi \in \mathrm{fm}_\sigma$
- $x \in \mathrm{var}, \varphi \in \mathrm{fm}_\sigma \Rightarrow \forall x : \varphi \in \mathrm{fm}_\sigma, \exists x : \varphi \in \mathrm{fm}_\sigma$

Определение 1.7.8: **Оценка переменных** – это любая функция $\pi : \mathrm{var} \to M$

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

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

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

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

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

- $[R(t_1, ..., t_n)](\pi) = 1 \Leftrightarrow ([t_1](\pi), ..., [t_n](\pi)) \in R^{\mathcal{M}}$
- $[\varphi \to \psi](\pi) = 1 \Leftrightarrow [\varphi](\pi) \to [\psi](\pi)$
- $[\forall x : \varphi](\pi) = 1 \Leftrightarrow \forall a \in M : [\varphi](\pi_x^a) = 1$, 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 $V : \mathrm{tm}_\sigma \cup \mathrm{fm}_\sigma \to \mathcal{P}(\mathrm{var})$, причём

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

Определение 1.7.12: Определим функцию, возвращающую **свободные переменные формулы**

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

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

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

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

Определение 1.7.13: Пусть
- $\mathrm{fm}_\sigma(x_1, ..., x_n) := \{\varphi \in \mathrm{fm}_\sigma |\ FV(\varphi) \subseteq \{x_1, ..., x_n\}\}$
- $\mathrm{tm}_\sigma(x_1, ..., x_n) := \{t \in \mathrm{tm}_\sigma |\ V(t) \subseteq \{x_1, ..., x_n\}\}$

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

Пусть $t \in \mathrm{tm}_\sigma(x_1, ..., x_n), \varphi \in \mathrm{fm}_\sigma(x_1, ..., x_n)$:
- $[t]_{\mathcal{M}}(\vec{a}) := [t]_{\mathcal{M}}\left(\pi^{a_1 ... a_n}_{x_1 ... x_n}\right)$
- $[\varphi]_{\mathcal{M}}(\vec{a}) := [\varphi]_{\mathcal{M}}\left(\pi^{a_1 ... a_n}_{x_1 ... x_n}\right)$

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

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. □

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

Определение 1.7.15: **Функция $f : M^n \to M$ выразима в $\boldsymbol{\sigma}$-структуре** $\mathcal{M} \Leftrightarrow \exists t \in \mathrm{tm}_\sigma(x_1, ..., x_n) : t^{\mathcal{M}} = f$

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

$$\mathrm{Aut}\ (\mathcal{M}) = \left\{\alpha \mid \mathcal{M} \overset{\alpha}{\simeq} \mathcal{M}\right\}$$

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.

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

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

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, по по предположению индукции, заменяем формулу под этим квантором на эквивалентную предварённую.

Если φ начинается с отрицания, то по предположению индукции заменяем форумулу под отрицанием на эквивалентную предварённую. Затем проносим отрицание во внутрь, переменяя кванторы.

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

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 $\mathbb{R} \not\simeq \mathbb{Q} \Rightarrow (\mathbb{R}, <) \not\equiv (\mathbb{Q}, <)$

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

Если T – теория и $\varphi \in \mathrm{st}_\sigma$, то

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

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

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

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

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

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

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

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 T-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 $x \in \operatorname{dom} f$ выписывает $f(x)$ и завершается, а на любом входе $x \in A \setminus \operatorname{dom} f$ не завершается ни за какое конечное количество шагов.

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

Определение 1.10.3: Множество A **перечеслимо**, 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 перечеслимо

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 перечеслимы, то перечеслимы
- $A \cup B$
- $A \cap B$
- $A \times B$
- $\mathrm{pr}^i A$

Доказательство: Будем запускать перечесляющие 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 $U : \mathbb{N}^2 \overset{p}{\to} \mathbb{N}$ называется **универсальной вычислимой**, если она вычислима и для всякой вычислимой функции $f : \mathbb{N} \overset{p}{\to} \mathbb{N}$ 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 (**T-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 перечеслимо

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

- $m \in K \Rightarrow f(m)$ 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! □

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 $S : \mathbb{N} \to \mathbb{N}$, 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 $f : \mathbb{N} \to \mathbb{N}$ 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 $V : \mathbb{N}^2 \to \mathbb{N}$ – 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

$\square$

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 $A = \{a_1, ..., a_n\}; B = \{b_1, ..., b_m\}$:

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 $\alpha_1, ..., \alpha_n$.

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:

$$N(\alpha'_1, ..., \alpha'_n) = N - N(\alpha_1) - ... - N(\alpha_n) +$$
$$N(\alpha_1, \alpha_2) + ... + N(\alpha_{n-1}, \alpha_n) - ...$$
$$+(-1)^n N(\alpha_1, ..., \alpha_n)$$

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

$$N(\alpha_1', ..., \alpha_n') = \underbrace{n!}_{N(\emptyset)} - C_n^1 \underbrace{(n-1)!}_{N(\alpha_i)} + C_n^2 \underbrace{(n-2)!}_{N(\alpha_i, \alpha_j)} - ... + (-1)^n C_n^n \underbrace{1}_{N(\alpha_1, ..., \alpha_n)} =$$

$$n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - ... + (-1)^n \frac{1}{n!}\right) \overset{n\to\infty}{\to} \frac{n!}{e}$$

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

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 набор 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 $j = \mathrm{const} \cdot n$ 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
$$(a+b)^n = \underbrace{(a+b)(a+b)...(a+b)}_{n \text{ раз}}$$

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. □

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

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

Количество способов это сделать равно
$$P(n_1, ..., n_t) = C_n^{n_1} C_{n-n_1}^{n_2} ... C_{n-n_1-...-n_{t-1}}^{n_t} =$$
$$\frac{n!}{n_1!(n-n_1)!} \frac{(n-n_1)!}{n_2!(n-n_1-n_2)!} ... \frac{(n-n_1-...-n_{t-1})!}{n_t!(n-n_1-...-n_t)!} =$$
$$\frac{n!}{n_1! n_2! ... n_t!}$$

Оно называется **полиномиальный коэффициентом**

Теорема 2.2.2 (Полиномиальная формула): **Полиномиальной формулой** называется выражение
$$(x_1 + ... x_t)^n = \sum_{n_1+...+n_t=n} P(n_1, ..., n_t) x_1^{n_1} ... x_t^{n_t}$$

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 Паксказя**: $C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$
- $\sum_{k=0}^{n} (-1)^k C_n^k = 0$

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

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

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

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

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

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

$$C_n^{[an]} \sim \frac{\Theta\left(\frac{1}{\sqrt{n}}\right)}{a^{an}(1-a)^{n-an}} = \Theta\left(\frac{1}{\sqrt{n}}\right)\left(\frac{1}{a^a(1-a)^{1-a}}\right)^n =$$

$$\left(\frac{1}{a^a(1-a)^{1-a}} + o(1)\right)^n; \quad n \to \infty$$

□

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

Доказательство: Распишем биномиальный коэффициент:

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

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

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

□

2.3. Определение простого графа, орграфа, мультиграфа, псевдографа, гиперграфа. Маршруты в графах, пути и простые пути, степени вершин. Изоморфизм графов, гомеоморфизм графов. Понятия связности и компонент связности. Три эквивалентных определения деревьев (с использованием условий ацикличности, связности, числа вершин и ребер) с доказательством их эквивалентности. Блоки и точки сочленения, теорема о пересечении блоков (с доказательством) и теорема о графе блоков и точек сочленения (б/д).

Определение 2.3.1: **Графом** называется пара множеств $(V, E) = G$, где V – множество каких-то объектов, а E – множество пар объектов из V.

Определение 2.3.2: **Ориентированным графом** G называется пара $G = (V, E)$, где V – множество вершин, а $E \subseteq V \times V$ – множество **дуг**.

Определение 2.3.3: **Граф с петлями (псевдограф)** – граф, в котором есть ребро, исходящее из вершины и возвращающееся в ту же вершину

Определение 2.3.4: Если v_1, v_2 – вершины, а $e = (v_1, v_2)$ – соединяющее их ребро, тогда вершина v_1 и ребро e **инцидентны**, вершина v_2 и ребро e тоже инцидентны.

Определение 2.3.5: **Граф с кратными рёбрами (мультиграф)** – граф, имеющий рёбра, инцидентные одной паре вершин.

Определение 2.3.6: **Маршрутом** в графе $G = (V, E)$ называется последовательность $v_1 e_1 v_2 ... e_n v_{n+1}$, где вершины v_i могут повторяться, а рёбра e_j инцидентно вершинами v_j, v_{j+1}

Определение 2.3.7: Если все рёбра в маршруте различны, то замкнутый ($v_1 = v_{n+1}$) маршрут называется **циклом**, а незамкнутый – **путём (цепью)**.

Определение 2.3.8: Пусть или цикл называется **простым**, если все вершины в нём различны

Определение 2.3.9: Две вершины u и v называются **связанными**, если в графе G существует путь из u в v.

Определение 2.3.10: **Компонентой связности** называется класс эквивалентности относительно связности.

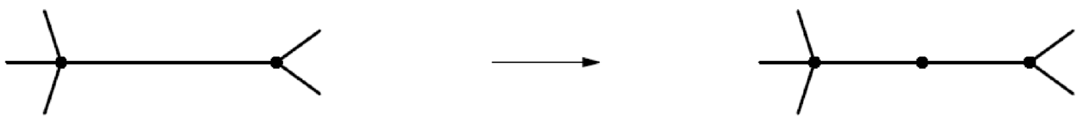
Определение 2.3.11: Граф называется **связным**, если он состоит из одной компоненты связности.

В противном случае граф называется **несвязным**.

Определение 2.3.12: **Гиперграфом** называется пара $H = (V, E)$, где V – множество вершин, а E – произвольное подмножество $\mathcal{P}(V)$.

Определение 2.3.13: Гиперграф называется ***k*-однородным** ($k \geq 2$), если $\forall a \in E : |a| = k$

Определение 2.3.14: Операция **подразделения** ребра показана на рисунке:



Определение 2.3.15: Два графа называются **гомеоморфными**, если от одного можно перейти к другому при помощи подразделения ребра и обратных к ним

Определение 2.3.16: Два графа G_1, G_2 называются **изоморфными**, если существует такая перестановка $\varphi : V(G_1) \to V(G_2)$:

$$\forall (u, v) \in E(G_1) : (\varphi(u), \varphi(v)) \in E(G_2)$$

Определение 2.3.17: Связный граф без циклов называется **деревом**.

Теорема 2.3.1: Для графа $G = (V, E)$ эквивалентны следующие утверждения:
1. G – дерево
2. Любые две вершины графа G соединены единственным простым путём
3. G – связен и $|V| = |E| + 1$
4. G – ацикличен и $|V| = |E| + 1$

Доказательство: $(1 \Rightarrow 2)$:
- Граф связен, поэтому любые две вершины соединены путём
- Граф ацикличен, значит путь единственнен, а также прост, поскольку никому путь не может зайти в одну вершину два раза, потому что это противоречит ацикличности

$(2 \Rightarrow 3)$:
- Очевидно, что граф связан, так как любые две вершины соединены простым путём
- Докажем по индукции соотношение $|V| = |E| + 1$:
  - Утверждение очевидно для связных графов с одной и двумя вершинами
  - Предположим, что оно верно для графов имеющих меньше p вершин
  - Если же граф G имеет p вершин, то удаление из него любого ребра делает граф G несвязным в сиду единственности простых цепей, более того, получаемый граф будет иметь в точности две компоненты. По предположению индукции, в каждой компоненте число вершин на единицу больше числа рёбер.

$(3 \Rightarrow 4)$:
- Представим, что мы добавляем рёбра в граф, после каждого добавления мы обязаны увеличивать наибольшую компоненту связности на 1, иначе в конце граф не станет связным
- Если между какими-то двумя вершинами образовался цикл, то на какой-то итерации мы бы не увеличили компоненту связности, что противоречит условию

$(4 \Rightarrow 1)$:
- Обратно, если мы добавляем по ребру, то в следствие ацикличности, мы должны увеличивать максимальную компоненту связности на 1, иначе после какого-то шага в одной из компонент образуется цикл, что противоречит ацикличности

- Значит после добавления всех рёбер останется 1 компонента связности, что эквивалентно связности графа

□

Определение 2.3.18: **Мост** – это ребро, после удаления которого увеличивается число компонент связности

Определение 2.3.19: **Точка сочленения** – это вершина, после удаления которой увеличивается число компонент связности

Определение 2.3.20: **Блок** – это максимальный по включению связный подграф в графе, в котором нет собственных точек сочленения

Теорема 2.3.2: Любые 2 блока в графе либо не пересекаются, либо пересекаются ровно по одной точке, причём она является точкой сочленения всего графа

Доказательство: Пусть 2 блока пересекаются по ≥ 2 точкам. Тогда рассмотрим подграф-объединение этих двух блоков
- Если мы удалим точку в любом из изначальных блоков, то количество компонент связности не изменится по определению
- Если мы удалим какую-либо из точек пересечения, то останется хотя бы 1 другая, что также не изменит количество компонент связности объединения подграфов
- Получили противоречие с минимальностью по включению каждого из блоков

□

Теорема 2.3.3: Пусть G – связный граф, а $C = \{c_1, ..., c_k\}$ – его точки сочленения и $B = \{b_1, ..., b_l\}$ – его блоки.

Тогда граф $G' = (V', E')$, где
- $V' = C \cup B$
- $E' = \{(b, c) \in B \times C \mid c \in b\} \cup \{(c, b) \in C \times B \mid c \in b\}$

Является деревом

2.4. Планарность графов: определение планарного графа, формула Эйлера, верхняя оценка числа рёбер в планарном графе. Теорема о 5 красках для планарных графов. Критерий Понтрягина–Куратовского (доказательство необходимости; достаточность без доказательства).

Определение 2.4.1: Пусть дан граф $G = (V, E)$.

Укладкой графа G на плоскости назовём пару отображений (F, H):

- $F : V \to S, S \subseteq \mathbb{R}^2, |S| < \infty$ – биекция
- $H : E \to$ кривые на плоскости, причём $(u, v) \in E \Leftrightarrow H(u, v)$ соединяет $F(u)$ cu $F(v)$

Определение 2.4.2: **Плоской (планарной)** называют такую укладку, у которой никакая пара кривых, соответствующих рёбрам графа G, не пересекаются в точках, отличных от образа F.

Причём если две кривые пересекаются в точке, то эта вершина является концом этих кривых.

Определение 2.4.3: Граф называется **планарным**, если существует его плоская укладка на плоскости.

Определение 2.4.4: **Грани** планарной укладки – части плоскости, которые образуются в результате «разрезания» плоскости по рёбрам планарного графа.

Объединение этих граней представляет из себя всю плоскость.

Теорема 2.4.1 (Эйлера): Пусть граф G связен и планарен, $|V| = n; |E| = e$.

Тогда для любой его планарной укладки с числом граней f верно равенство

$$n - e + f = 2$$

Доказательство: Докажем индукцией по величине $e - n$:

- База
$$e - n = -1 \Rightarrow G - \text{дерево} \wedge f = 1$$
- Переход. Поскольку G не дерево, то в нём имеются циклы, удалим из G одно ребро (из некоторого цикла), отделяющее две различные грани. Получим граф G', в котором $f' = f - 1, e' = e - 1, n' = n$:
$$2 = n' - e' + f' = n - (e - 1) + (f - 1) = n - e + f$$

□

Следствие 2.4.1.1: Пусть G – связный планарный граф и есть какая-то его укладка. Пусть t – длина наименьшего цикла в G.

Тогда

$$e \geq \frac{t}{2} f$$

Доказательство: Заметим, что каждая часть ограничена хотя бы t рёбрами, а каждое ребро разделяет две грани, откуда получаем требуемое □

Следствие 2.4.1.2: Пусть G – связный планарный граф и есть какая-то его укладка.

Пусть t – длина наименьшего цикла в G.

Тогда

$$e \leq \frac{t}{t-2}(n-2)$$

Доказательство: По теореме Эйлера:

$$2 = e - n + f \leq n - e + \frac{2e}{t} = \frac{2-t}{t} e + n$$

□

Утверждение 2.4.1: Графы K_5 и $K_{3,3}$ непланарны

Доказательство: Применим отрицание Следствие 2.4.1.2:
- Для $K_5 : n = 5, e = 10, t = 3 \Rightarrow 10 > 9$
- Для $K_{3,3} : n = 6, e = 9, t = 4 \Rightarrow 9 > 8$

□

Теорема 2.4.2 (Критерий Понтрягина-Куратовского): Граф планарен тогда и только тогда, когда он не содержит подграфа, гомеоморфного K_5 или $K_{3,3}$

Доказательство: Ясно, что гомеоморфные графы являются или не являются планарными одновременно, из Утверждение 2.4.1 следует необходимость □

Определение 2.4.5: **Хроматическим числом** графа G называется величина

$$\chi(G) = \min\{k \in \mathbb{N} \mid V = V_1 \sqcup ... \sqcup V_k : \forall i : \forall x, y \in V_i : (x, y) \notin E\}$$

– минимальное число цветов, в которое можно раскрасить вершины графа G так, чтобы концы любого ребра имели разные цвета.

Определение 2.4.6: **Степенью** вершины графа $G = (V, E)$ называют $\deg v$ – число рёбер, которым она инцидентна

Также существует обозначение $\max_{v \in V} \deg v = \Delta(G)$

Лемма 2.4.1 (О рукопожатиях): В любом графе $G = (V, E)$:

$$2|E| = \sum_{v \in V} \deg v$$

Доказательство: Каждое ребро инцидентно каким-то двум вершинам □

Лемма 2.4.2: В любом планарном графе $G = (V, E)$ найдётся вершина степени ≤ 5

Доказательство: Пусть это не так, тогда

$$|E| = \frac{\sum_{v \in V} \deg v}{2} \geq 3|V|$$

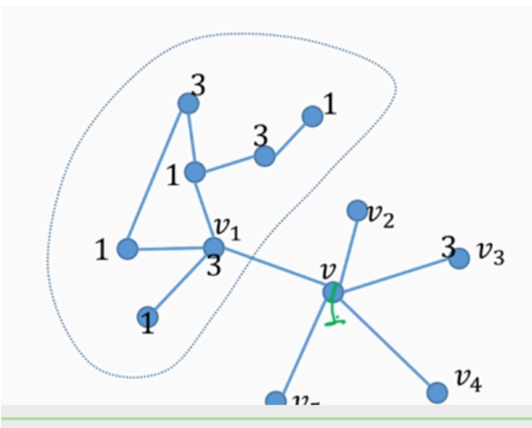
Что противоречит оценке Следствие 2.4.1.2 (для любого графа как минимум $t = 3$). □

Теорема 2.4.3 (О пяти красках): Для любого планарного графа G выполнено

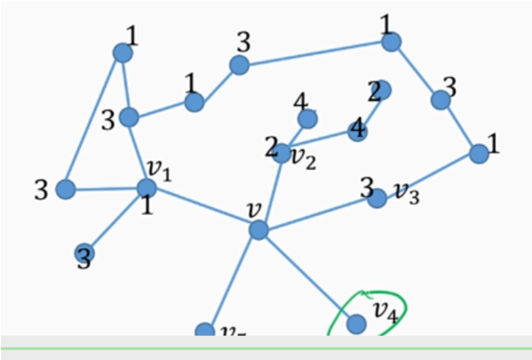
$$\chi(G) \leq 5$$

Доказательство: Будем доказывать индукцией по количеству вершин.

- Переход: по предыдущей лемме $\exists v : \deg v \leq 5$. Тогда рассмотрим случаи:
  - Среди смежных ей вершин нашлось не более 4 различных цветов (то есть $\deg v < 5$ или среди 5 смежных есть хотя бы два повторяющихся цвета). Тогда применим предположение индукции к подграфу без v и покрасим вершину в пятый цвет
  - Иначе рассмотрим конкретную укладку графа и запустим от вершины с цветом 1 BFS, который заходит только в вершины с цветом 1 или 3. Возможны два случая:
    - Если путь выглядит так, то поменяем местами цвета 1 и 3 и мы победили



– Иначе запустим аналогичный BFS из вершины цвета 2 по вершинам цвета 2 или 4, однако в этом случае плохой вариант захода в 4 невозможен, так как для этого нужно будет пересечь «забор» из вершин цвета 1 и 3, что из-за планарности графа невозможно. Меняем местами цвета 2 и 4 и победили



□

2.5. Эйлеровы и гамильтоновы циклы в графах: критерий эйлеровости, алгоритм Флёри (с доказательством корректности), достаточное условие гамильтоновости (теорема Дирака или Оре). Признак Эрдеша-Хватала (б/д). Два необходимых условия гамильтоновости.

Определение 2.5.1: Граф называется **эйлеровым**, если существует замкнутый маршрут, проходящий по всем рёбрам этого графа ровно один раз.

Теорема 2.5.1 (Критерий эйлеровости графа): Для связного графа следующие утверждения эквивалентны:
1. Граф эйлеров
2. Степень каждой вершины графа чётна
3. Множество рёбер графа распадается в объединение непересекающихся по рёбрам простых циклов

Доказательство: $(1 \Rightarrow 2)$:
- Эйлеров граф есть цикл, а цикл есть замкнутый маршрут. Вершина, встречающаяся в этом маршруте, как составляющая, задаётся конструкцией $e_i v_i e_{i+1}$, то есть каждое её вхождение в маршрут увеличивает степень на 2.

  Вхождение в маршрут первой и последней вершины увеличивают степень только на 1, но так как $v_1 = v_{n+1}$, то суммарно степень увеличилась на 2

$(2 \Rightarrow 3)$:

- Зафиксируем вершину x_1 ненулевой степени. Выберем её любую соседнюю вершину x_2. Так как $\deg(x_2) > 0 \wedge \deg(x_2) \vdots 2$, то $\exists x_3 \neq x_1 \in V$, связанная ребром с x_2.

  Будем идти далее по произвольному ребру из только что выбранной вершины x_k, пока не вернёмся в одну из уже выбранных вершин. Тогда мы найдём некоторый простой цикл Z_1.

  Удалим все его рёбра из G и получим новый граф, возможно с несколькими компонентами связности. Проделаем аналогичную операцию в каждой из новых компонент связности и замети, что величина $|E|$ строго уменьшается.

  Проделав данную операцию индуктивно для каждой компоненты, мы разобьём множество E на требуемое объединение.

$(3 \Rightarrow 1)$:
- Доказательство по индукции. Для одного простого цикла утверждение очевидно.

  Предположим, что в G больше простых циклов. Удалим один простой цикл C. Полученный граф G' распадается на некоторые компоненты связности, каждая из которых распадается на простые циклы.

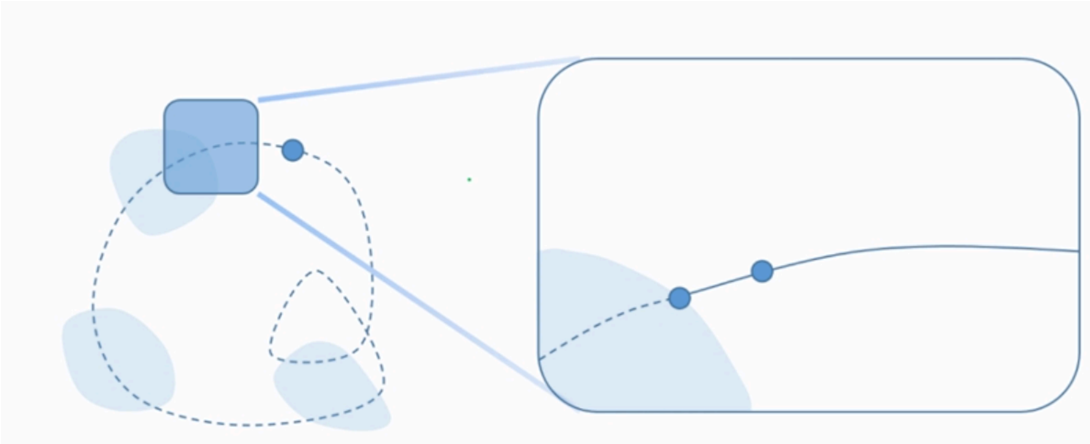
  Начнём обходить граф по вершинам цикла C, причём если мы попали в вершину $v \in V$, лежащую в одной из компонент связности G', то обойдём её по предположению индукции и вернёмся в v.

  Продолжим идти по циклу C, обходя ещё не посещённые компоненты связности G'. Таким образом, мы обойдём весь граф G.

□

Утверждение 2.5.1 (Алгоритм Флёри):
- Стартуем из любой вершины графа
- На каждом шаге проходим ещё не пройденное ребро и удаляем его из графа
- Идём по мосту только если нет другой возможности
- Если идти стало некуда, значит эйлеров цикл только что простроен

Доказательство:
- Построенный алгоритмом маршрут является циклом, так как степень каждой вершины чётная, а значит
  - Невозможна ситуация, когда нам некуда идти,
  - Более того, для достижения чётности начальной вершины, мы обязаны вернуться в неё в конце
- Мы обойдём все рёбра, так как если бы остались непосещённые рёбра, то на каком-то шаге мы бы прошли по мосту, когда существовала альтернатива (голубые зоны – потенциально непосещённые рёбра):



□

Определение 2.5.2: **Гамильтонов путь** – простой путь, проходящий через все вершины графа по одному разу

Определение 2.5.3: **Гамильтонов цикл** – замкнутый гамильтонов путь

Определение 2.5.4: Граф называется **гамильтоновым**, если в нём существует гамильтонов цикл

Теорема 2.5.2 (Дирака): Если в связном графе n вершин и степень любой вершины $\geq \frac{n}{2}$, то этот связный граф – гамильтонов

Доказательство: Пусть $P = v_1 v_2 ... v_k$ – самый длинный путь в графе G.

Если v_1 смежна с некоторой вершиной $x \notin P$, то существует путь длиннее P – противоречие.

Аналогичное рассуждение с $v_k \Rightarrow v_k$ и v_1 смежны только с вершинами из P. Тогда поскольку $\deg(v_1) \geq \frac{n}{2}$ и в графе нет петель, то $k \geq \frac{n}{2} + 1$.

Далее докажем, что существует $j : v_j$ инцидентна с v_k, а v_{j+1} с v_1:

- Предположим, что такой ситуации не оказалось. Тогда в P есть как минимум $\deg(v_1)$ вершин, несвязанных с v_k.

  Поскольку все вершины, связанные с v_k находятся в пути и v_k не инцидентна сама с собой, то в P хотя бы $\deg(v_1) + \deg(v_k) + 1 = n + 1$ вершин – противоречие.

Из утверждения выше следует, что в G существует простой цикл $C = v_{j+1} ... v_k v_j v_{j-1} ... v_1 v_{j+1}$. Покажем, что этот цикл – гамильтонов.

Предположим, что существует $v \in V \setminus C$. Поскольку граф связен, v должна быть связана каким-то путём с некоторой $v_i \in C$, но тогда существует путь P' от v до $C \to$ круг по C, который длиннее, чем P, что противоречит выбору P. □

Определение 2.5.5: **Вершинной связностью** графа G называется минимальное количество вершин, в результате удаления которых граф перестанет быть связным.

Обозначение $\kappa(G)$

Определение 2.5.6: **Числом независимости** графа G называется максимальное количество вершин в свободном от рёбер подмножестве (**независимое подмножество**).

Обозначение $\alpha(G)$

Утверждение 2.5.2: Пусть G – гамильтонов граф.

Тогда

$$\forall \text{ независимого } W : \quad \underbrace{|v(W)|}_{\text{множество соседей}} \geq |W|$$

Доказательство: Гамильтонов цикл содержит все вершины, в том числе все $w \in W$.

Заметим, что после любой вершины из независимого множества должна стоять вершина из $v(W)$, так как никакие две вершины в W не связаны.

А значит соседей у W должно быть как минимум столько же, сколько в нём вершин, чтобы построить корретный цикл. □

Утверждение 2.5.3: Пусть G – гамильтонов граф и S – произвольное непустое множество вершин.

Тогда граф $G \setminus S$ имеет не более $|S|$ компонент связности.

Доказательство: Возьмём гамильтонов цикл исходного графа и, удалив в нём $|S|$ точек, в худшем случае он разобьётся на $|S|$ компонент связности. □

Теорема 2.5.3 (Эрдеша-Хватала): Пусть количество вершин в графе $G(V, E) : |V| \geq 3$ и $\alpha(G) \leq \kappa(G)$.

Тогда граф гамильтонов.

2.6. Хроматическое число, хроматический индекс, число независимости, кликовое число. Нижняя оценка хроматического числа через число независимости и через кликовое число. Теорема Визинга (с доказательством).

Утверждение 2.6.1:
$$\chi(G) \geq \frac{|V|}{\alpha(G)}$$

Доказательство: Действительно, вершины окрашены в один цвет $\Leftrightarrow$ между никакой парой из них нет ребра $\Leftrightarrow$ они лежат в одном независимом подмножестве.
$$|V| = \sum_{i=1}^{\chi(G)} |V_i| \leq \chi(G) \max|V_i| \leq \chi(G)\alpha(G)$$

□

Определение 2.6.1: **Кликовым числом** графа G называется
$$\omega(G) = \max\{k \in \mathbb{N} \mid \exists W \subseteq V : |W| = k \land \forall x, y \in W : (x, y) \in E\}$$

Утверждение 2.6.2 (Свойства кликового числа):
- $\alpha(G) = \omega\left(\overline{G}\right)$
- $\chi(G) \geq \max\left\{\omega(G), \frac{|V|}{\alpha(G)}\right\}$

Доказательство:
- Очевидно, что наличие ребра между вершинами в графе эквивалентно отсутствию оного в дополнении графа
- Очевидно, что мы не сможем покрасить граф в число, меньшее велечине максимальной клики, так как вершины в ней попарно связаны

□

Определение 2.6.2: **Хроматический индекс** графа G – минимальное число цветов, в которое можно раскрасить рёбра графа так, что любые два смежных ребра не одноцветны.

Обозначение $\chi'(G)$.

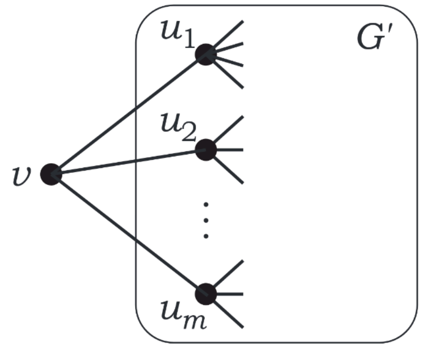
Лемма 2.6.1: Пусть $G = (V, E)$ и v – его вершина, причём $\deg v \leq k$.

Если степень каждого из соседей v также не превосходит k, причём степень k достигается не более чем для одного из соседей v, то если рёбра графа $G \setminus \{v\}$ можно покрасить в k цветов, то в k цветов можно покрасить и рёбра графа G

Доказательство: Докажем по индукции. Для $k = 1$ – это либо мост, либо изолированная вершина, доказано.

Переход. Пусть $u_1, ..., u_m$, где $m = \deg v$ – соседи вершины v в графе G, из которых БОО $\deg u_1 = k$, а deg остальных равен $k - 1$.

Тогда в $G' = G \setminus \{v\}$ они имеют степени $k - 1$ и $k - 2$ соответственно:



Для каждого цвета i пусть $X_i \subseteq \{u_1, ..., u_m\}$ – подмножество вершин-соседей, в которые не попадает цвет i, то есть, никакие инцидентные им рёбра не раскрашены в этот цвет.

Тогда вершина u_1 имеющая степень $k - 1$ попадает ровно в одно из множеств $X_1, ..., X_k$, а остальные – ровно в два. Отсюда суммарное число элементов в этих множествах равно

$$\sum_{i=1}^{k} |X_i| = 2 \deg v - 1 < 2k$$

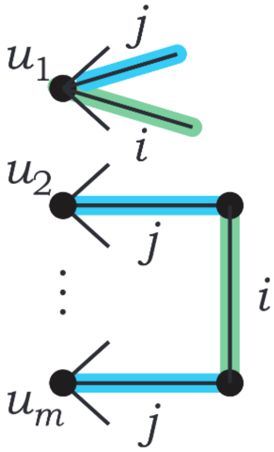
Пусть число вхождений каких-то двух цветов различается более чем на два, то есть

$$|X_i| > \left|X_j\right| + 2$$

Тогда рассмотривается подграф $G'_{i,j}$ графа G', образованный рёбрами, раскрашенными в цвета i и j.

Каждый компонент связности в этом подграфе – это или простой путь, или простой цикл; в них чередуются i-рёбра и j-рёбра.

Каждая вершина, не принадлежащая $X_i \cap X_j$ попадает в один из этих компонент связности:



Тогда непременно найдётся компонент, в который попадает больше вершин из X_i, чем вершин из X_j (по принципу Дирихле). Тогда этот путь можно перекрасить, поменяв местами цвета i и j. При этом $|X_i|$ уменьшится на 1 или 2, а $|X_j|$ на столько же увеличится.

Повторив такое перекрашивание необходимое число раз, можно добиться неравенства

$$\forall i, j : \left||X_i| - |X_j|\right| \leq 2$$

Поскольку сумма $\sum_{i=1}^{k} |X_i|$ нечётна, то хотя бы одно из её слагаемых должно быть нечётным $\Rightarrow$ хотя бы одно слагаемое должно быть равно 1, поскольку в противном случае все слагаемые меньше или равны двум, и их сумма будет не менее $2k$.

Пусть $X_i = \{u_l\}$ – найденное выше множество. Далее, строится граф $\tilde{G} = (V, \tilde{E})$, полученный из G удалением ребра (u_l, v), а также всех рёбер, покрашенных в G' в цвет i.

Степень вершины v уменьшилась на единицу и степени всех соседей v также уменьшились на единицу каждая – применимо предположении индукции, согласно которому, рёбра графа $\tilde{G}$ раскрашиваются в $k - 1$ цветов.

Осталось вернуть все удалённые из G рёбра и покрасить их в цвет i. □

Теорема 2.6.1 (Визинга): Для любого графа G:

$$\chi'(G) \leq \Delta(G) + 1$$

Доказательство: Пусть G_i – подграф G на вершинах $v_1, ..., v_i$.

Утверждается, что рёбра каждого G_i можно покрасить в $\Delta(G) + 1$ цветов.

База индукции по i очевидна – одинокая вершина.

Иначе для перехода применяем лемму, так как степень каждой вершины подграфов $\leq \Delta(G) + 1$. □

2.7. Системы общих представителей (с.о.п.): определение, примеры задач, сводящихся к построению с.о.п.. Тривиальные верхняя и нижняя оценки размера минимальной с.о.п.. Жадный алгоритм построения с.о.п., теорема о верхней оценке размера «жадной с.о.п.». Теорема о неулучшаемости этой оценки в общем случае (б/д).

Определение 2.7.1: Определим гиперграф $H = (R_n, \mathcal{M})$, где
- $R_n := \{1, ..., n\}$
- $\mathcal{M} \subseteq \mathcal{P}(R_n)$

Тогда **системой общих представителей (соп)** для совокупности множеств $\mathcal{M}$ назовём любое

$$S \subseteq R_n : \forall M \in \mathcal{M} : M \cap S \neq \emptyset$$

Также введём величину $\tau(\mathcal{M})$ – минимальная мощности соп для данной совокупности множеств $\mathcal{M}$

Пусть $\forall M \in \mathcal{M} : |M_i| = k; |\mathcal{M}| = s$ и $M_i \subseteq R_n$.

При фиксированных n, s, k обозначим $\mathcal{M}$ с такими параметрами за $\mathcal{M}(n, k, s)$.

Теорема 2.7.1 (Тривиальная оценка сверху):

$$\forall n, k, s \in \mathbb{N} : \forall \mathcal{M}(n, k, s) : \tau(\mathcal{M}) \leq \min\{s, n-1\}$$

Доказательство: От $n - k + 2$ до n ровно $k - 1$, а значит если мы возьмём все числа от 1 до $n - k + 1$, то мы не сможем получить пустое пересечение с каким-либо представителем, так как в нём не найдётся k не взятых нами чисел. □

Теорема 2.7.2 (Тривиальная оценка снизу):

$$\forall n, k, s \in \mathbb{N} : \exists \mathcal{M}(n, k, s) : \tau(\mathcal{M}) \geq \min\left\{\left[\frac{n}{k}\right], s\right\}$$

Доказательство: Возможны два случая:
1. $s \leq \left[\frac{n}{k}\right]$. Тогда $\mathcal{M} = \{\{1, ..., k\}, \{k+1, ..., 2k\}, ..., \{(s-1)k+1, ..., sk\}\}$
2. $s > \left[\frac{n}{k}\right]$. В таком случае строим систему $\mathcal{M}$ аналогично предыдущему случаю, но в дополнение добиваем её до s случайным подмножествами.

□

Теорема 2.7.3 (Жадный алгоритм): По сути, формулировка есть в шпаргалке.

$$\forall n, k, s : \forall \mathcal{M}(n, k, s) : \tau(\mathcal{M}) \leq \max\left\{\frac{n}{k}, \frac{n}{k} \ln \frac{sk}{n}\right\} + \frac{n}{k} + 1$$

Доказательство: Возможны следующие случаи:
1. $s \leq \frac{n}{k} \Rightarrow \tau(\mathcal{M}) \leq s \leq \frac{n}{k}$
2. $\frac{n}{k} \ln \frac{sk}{n} \geq n \Rightarrow \tau(\mathcal{M}) \leq n \leq \frac{n}{k} \ln \frac{sk}{n}$
3. $s > \frac{n}{k} \wedge \frac{n}{k} \ln \frac{sk}{n} < n$

Для доказательства последнего случая воспользуемся жадным алгоритмом построения соп.

Возьмём любой элемент $\nu_1 \in R_n$, который принадлежит наибольшему числу множеств в $\mathcal{M}$.

Пусть их ρ_1 штук. Тогда $\rho_1 \geq \frac{sk}{n}$, поскольку $sk = \sum_{i=1}^{n} \sum_{M \in \mathcal{M}} \mathbb{I}\{i \in M\} \leq \rho_1 n$.

Выкинем из $\mathcal{M}$ все множества, содержащие ν_1. Осталась совокупность $\mathcal{M}_1 : |\mathcal{M}_1| = s - \rho_1 =: s_1$. Снова сделаем шаг жадного алгоритма.

Сделаем $N = \left[\frac{n}{k} \ln \frac{sk}{n}\right] + 1$ шагов жадного алгоритма, причём $\rho_i \geq \frac{s_{i-1} k}{n}$.

После этого имеем построенное жадным алгоритмом множество $S = \{\nu_1, ..., \nu_N\}$ и совокупность $\mathcal{M}_N$, такую, что

$$|\mathcal{M}_n| = s_N = s_{N-1} - \rho_N \leq s_{N-1} - \frac{s_{N-1} k}{n} \leq ... \leq$$

$$s\left(1 - \frac{k}{n}\right)^N = se^{N \ln\left(1 - \frac{k}{n}\right)} \leq se^{-\frac{kN}{n}} \leq se^{-\ln \frac{ks}{n}} = \frac{n}{k}$$

Итого $\tau(\mathcal{M}) \leq M + \frac{n}{k} \leq \frac{n}{k} \ln \frac{sk}{n} + 1 + \frac{n}{k}$ □

Теорема 2.7.4 (Неулучшаемость жадной соп): По сути, формулировка есть в шпаргалке.

Пусть k, s такие, что

$$\exists n_0 : \forall n \geq n_0 : 2 \leq \ln \frac{sk}{n} \leq k \leq \frac{n}{8} : \exists \mathcal{M}(n, k, s) : \tau(\mathcal{M}) \geq \frac{1}{16} \frac{n}{k} \ln \frac{sk}{n}$$

2.8. Числа Рамсея: определение, и точные значения $R(s,t)$ при $s \leq 3, t \leq 4$. Верхняя оценка Эрдёша-Секерёша, её следствие для диагональных чисел Рамсея; нижняя оценка диагональных чисел с помощью простого вероятностного метода.

Определение 2.8.1: Пусть $s, t \in \mathbb{N}$.

Тогда **числом Рамсея** называют величину

$$R(s, t) := \min\{n \in \mathbb{N} \mid \forall G = (V, E) : |V| = n \wedge (\omega(G) \geq s \vee \alpha(G) \geq t)\}$$

Замечание 2.8.1:
1. Число Рамсея симметрично по своим аргументам
2. $R(1, t) = 1$ – любая вершина является кликой
3. $R(2, t) = t$ – в случае антиклики придётся взять в независимое множестве все вершины

Теорема 2.8.1 (Эрдеша-Секёреша):
$$R(s, t) \leq R(s-1, t) + R(s, t-1)$$

Доказательство: Пусть $n := R(s-1, t) + R(s, t-1)$.

Зафиксируем произвольную раскраску K_n в 2 цвета и вершину $v \in V$. Из неё выходит $n - 1$ ребро.

От противного получаем, что из неё выходит либо $\geq R(s-1, t)$ красных рёбер, либо $\geq R(s, t-1)$ синих.

Без ограничения общности считаем, что $\geq R(s-1, t)$ красных.

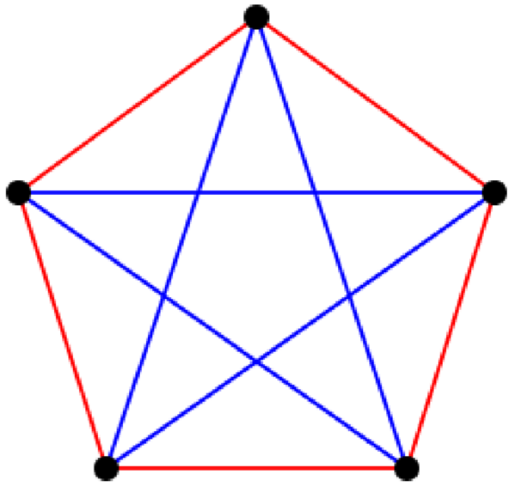
Построим новый граф состоящий только из красных рёбер, выходящих из v. Поскольку $|V_1| \geq R(s-1, t)$, то в V_1 есть либо синий K_t, либо красный K_{s-1}, который вместе с вершиной v даёт искомый красный K_s. $\square$

Следствие 2.8.1.1 *(Для диагональных чисел)*:
$$R(s, s) \leq C_{2s-2}^{s-1}$$

Следствие 2.8.1.2: Если $R(s-1, t)$ и $R(s, t-1)$ – чётные числа, то можно усилить оценку
$$R(s, t) \leq R(s-1, t) + R(s, t-1) - 1$$

Теорема 2.8.2:
$$R(3, 3) = 6$$

Доказательство: Покажем, что для K_5 найдётся такая, раскраска, при которой в нём не будет ни синего, ни красного K_3:



Стало быть, $K(3,3) > 5$.

Воспользуемся Теорема 2.8.1 и получим, что

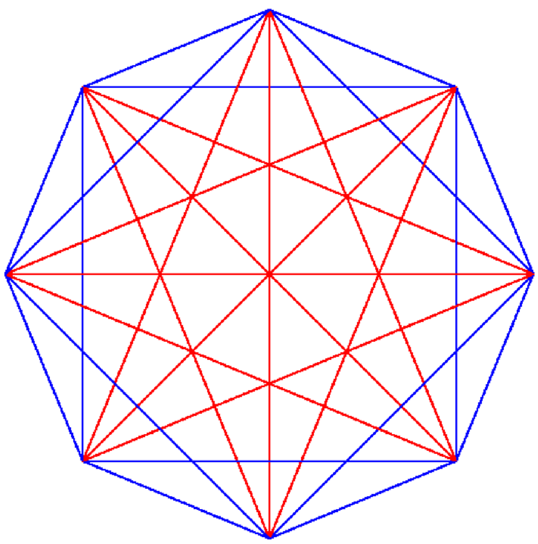
$$R(3,3) \le R(2,3) + R(3,2) = 6$$

$\square$

Теорема 2.8.3:

$$R(3,4) = 9$$

Доказательство: Покажем, что для K_8 найдётся такая, раскраска, при которой в нём не будет ни синего K_4, ни красного K_3:



Стало быть, $K(3,4) > 8$.

Воспользуемся Следствие 2.8.1.2 и получим, что

$$R(3,4) \le R(3,3) + R(2,4) - 1 = 9$$

$\square$

Теорема 2.8.4:
$$R(s,s) \geq (1+o(1))\frac{s2^{\frac{s}{2}}}{\sqrt{2}e}$$

Доказательство: Пусть $n := (1+o(1))\frac{s2^{\frac{s}{2}}}{\sqrt{2}e}$. Покажем, что существует раскраска K_n, в которой нет одноцветного K_s.

Рассмотрим случайную раскраску рёбер K_n в два цвета, где $\mu(\{e \text{ красное}\}) = \mu(\{e \text{ синее}\}) = \frac{1}{2}$.

Пусть $S \subseteq V; |S| = s$. Тогда вероятность события A_s того, что клика на этих вершинах будет одноцветной:
$$\mu(A_s) = 2s^{-C_n^2}$$

Посчитаем вероятность по всем наборам вершин:
$$\mu\Big(\cup_{S\subseteq V, |S|=s} A_S\Big) \leq \sum_{S\subseteq V, |S|=s} \mu(A_s) = C_n^s 2^{1-C_s^2} \leq \frac{n^s}{s!}2^{1-C_s^2} =$$

$$\frac{n^s}{s!}2^{1-\frac{s(s-1)}{2}} \overset{n:=(1+o(1))\frac{s2^{\frac{s}{2}}}{\sqrt{2}e}}{=} \frac{1}{s!}(1+o(1))^s s^s \frac{2^{\frac{s^2}{2}}}{2^{\frac{s}{2}}e^s} 2^{1-\frac{s^2}{2}+\frac{s}{2}} = \frac{2s^s}{e^s s!}(1+o(1))^s \overset{\text{Стирлинга}}{=}$$

$$\frac{2}{\sqrt{2\pi s}}\frac{(1+o(1))^s}{1+o(1)}$$

Причём в итоговой формуле можно подогнать $o(1)$ так, чтобы полученное число было < 1 при всех s □

2.9. Совершенные паросочетания. Теорема Холла (б/д). Использование теоремы Холла для доказательства того, что k-регулярный двудольный граф содержит k непересекающихся совершенных паросочетаний. Экстремальная теория графов: теорема Турана.

Определение 2.9.1: **Паросочетанием** называется множество рёбер без общих вершин

Определение 2.9.2: Паросочетание $P \subseteq E$ графа $G = (V,E)$ **покрывает** набор вершин $S \subseteq V$, если
$$\forall v \in S : \exists e \in P : \exists u \in V : e = (v,u) \vee e = (u,v)$$

Определение 2.9.3: Паросочетание называется **совершенным**, если оно покрывает все вершины.

Теорема 2.9.1 (Холла): Пусть G – двудольный граф с долями X и Y. ($|X| \leq |Y|$)

Тогда в нём $\exists$ совершенное паросочетание

$$\Leftrightarrow \forall A \subseteq X : |v(A)| \geq |A|$$

Пример: Любой k-регулярный двудольный граф содержит k непересекающихся совершенных паросочетаний, так как мы можем применить теорему Холла k раз, выкидывая выбранные рёбра после каждого шага.

Стоит учесть, что после какого-то шага условие для изначальных долей будет нарушено, поэтому потребуется их переопределить

Теорема 2.9.2 (Турана): Пусть $G = (V, E)$

Если

- $|V| = n$
- $\omega(G) \leq k$
- $|E|$ максимально возможное для таких n и k

Тогда G – полный k-дольный, с почти равными долями (отличающимися не более, чем на 1).

Доказательство: Заметим, что полная многодольность графа G эквивалентна свойству

$$\forall u, v, w \in V : (u, v) \notin E \wedge (v, w) \notin E \Rightarrow (u, w) \notin E$$

От противного, допустим, что $(u, v), (v, w) \notin E$, но $(u, w) \in E$. Докажем, что тогда такой граф не мог быть максимальным по количеству вершин.

Пусть $\deg v < \deg u$. Тогда выкинем из графа все рёбра, инцидентные v и соединим v со всеми вершинами, смежными u:

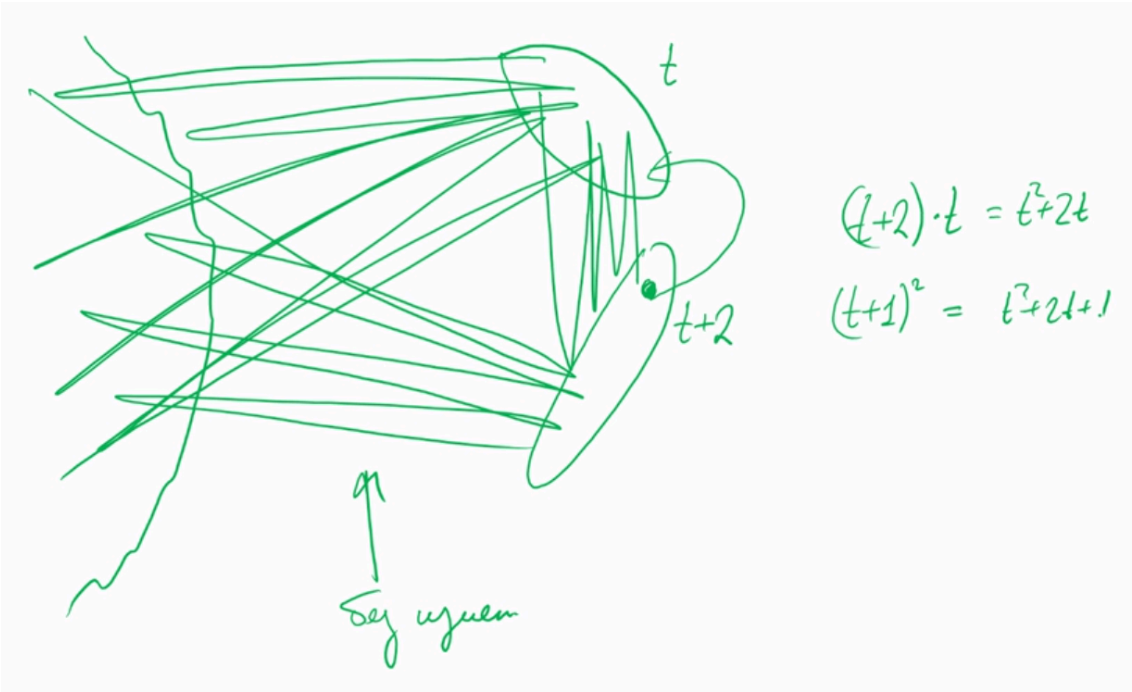
Заметим, что клика большего размера появиться не могла, так как:

- Она содержит либо u, либо v, но не обе сразу
- Если она содержит только u, то она была в исходном графе
- Если она содержит только v, то при замене на $v \to u$ получим клику такого же размера (так как у v теперь все соседи совпадают с u) и снова получим клику большего размера в исходном графе

Заметим, что случай $\deg v < \deg w$ полностью аналогичен рассмотренному только что.

В случае же $\deg(v) \geq \deg(u) \wedge \deg(v) \geq \deg(w)$ перевесим соседей v на u и w, проведя аналогичные рассуждения о невозможности появляения клики большего размера.

Осталось доказать «почти-равнодольность» долей полученного полного графа: перебросим вершину из большей доли в меньшую и получим увеличение числа рёбер, подробнее на пикче



$\square$