Содержание

1 Множества

1.1 Вопросы на удос

1.1.1 Включение и равенство множеств. Основные способы задания множеств

Включение и равенство множеств

Лемма о свойствах включения

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

Лемма о свойствах равенства

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

Основные способы задания множеств

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

1.1.2 Операции алгебры множеств и их основные свойства

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

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

Доказательство:

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

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

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

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

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

Доказательство очевидное.

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

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

Композиция и обращение отношений

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

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

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

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

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

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

Доказательство:

Для произвольной пары (a, d) имеем

$(a, d) \in R \circ (Q \circ P) \Leftrightarrow \exists c(a(Q \circ P)c \wedge cRd) \Leftrightarrow \exists c \exists b(aPb \wedge bQc \wedge cRd) \Leftrightarrow \exists b(aPb \wedge \exists C(bQc \wedge cRd)) \Leftrightarrow \exists b(aPb \wedge b(R \circ Q)d) \Leftrightarrow (a, d) \in (R \circ Q) \circ P$

Обращение композиции Пусть P и Q - бинарные отношения. Тогда $(Q \circ P)^{-1} = P^{-1} \circ Q^{-1}$

Доказательство:

Для произвольной пары (a, c) получаем

$(a, c) \in (Q \circ P)^{-1} \Leftrightarrow (c, a) \in Q \circ P \Leftrightarrow \exists b(cPb \wedge bQa) \Leftrightarrow \exists b((b, c) \in P^{-1} \wedge (a, b) \in Q^{-1}) \Leftrightarrow (a, c) \in P^{-1} \circ Q^{-1}$.

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

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

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

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

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

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

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

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

Обращение таких отношений

1. R функционально $\Leftrightarrow R^{-1}$ инъективно.

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

Доказывается непосредственной проверкой.

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

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

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

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

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

Доказательство:

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

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

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

1. $f \upharpoonright X : X \xrightarrow{p} B$

2. Если f инъективно, то инъективно и $f \upharpoonright X$

3. Если f тотальна для A и $X \subset A$, то $f \upharpoonright X$ тотальна для X.

1.1.6 Инъекции, сюръекции и биекции. Критерий биективности отношения

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

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

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

Доказательство.

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

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

1.1.7 Аксиома выбора. Существование правой обратной у каждой сюръекции

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

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

Доказательство.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Доказательство.

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

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

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

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

Частично упорядоченное множество

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Цепи и антицепи

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

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

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

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

Решётки

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

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

Линейные порядки

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

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

Изоморфизм ч.у.м.

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

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

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

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

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

Классы эквивалентности и их свойства

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

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

классом эквивалентности элемента x по отношению E.

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

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

Доказательство.

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

Фактор-множество и разбиение множества

Определение фактор-множества Множество

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

называется фактор-множеством множества A по отношению E.

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

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

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

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

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

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

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

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

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

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

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

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

Доказательство.

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

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

Примеры рассуждений с характеристическими функциями.

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

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

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

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

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

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

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

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

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

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

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

1.1.14 Мощности множеств ...

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Доказательство.

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

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

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

Конкатенация слов, пустое слово

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

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

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

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

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

Доказательство.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1. В X есть наименьший элемент (обозначаемый 0 или 0_X)

2. Y есть в.у.м. относительно $<|_{Y^2}$

3. Если $Y \neq \varnothing$, то существует $\inf Y$

4. Если $x < s$, то существует и единственен y, называемый последователем x (обозначение $y = x + 1$), т.ч. $x < y \wedge \forall z > x\, (y \leqslant z)$ (эквивалентно, $y = \min\{z \mid z > x\}$)

5. Если существует верхняя грань Y, то существует (и единственен) $\sup Y$.

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

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

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

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

Доказательство.

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

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

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

1.1.19 Теорема о строении элементов в.у.м.

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

Доказательство.

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

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

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

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

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

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

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

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

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

Доказательство. Требуемые изоморфизмы несложно построить непосредственно.