Московский физико-технический институт
Физтех-школа прикладной математики и информатики

ОСНОВЫ КОМБИНАТОРИКИ И ТЕОРИИ ЧИСЕЛ

I СЕМЕСТР

Лекторы: *Райгородский Андрей Михайлович*

h\nu

Авторы: *Дамир Ачох*

Проект на Github

осень 2021

Содержание

1 Наивная теория множеств

Определение 1.1. Множество - это совокупность некоторых объектов. Каждый объект входит в множество не более 1 раза, иначе - это мультимножество.

Определение 1.2. $x \in Y$. Объект x является элементом множества Y.

Определение 1.3. $X \subset Y$. Множество X является подмножеством множества Y. $X \subset Y \overset{def}{\Leftrightarrow} (a \in X \Rightarrow a \in Y)$

Определение 1.4. Множества X и Y равны, если $(X \subset Y) \wedge (Y \subset X)$.

Утверждение 1.1. *Равенство множеств обладает следующими свойствами:*

1. *Рефлексивность* $(X = X)$.
2. *Транзитивность* $((X = Y) \wedge (Y = Z) \Rightarrow X = Z)$.
3. *Симметричность* $(X = Y \Rightarrow Y = X)$.

Утверждение 1.2. *Отношение подмножества обладает следующими свойствами:*

1. *Рефлексивность* $(X \subset X)$.
2. *Транзитивность* $((X \subset Y) \wedge (Y \subset Z) \Rightarrow X \subset Z)$.
3. *Антисимметричность* $((X \subset Y) \wedge (Y \subset X) \Rightarrow Y = X)$.

1.1 Операции над множествами

1. Объединение $A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$
2. Пересечение $A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}$
3. Разность $A \setminus B = \{x \mid (x \in A) \wedge (x \notin B)\}$
4. Симметрическая разность $A \triangle B = \{x \mid (x \in A) \oplus (x \in B)\}$
5. Дополнение $\overline{A} = \{x \mid x \notin A\}$

1.2 Упорядоченные пары и кортежи

Законы де Моргана:

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

Определение 1.5. Неупорядоченная пара - множество из двух элементов (возможно, одинаковых). Обозначение: $\{a, b\}$.

Определение 1.6. Упорядоченная пара - неупорядоченная пара, в которой зафиксирован первый элемент. Обозначение: (a, b).

Определение 1.7. Упрощенное определение Куратовского: $(a, b) = \{\{a, b\}, a\}$.

Определение 1.8. Полное определение Куратовского: $(a, b) = \{\{a, b\}, \{a\}\}$.

Определение 1.9. Декартово произведение $A \times B = \{(a, b) \mid (a \in A) \wedge (b \in B)\}$.

Определение 1.10. Кортеж длины 0 - это $\varnothing$. Кортеж длины $(n + 1)$ - это $\{a, \{a, t\}\}$, где t - кортеж длины n.

2 Отображения и соответствия

Определение 2.1. Соответствие из A в B - произвольное подмножество $A \times B$. $F \subset A \times B$. Обозначения: $(a, b) \in F$, $b \in F(a)$, $F : A \rightrightarrows B$.

Определение 2.2. Отображение - однозначное соответствие. Т.е. $(\forall a \in A)(\exists! b \in B)$. Обозначения: $(a, b) \in F$, $b = F(a)$, $F : A \to B$.

Определение 2.3. Инъективное соответствие: $(a \neq b) \Rightarrow (F(a) \cap F(b) = \varnothing)$.

Определение 2.4. Инъекция - это инъективное отображение. $(a \neq b) \Rightarrow (F(a) \neq F(b))$.

Определение 2.5. Сюръективное соответствие: $(\forall b \in B)(\exists a \in A)\ b \in F(a)$.

Определение 2.6. Сюръекция - сюръективное отображение. $(\forall b \in B)(\exists a \in A)\ b = F(a)$.

Определение 2.7. Биекция - отображение, являющееся и инъекцией и сюръекцией одновременно (взаимно однозначное соответствие). $((\forall a \in A)(\exists! b \in B)\ (a, b) \in F) \land ((\forall b \in B)(\exists! a \in A)\ (a, b) \in F)$.

Определение 2.8. Пусть $S \subset A$. Образ множества S - это $F(S) = \bigcup\limits_{a \in S} F(a)$

Определение 2.9. Пусть $T \subset B$. Прообраз множества T - это $F^{-1}(T) = \{a \mid F(a) \cap T \neq \varnothing\}$

2.1 Композиция соответствий

Определение 2.10. Пусть $F : A \rightrightarrows B$, $G : B \rightrightarrows C$. Композиция F и G - это соответствие $G \circ F : A \rightrightarrows C$, т.ч. $(x, z) \in G \circ F \Rightarrow (\exists y \in B)\ ((x, y) \in F \land (y, z) \in G)$.

Замечание. Если F и G - отображения, то $G \circ F(x) = G(F(x))$.

Замечание. Композиция соответствий ассоциативна. $H \circ (G \circ F) = (H \circ G) \circ F$.

Определение 2.11. Существует отображение F из множества A в A, т.ч. $(\forall a \in A)\ F(a) = a$.