Записки по дискретна математика и алгоритми

М. Соскова

20 януари 2015 г.

Съдържание

1 Множества и операции с тях **3**
- 1.1 Примери за множества . . . 3
  - 1.1.1 Празното множество . . . 3
  - 1.1.2 Основни числови множества . . . 3
- 1.2 Основни релации между множества . . . 4
- 1.3 Начини за задаване на множества . . . 5
  - 1.3.1 Задаване на множество чрез изреждане . . . 5
  - 1.3.2 Задаване на множество с отделяне от друго множество 5
- 1.4 Булеви операции с множества . . . 6
  - 1.4.1 Сечение на множества . . . 6
  - 1.4.2 Обединение на множества . . . 8
  - 1.4.3 Разлика и допълнение на множества . . . 9
  - 1.4.4 Обобщено обединение и сечение . . . 11
- 1.5 Степенно множество . . . 13
- 1.6 Задачи за упражнение . . . 13

2 Релации **17**
- 2.1 Наредени двойки, декартово произведение . . . 17
- 2.2 Релации . . . 19
  - 2.2.1 Представяне на релации . . . 19
  - 2.2.2 Операции над релации . . . 20
  - 2.2.3 Видове релации . . . 21
- 2.3 Релация на еквивалентност . . . 23
- 2.4 Частична наредба . . . 24
- 2.5 Задачи за упражнение . . . 28

3 Функции **33**
- 3.1 Дефиниция . . . 33
- 3.2 Операции над функции . . . 34
  - 3.2.1 Образ, първообраз, рестрикция и затваряне . . . 34
  - 3.2.2 Композиция на функции . . . 35
  - 3.2.3 Инекция, сюрекция, биекция . . . 36
- 3.3 Някои по-важни функции . . . 37
  - 3.3.1 Идентитет . . . 37
  - 3.3.2 Характеристична функция . . . 38
  - 3.3.3 Фамилии от множества, редици от множества . . . 38
- 3.4 Мощност на множество . . . 39
- 3.5 Задачи за упражнение . . . 43

4 Комбинаторика **47**
4.1 Основни комбинаторни принципи . . . 47
4.1.1 Принцип за биекцията . . . 47
4.1.2 Принцип за събирането . . . 47
4.1.3 Принцип за умножението . . . 50
4.2 Основни комбинаторни конфигурации . . . 50
4.2.1 Конфигурации с повторение, с наредба . . . 51
4.2.2 Конфигурации с наредба, без повторение . . . 52
4.2.3 Конфигурации без повторение, без наредба . . . 52
4.2.4 Конфигурации без наредба, с повторение . . . 55
4.3 Задачи за упражнение . . . 56

5 Дискретни функции **60**
5.1 Булеви функции.Представяния. . . . 60
5.2 Пълни множества булеви функции . . . 63
5.3 Затворени множества булеви функции . . . 68
5.3.1 Булеви функции запазващи константите . . . 68
5.3.2 Самодвойнствени булеви функции . . . 69
5.3.3 Линейни булеви функции . . . 70
5.3.4 Монотонни булеви функции . . . 70
5.4 Теорема на Пост-Яблонски . . . 72
5.5 Задачи за упражнение . . . 74

6 Графи и алгоритми за графи **79**
6.1 Основни дефиниции . . . 79
6.1.1 Представяне на графи . . . 80
6.1.2 Някои основни характеристики на граф . . . 81
6.1.3 Цикли. Ойлеров и Хамилтонов цикъл. . . . 83
6.2 Дървета . . . 87
6.3 Покриващо дърво . . . 88
6.3.1 Обхождане на графи . . . 89
6.3.2 Минимално покриващо дърво . . . 93
6.4 Минимален път. Алгоритъм на Дийкстра . . . 97
6.5 Задачи за упражнение . . . 99

Библиография **102**

Глава 1

Множества и операции с тях

Определение 1.1. Множество наричаме съвкупност от определени различни един от друг елементи.

Множествата ще означаваме с латински букви: A,B,C,...,X,Y,Z, a,b,c, ...,x,y,z. Основна характеристика на едно множество е кои елементи му принадлежат. Затова, ако A е множество, въвеждаме кратко означение:

- $x \in A$ за "елементът x принадлежи на множеството A".
- $x \notin A$ за "елементът x не принадлежи на множеството A".

1.1 Примери за множества

1.1.1 Празното множество

Множеството, което не съдържа нито един елемент, наричаме празното множество. Означаваме празното множество със специален символ $\emptyset$.

1.1.2 Основни числови множества

- Множеството на естествените числа означаваме с $\mathbb{N}$. Елементите на това множеството са числата 0,1,2,...,35,....678,...
- Множеството на целите числа означаваме с $\mathbb{Z}$. Елементите на това множеството са всяко естествено число n, както и неговото противоположно $-n$.
- Множеството на рационалните числа означаваме с $\mathbb{Q}$. Елементите на това множеството са числата, които могат да се представят като p/q, където p е цяло, а q е естествено число различно от 0.
- Множеството на реалните числа означаваме с $\mathbb{R}$. Всяко реално число може да се представи като граница на редица от рационални числа. Например числото e е граница на редицата $\{(1 + 1/n)^n\}$.
- Множеството на комплексните числа означаваме с $\mathbb{C}$. Всяко комплексно число може да се представи като $a + i.b$, където a и b са реални числа.

1.2 Основни релации между множества

Основни релации между две множества са релацията "подмножество", релацията "равенство" и релацията "строго подмножество".

Определение 1.2. Нека A и B са множества. Казваме, че A е под- множество на B, ако всеки елемент на A е елемент на B.

$$A \subseteq B \Leftrightarrow \forall x(x \in A \to x \in B).$$

За да докажем, че множеството A е подмножество на множеството B използваме следния шаблон:
Нека x е произволен елемент на множеството A.
....
Така $x \in B$. Тъй като x беше избран като произволен елемент на A, това е в сила за всеки елемент на A. Следователно $A \subseteq B$.

Забележка! Релацията "подмножество" е рефлексивна: за всяко множество A, $A \subseteq A$.

Твърдение 1.3. Празното множество е подмножество на всяко множество.

Доказателство. Нека A е произволно множество. Да допуснем, че $\emptyset \nsubseteq A$. Тогава има елемент x, за който $x \in \emptyset$ и $x \notin A$. Но $\emptyset$ няма нито един елемент, следователно допускането води до противоречие. Така допускането е грешно и следователно $\emptyset \subseteq A$. □

Твърдение 1.4. Релацията "подмножество" е транзитивна. Нека A, B и C са произволни множества. Ако $A \subseteq B$ и $B \subseteq C$, то $A \subseteq C$.

Доказателство. Нека A, B и C са множества такива, че $A \subseteq B$ и $B \subseteq C$. Нека x е произволен елемент на . Тогава щом, $A \subseteq B$, x е елемент и на B. Щом $B \subseteq C$, x е елемент и на C. Тъй като x беше избран като произволен елемент на A, това е в сила за всеки елемент на A. Следователно $A \subseteq C$. □

Определение 1.5 (Аксиома за обема)**.** Нека A и B са множества. Казваме, че $A = B$, ако $A \subseteq B$ и $B \subseteq A$.

Твърдение 1.6. Ако $n \in \mathbb{N}$, $n \geq 2$ и $A_1, A_2, \ldots A_n$ са множества, за които $A_1 \subseteq A_2 \subseteq A_3 \cdots \subseteq A_n \subseteq A_1$, то $A_1 = A_2 = \cdots = A_n$.

Доказателство. Доказателството ще извършим с индукция по n.
База: При $n = 2$ твърдението е точно аксиома за обема.
Индукционно предположение: Нека твърдението е в сила за произволно дадени n множества.
Индукционна стъпка: Нека $A_1, A_2, \ldots A_n, A_{n+1}$ са множества, за които:

$$A_1 \subseteq A_2 \subseteq A_3 \cdots \subseteq A_n \subseteq A_{n+1} \subseteq A_1.$$

Тогава от транзитивност на релацията $\subseteq$, и $A_n \subseteq A_{n+1}$, $A_{n+1} \subseteq A_1$, следва, че $A_n \subseteq A_1$. Съгласно индукционното предположение, $A_1 = A_2 \cdots = A_n = A$. Така $A_n = A \subseteq A_{n+1}$ и $A_{n+1} \subseteq A_1 = A$. От аксиомата за обема следва, че $A_1 = A_2 = \cdots = A_n = A_{n+1}$. □

Определение 1.7. Нека A и B са множества. Казваме, че A е строго подмножество на B, ако A е подмножество на B и A не е равно на B:

$$A \subset B \Leftrightarrow A \subseteq B \ \& \ A \neq B.$$

За да докажем, че множеството A е строго подмножество на множеството B използваме следния шаблон:
Нека x е произволен елемент на множеството A.
....
Така $x \in B$. Тъй като x беше избран като произволен елемент на A, това е в сила за всеки елемент на A. Следователно $A \subseteq B$.
Елементът .... принадлежи на B и не принадлежи на A. Следователно $A \subset B$.

Забележка! Релацията "строго подмножество" е антирефлексивна: никое A не е строго подмножество на себе си.

1.3 Начини за задаване на множества

1.3.1 Задаване на множество чрез изреждане

Нека множеството се състои от елементите $x_1, x_2, \dots x_k$. Тогава можем да зададем множеството A като изредим неговите елементи, заградени във фигурни скоби и отделени със запетая:

$$A = \{x_1, x_2, \dots, x_k\}.$$

Редът, в който изреждаме елементите на множество, няма значение, на пример:

$$\{1, 2, 3\} = \{1, 3, 2\} = \{2, 1, 3\} = \{2, 3, 1\} = \{3, 1, 2\} = \{3, 2, 1\}.$$

Повторението на елементи също няма значение, на пример:

$$\{1, 2, 3\} = \{1, 2, 2, 3\} = \{1, 2, 2, 2, 3\}.$$

Този метод на задаване на множество е приложим само за крайни множества, а на практика само за множества с малко на брой елементи.

1.3.2 Задаване на множество с отделяне от друго множество

Ако искаме да зададем безкрайно множество, например множеството от всички четни числа, $2\mathbb{N}$, не бихме могли да изредим всичките му елементи. В най-добрия случай бихме могли да ирзедим първите няколко елемента на това множество и след последната запетая да поставим многоточие:

$$2\mathbb{N} = \{0, 2, 4, 6, 8, \dots\}$$

Този начин за дефиниция на множеството на четните числа разчита на това, че всеки би могъл да се досети по какъв начин трябва да се попълни многоточието. Наистина, първите няколко елемента подсещат за специфично свойство, което характеризира четните числа: едно естествено число е четно, тогава и само тогава, когато се дели на две.

Така получаваме втори метод за задаване на множество. От дадено множество можем да отделим всички елементи, които изпълняват някакво свойство, и от тях да образуваме ново множество. Свойствата, обикновено се описват с формули. Ако P е свойство, то с $P(x)$, ще означим твърдението "x има свойството P".

Определение 1.8 (Аксиома за отделянето)**.** Нека A е множество, а P е свойство. Тогава съвкупността от всички елементи на A, които имат свойството P също е множество, което задаваме чрез:

$$\{x \in A \mid P(x)\}.$$

Така множеството от всички четни числа можем да зададем чрез:

$$2\mathbb{N} = \{x \in \mathbb{N} \mid \exists k(x = 2k)\}.$$

Забележка! Ограничението винаги да отделяме елементи от друго дадено множество е съществено и не може да се премахне.

Твърдение 1.9. Не съществува множество U, чиито елементи са всички множества.

Доказателство. Да допуснем, че съществува множество U, чиито елементи са всички множества. Да разгледаме свойството P, което е в сила за едно множество X, ако $X \notin X$. С аксиома за отделянето можем да образуваме множеството:

$$R = \{X \in U \mid X \notin X\}.$$

Но тогава достигаме до противоречие, когато разгледаме въпроса, дали самото множество R изпълнява свойството P:

$$R \in R \Leftrightarrow R \notin R.$$

Следователно допускането е грешно и не съществува множество на всички множества. □

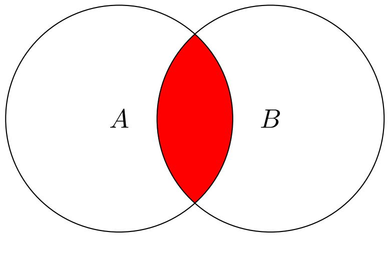
1.4 Булеви операции с множества

1.4.1 Сечение на множества

Определение 1.10. Нека A и B са множества. Сечението на множествата A и B е множеството

$$A \cap B = \{x \mid x \in A \ \& \ x \in B\}.$$

За графично представяне на булеви операции с множества е удобно да се използват диаграми на Вен. Сечението се представя със следната диаграма.



Твърдение 1.11. Нека A и B са множества. Сечението на A и B е най-голямото множество по отношение на релацията $\subseteq$, което е подмножество на A и B

Доказателство. За да докажем това твърдение трябва да покажем, две неща:

1. Самото сечение е подмножество и на двете дадени множества: $A \cap B \subseteq A$ и $A \cap B \subseteq B$. Но това следва директно от дефиницията на операцията сечение. Наистина ако $x \in A \cap B$, то $x \in A$, следователно $A \cap B \subseteq A$, и $x \in B$, следователно $A \cap B \subseteq B$.

2. Всяко друго множество, което подмножество и на двете дадени множества, е подмножество на тяхното сечение: Ако $X \subseteq A$ и $X \subseteq B$, то $X \subseteq A \cap B$.

   Нека $X \subseteq A$ и $X \subseteq B$. Нека $x \in X$. Тогава понеже $X \subseteq A$, имаме, че $x \in A$. От $X \subseteq B$, следва, че $x \in B$. Така $x \in A$ и $x \in B$, и следователно $x \in A \cap B$.

□

В следващото твърдение са събрани някои основни свойства на операцията сечение. Тяхното доказателство се провежда по схемата за доказателство за равенства между множества. Ние ще илюстрираме тази схема само за едно свойство. Останалите доказателства са аналогични.

Твърдение 1.12. Нека A, B и C са множества.

1. Комутативност: $A \cap B = B \cap A$.

2. Асоциативност: $(A \cap B) \cap C = A \cap (B \cap C)$.

3. Идемпотентност: $A \cap A = A$.

4. $A \cap \emptyset = \emptyset$.

Доказателство. (2.) За да докажем, че две множества са равни, трябва да покажем, че първото е подмножество на второто и второто е подмножество на първото. Затова нека x е произволен елемент на $(A \cap B) \cap C$. Съгласно дефиницията на операцията сечение това означава, че $x \in A \cap B$ и $x \in C$. Отново разписваме дефиницията на сечение и получаваме, че $x \in A$ и $x \in B$. Щом $x \in B$ и $x \in C$, то $x \in B \cap C$. Щом $x \in A$ и $x \in B \cap C$, то $x \in A \cap (B \cap C)$. Така получаваме, че $(A \cap B) \cap C \subseteq A \cap (B \cap C)$.

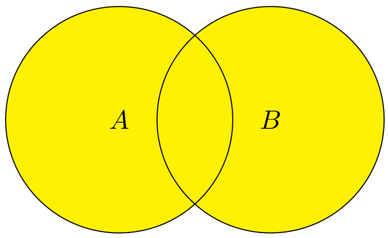
Нека сега x е произволен елемент на $A \cap (B \cap C)$. Съгласно дефиницията на операцията сечение това означава, че $x \in A$ и $x \in B \cap C$. Отново разписваме дефиницията на сечение и получаваме, че $x \in B$ и $x \in C$. Щом $x \in A$ и $x \in B$, то $x \in A \cap B$. Щом $x \in A \cap B$ и $x \in C$, то $x \in (A \cap B) \cap C$. Така получаваме, че $A \cap (B \cap C) \subseteq (A \cap B) \cap C$. Съгласно аксиомата за обема $(A \cap B) \cap C = A \cap (B \cap C)$. □

Определение 1.13. Множества A и B наричаме непресичащи се, ако $A \cap B = \emptyset$. Множества $A_1, A_2, \dots A_n$ наричаме взаимно непресичащи се, ако за всяка двойка различни индекси $i \neq j$, A_i и A_j са непресичащи се.

1.4.2 Обединение на множества

Определение 1.14. Нека A и B са множества. Обединението на множествата A и B е множеството

$$A \cup B = \{x \mid x \in A \vee\ x \in B\}.$$



Операцията обединение е дуална на операцията сечение. Свойствата на обединението са подобни на свойствата на сечението, и се доказват по аналогичен начин. Оставяме ги за упражнение.

Твърдение 1.15. Нека A и B са множества. Обединението на A и B е най-малкото множество по отношение на релацията $\subseteq$ множество, на което A и B са подмножества.

Доказателство. За да докажем това твърдение трябва да покажем, две неща:

1. A и B са подмножества на $A \cup B$.
2. Ако $A \subseteq X$ и $B \subseteq X$, то $A \cup B \subseteq X$.

□

Твърдение 1.16. Нека A, B и C са множества.

1. Комутативност: $A \cup B = B \cup A$.
2. Асоциативност: $(A \cup B) \cup C = A \cap (B \cup C)$.
3. Идемпотентност: $A \cup A = A$.
4. $A \cup \emptyset = A$.

Допълнително свойство на обединението и сечението са законите за дистрибутивност на двете операции.

Твърдение 1.17. Нека A, B и C са множества.

1. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
2. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Доказателство. Ще докажем първия закон за дистрибутивност.

Нека x е произволен елемент на $A \cup (B \cap C)$. Тогава $x \in A$ или $x \in B \cap C$. Имаме две възможности:
I сл.: $x \in A$. Ние вече видяхме, че $A \subseteq A \cup B$ и $A \subseteq A \cup C$. Тогава $x \in A \cup B$ и $x \in A \cup C$ и следователно $x \in (A \cup B) \cap (A \cup C)$.

II сл.: $x \in B \cap C$. Тогава $x \in B$ и $x \in C$. Но $B \subseteq A \cup B$ и $C \subseteq A \cup C$. Тогава $x \in A \cup B$ и $x \in A \cup C$ и следователно и в този случай $x \in (A \cup B) \cap (A \cup C)$.

Така и в двата случая получаваме, че $x \in (A \cup B) \cap (A \cup C)$, следователно $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.

Нека x е произволен елемент на $(A \cup B) \cap (A \cup C)$. Тогава $x \in (A \cup B)$ и $x \in (A \cup C)$. Тогава $x \in A$ или $x \in B$. Освен това $x \in A$ или $x \in B$. Имаме две възможности:

I сл.: $x \in A$. Но $A \subseteq A \cup (B \cap C)$ и следователно $A \cup (B \cap C)$.

II сл.: $x \notin A$. Тогава единствената възможност остава $x \in B$ и $x \in C$. Тогава $x \in B \cap C$. Но $B \cup C \subseteq A \cup (B \cap C)$ и следователно $x \in A \cup (B \cap C)$.

Така и в двата случая получаваме, че $x \in A \cup (B \cap C)$, следователно $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

От аксиомата за обема следва, че $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. $\square$

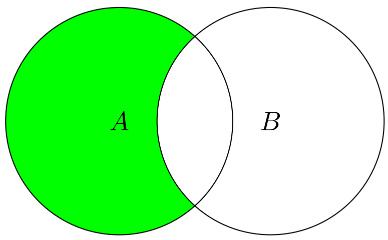
Когато A и B са непресичащи се множества с краен брой елементи, лесно можем да преброим елементите на $A \cup B$. Просто трябва да съберем броя на елементите на A с броя на елементите на B. Брой на елементи на множество A ще означаваме с $|A|$. Така *принципа за събирането* може да се изкаже накратко така:

$$A \cap B = \emptyset \Rightarrow |A \cup B| = |A| + |B|.$$

1.4.3 Разлика и допълнение на множества

Определение 1.18. Нека A и B са множества. Разликата на множествата A и B е множеството

$$A \setminus B = \{x \mid x \in A \ \&\ x \notin B\}.$$



Забележка! Операцията разлика не е комутативна и не е асоциативна, т.е. в общия случай

$$A \setminus B \neq B \setminus A$$

и

$$(A \setminus B) \setminus C \neq A \setminus (B \setminus C)$$

За да се уверите в това, начертайте диаграма на Вен за всеки от изразите. Това ще ви ориентира за конкретен контрапример.

Законите на Де Морган дават връзка между операциите сечение, обединение и разлика.

Твърдение 1.19. Нека A, B и C са множества.

1. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$;

2. $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

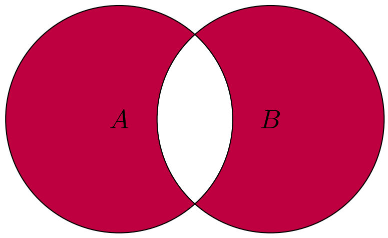
Доказателство. Ще докажем втория закон на Де Морган.

Нека $x \in A \setminus (B \cup C)$. Тогава $x \in A$ и $x \notin B \cup C$. Щом $x \notin B \cup C$, не е вярно, че $x \in B$ или $x \in C$. Това означава, че нито $x \in B$, нито $x \in C$, или по друг начин казано: $x \notin B$ и $x \notin C$. Така $x \in A$ и $x \notin B$, следователно $x \in A \setminus B$. От друга страна $x \in A$ и $x \notin C$ и така $x \in A \setminus C$. От дефиницията на сечение на две множества следва, че $x \in (A \setminus B) \cap (A \setminus C)$. Така $A \setminus (B \cup C) \subseteq (A \setminus B) \cap (A \setminus C)$.

Нека сега $x \in (A \setminus B) \cap (A \setminus C)$. Тогава $x \in A \setminus B$ и $x \in A \setminus C$. Така $x \in A$, $x \notin B$ и $x \notin C$. Тогава $x \notin B \cup C$ и следователно $x \in A \setminus (B \cup C)$. От дефиницията на операцията разлика, получаваме второто включване: $(A \setminus B) \cap (A \setminus C) \subseteq A \setminus (B \cup C)$. Следователно двете множества са равни. $\square$

Определение 1.20. Нека A и B са множества. Симетрична разликата на множествата A и B е множеството

$$A \Delta B = \{x \mid x \in A \;\&\; x \notin B\} \cup \{x \mid x \in B \;\&\; x \notin A\}.$$



За упражнение проверете, че релацията симетрична разлика е комутативна и асоциативна. Също, че:

$$A \Delta B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$$

Често пъти ще се случва да ограничим нашите разглеждания на множества до всички подмножества на някое отнапред зададено множество U. В такъв случай U ще наричаме универсум U. При такова условие можем да дефинираме допълнение на множество $A \subseteq U$:

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

Законите на Де Морган в този случай изглеждат така:

1. $\overline{B \cap C} = \overline{B} \cup \overline{C}$;

2. $\overline{B \cup C} = \overline{B} \cap \overline{C}$.

В този случай можем да формулираме и още един закон, който произлиза от логическия закон за двойното отрицание:

$$\overline{\overline{A}} = A.$$

1.4.4 Обобщено обединение и сечение

Нека I е непразно множество и с всеки елемент от $i \in I$ сме свързали множество A_i. Тогава I наричаме индексно множество, а съвкупността от всички индексирани множества: $\{A_i \mid i \in I\} = \{A_i\}_{i\in I}$, ще наричаме фамилия от множества, индексирана с I.

Определение 1.21. Нека I е индексно множество и $\{A_i\}_{i\in I}$ е фамилия от множества, индексирана с I.

1. Обобщено обединение на $\{A_i\}_{i\in I}$ наричаме множеството

$$\bigcup_{i\in I} A_i = \{x \mid \exists i \in I(x \in A_i)\}.$$

2. Обобщено сечение на $\{A_i\}_{i\in I}$ наричаме множеството

$$\bigcap_{i\in I} A_i = \{x \mid \forall i \in I(x \in A_i)\}.$$

Лесно се вижда, че много от свойствата на сечение и обединение се пренасят към обобщените операции. Например за всяко $i \in I$ $\bigcap_{i\in I} A_i \subseteq A_i$ и $A_i \subseteq \bigcup_{i\in I} A_i$. В сила е и следната характеризация:

Твърдение 1.22. Нека X е множество, I е индексно множество и $\{A_i\}_{i\in I}$ е фамилия от множества, индексирана с I.

1. $X \subseteq \bigcap_{i\in I} A_i \Leftrightarrow \forall i(X \subseteq A_i)$.
2. $\bigcup_{i\in I} A_i \subseteq X \Leftrightarrow \forall i(A_i \subseteq X)$.

Доказателство. Ще покажем второто твърдение. Трябва да покажем еквивалентност на две условия, следователно трябва да докажем, че от първото следва второто и от второто следва първото:

Нека $\bigcup_{i\in I} A_i \subseteq X$. Нека i е произволен индекс. Тогава $_i \subseteq \bigcup_{i\in I} A_i$. От транзитивност на релацията $\subseteq$, получаваме, че $A_i \subseteq X$. Тъй като i беше избран като произволен индекс, това е в сила за всяко i.

Нека сега за всеки индекс i, $A_i \subseteq X$. Нека $x \in \bigcup_{i\in I} A_i$. Тогава има индекс i такъв, че $x \in A_i$. Да фиксираме един такъв индекс i_0. Тогава $x \in A_{i_0} \subseteq X$, следователно $x \in X$. Така $\bigcup_{i\in I} A_i \subseteq X$. $\square$

Дистрибутивните закони и законите на Де Морган също могат да се обобщят:

Твърдение 1.23. Нека X е множество, I е индексно множество и $\{A_i\}_{i\in I}$ е фамилия от множества, индексирана с I.

1. $X \cap \bigcup_{i\in I} A_i = \bigcup_{i\in I}(X \cap A_i)$.
2. $X \cup \bigcap_{i\in I} A_i = \bigcap_{i\in I}(X \cup A_i)$.
3. $X \setminus \bigcap_{i\in I} A_i = \bigcup_{i\in I}(X \setminus A_i)$.
4. $X \setminus \bigcup_{i\in I} A_i = \bigcap_{i\in I}(X \setminus A_i)$.

Доказателство. Ще покажем (3). Нека $x \in X \setminus \bigcap_{i \in I} A_i$. Тогава $x \in X$ и $x \notin \bigcap_{i \in I} A_i$. Не е вярно, че $\forall i \in I (x \in A_i)$, следователно има поне едно i, за което $x \notin A_i$. Нека $i_0 \in I$ е такова, че $x \notin A_{i_0}$. Имаме, че $x \in X$ и $x \notin A_{i_0}$. Следователно $x \in X \setminus A_{i_0}$. Така получаваме, че съществува индекс i, за който $x \in X \setminus A_i$, (а именно $i = i_0$). Съгласно дефиницията на обобщено обединение, $x \in \bigcup_{i \in I} (X \setminus A_i)$. Така $X \setminus \bigcap_{i \in I} A_i \subseteq \bigcup_{i \in I} (X \setminus A_i)$. Обратното включване се показва аналогично. □

Нека отново ограничим разглежданията си до универсум U. Операцията обобщеното обединение ни дава нов метод за дефиниция на множество: индуктивно задаване на множество.

Определение 1.24. Нека $A \subseteq U$ е множество, а f е правило (функция), което на елементи $x \in U$ съпоставя елементи $f(x) \in U$. С индукция по $n \in \mathbb{N}$ дефинираме фамилия от множества, индексирана с $\mathbb{N}$.
База: $A_0 = A$.
И.П.: Нека сме дефинирали множеството A_n.
И.С.: Тогава $A_{n+1} = A_n \cup \{f(x) \mid x \in A_n\}$.

Множеството $\mathcal{A} = \bigcup_{n \in \mathbb{N}} A_n$ наричаме множеството получено индуктивно от A по правилото f.

Интуицията, която стои зад тази дефиниция, е следната. Започвайки от множеството A, добавяме нови и нови елементи всеки път, когато правилото f съпоставя на някой от добавените елементи, някой нов, докато не получим множество $\mathcal{A}$, което има свойството, че ако x е елемент на $\mathcal{A}$, то $f(x)$ също е елемент на $\mathcal{A}$. Такива множества наричаме затворени относно правилото f.

Ще дадем втора еквивалентна дефиниция, която изказва точно тази дефиниция:

Твърдение 1.25. Нека $\mathcal{A}$ е множество получено индуктивно от A по правилото f. Тогава $\mathcal{A}$ е най-малкото, по отношение на релацията $\subseteq$, множество, което съдържа A е е затворено по отношение на правилото f.

Доказателство. Отново трябва да покажем две неща:

1. $\mathcal{A}$ изпълнява тези условия. Наистина, $A = A_0 \subseteq \bigcup_{n \in \mathbb{N}} A_n$, следователно $\mathcal{A}$ съдържа A. Нека сега $x \in \mathcal{A}$. Съгласно дефиницията на обобщено обединение, има индекс n, такъв че $x \in A_n$. Нека n_0 е такъв индекс. От дефиницията на фамилията $\{A_n\}_{n \in \mathbb{N}}$ следва, че $f(x) \in A_{n_0+1} \subseteq \bigcup_{n \in \mathbb{N}} A_n$. Следователно $\mathcal{A}$ е затворено относно правилото f.

2. Нека X е множество, което съдържа A и е затворено относно f. С индукция по n ще покажем, че за всяко n $A_n \subseteq X$ и следователно $\mathcal{A} = \bigcup_{n \in \mathbb{N}} A_n \subseteq X$.

   $A_0 = A \subseteq X$ съгласно избора на X.

   Нека $A_n \subseteq X$. Понеже X е затворено относно f, за всяко $x \in A_n$, $f(x) \in X$. Така $\{f(x) \mid x \in A_n\} \subseteq X$ и следователно $A_{n+1} = A_n \cup \{f(x) \mid x \in A_n\} \subseteq X$.

1.5 Степенно множество

Определение 1.26. Нека A е множество. Степенното множество на A е множеството 2^A, чиито елементи са всички подмножества на A.

$$2^A = \{B \mid B \subseteq A\}.$$

Забележка! Понякога степенното множество на A се означава с $\mathcal{P}(A)$.

Например ако $A = \{1, 2, 3\}$, то

$$2^A = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}.$$

Теорема 1.27. Нека е множество с n на брой елементи. Тогава 2^A име 2^n на брой елементи:

$$|2^A| = 2^{|A|}.$$

Доказателство. Ще докажем твърдението с индукция по n.
Единственото множество с 0 на брой елементи е $\emptyset$. $2^\emptyset = \{\emptyset\}$ е множество с един елемент, синглетон. $1 = |2^\emptyset| = 2^{|\emptyset|}$.
Нека твърдението е вярно за множества с n елемента. И нека е множество с $n+1$ елемент. Нека $x \in A$. Ще разделим 2^A на две непресичащи се множества: $U_0 = \{B \mid B \subseteq A \ \&\ x \notin B\}$ и $U_1 = \{B \mid B \subseteq A \ \&\ x \in B\}$. Така $2^A = U_0 \cup U_1$ и съгласно принципа за събирането $|2^A| = |U_0| + |U_1|$.

$B \in U_0$ тогава и само тогава когато $B \subseteq A \setminus \{x\}$. Следователно $U_0 = 2^{A \setminus \{x\}}$. $A \setminus \{x\}$ е множество с n елемента. Съгласно индукционното предположение $|U_0| = 2^n$.

Всеки елемент $B \in U_1$ може да се представи като $B = \{x\} \cup C$, където $C \in U_0$. Следователно броят на елементите на U_1 е равен на броя на елементите на U_0.

Така $|2^A| = |U_0| + |U_1| = 2^n + 2^n = 2^{n+1}$.

Съгласно метода на математическата индукция, твърдението е в сила за всяко $n \in \mathbb{N}$. □

1.6 Задачи за упражнение

Задача 1. Нека A е множеството от всички положителни естествени числа, които са по-малки или равни на 10. Нека B е множеството от всички прости числа, които са по-малки от 11. Нека C е множеството от всички нечетни естествени числа, които са по-големи от 1 и по-малки или равни на 6. Нека D е множеството от числата 1 и 2, а E е множеството с единствен елемент 1. Задайте всяко от множествата с изреждане на елементите му. Определете за всяка двойка множества, дали първото е подмножество на второто.

Задача 2. Кое от следните твърдения е вярно:

1. $\{1, 2\} \in \{\{1, 2, 3\}, 1, 2, \{1, 3\}\}$.
2. $\{1, 2\} \subseteq \{\{1, 2, 3\}, 1, 2, \{1, 3\}\}$.

Задача 3. Дайте пример за множества A, B и C, такива че:

1. $A \in B$, $B \in C$, $A \notin C$.
2. $A \subseteq B$, $B \subseteq C$, $A \in C$.
3. Всеки елемент на A е подмножество на A.

Задача 4. Кои от следните двойки множества са равни:

1. $\{1, 3, 4, 5, 6\}$ и $\{6, 4, 5, 3, 1\}$.
2. $\{9, 5, 7\}$ и $\{9, 9, 9, 5, 5, 7, 7\}$.
3. $\{0, 2, 8\}$ и $\left\{\sqrt{2}, 5 - 5, 2^3\right\}$.
4. $\{7\}$ и 7.
5. $\{\{8\}\}$ и $\{8\}$.

Задача 5. Верни ли са следните твърдения:

1. Ако $A \subseteq B$ и $B \subseteq C$, то $A \subseteq C$.
2. Ако $A \subseteq B$ и $C \subseteq B$, то $A \subseteq C$.
3. Ако $A \subseteq B$, то $A \subset B$ или $A = B$.
4. Ако $A = B$, ако нито $A \subset B$, нито $B \subset A$.
5. Ако $A \subseteq B$ и $B \subset C$, то $A \subset C$.
6. Ако $A \subset B$ и $B \subseteq C$, то $A \subset C$.

Задача 6. Нека $A = \{x \in \mathbb{R} \mid |x| \leq 1\}$, $B = \{x \in \mathbb{R} \mid |x - 1| \leq \frac{1}{2}\}$. Намерете: $A \cap B$; $A \cup B$; $A \setminus B$ и $A \Delta B$.

Задача 7. Покажете че за всяко множество A:

1. $\emptyset \subseteq A$.
2. $A \subseteq \emptyset \Leftrightarrow A = \emptyset$.
3. $A \cup \emptyset = A$.
4. $A \cap \emptyset = \emptyset$.
5. $A \setminus \emptyset = A$.
6. $\emptyset \setminus A = \emptyset$.
7. $A \Delta \emptyset = A$.

Задача 8. Докажете свойствата на обединение и сечение от Твърдения 1.12, 1.16 и 1.17, на които не е представено доказателство.

Задача 9. Вярно ли е, че:

1. $A \setminus B = B \setminus A$.
2. $(A \setminus B) \setminus C = A \setminus (B \setminus C)$.
3. $A \setminus (A \setminus B) = A \cap B$.
4. $A \setminus (B \cup C) = A \setminus B \cup B \setminus C$.
5. $A \setminus (B \cap C) = A \setminus B \cap B \setminus C$.

Задача 10. Докажете, че

1. $A \cup B = B \Leftrightarrow A \subseteq B$.
2. $A \cap B = A \Leftrightarrow A \subseteq B$.
3. $A \setminus B = A \Leftrightarrow A \cap B = \emptyset$.
4. $A \Delta B = \emptyset \Leftrightarrow A = B$.

Задача 11. Вярно ли е, че:

1. $A \Delta B = (A \cup B) \setminus (A \cap B)$.
2. $(A \Delta B) \cap C = (A \Delta C) \cap (B \Delta C)$.
3. $(A \cap B) \Delta C = (A \cap C) \Delta (B \cap C)$.

Задача 12. Докажете, че

1. $A \cap (\bigcup_{i \in I} B_i) = \bigcup_{i \in I} (A \cap B_i)$.
2. $A \cup (\bigcap_{i \in I} B_i) = \bigcap_{i \in I} (A \cup B_i)$.
3. $X \subseteq \bigcap_{i \in I} A_i \Leftrightarrow \forall i (X \subseteq A_i)$.
4. $X \setminus \bigcup_{i \in I} A_i = \bigcap_{i \in I} (X \setminus A_i)$.

Задача 13. Намерете редица от множества $\{A_i\}_{i \in \mathbb{N}}$ такава, че за всяко $i \in \mathbb{N}$, $A_{i+1} \subset A_i$, но $\bigcap_{i \in \mathbb{N}} A_i = \emptyset$.

Задача 14. Дайте индуктивна дефиниция за множеството:

1. $2\mathbb{N}+1$ (множеството на всички нечетни числа) като за базово множество използвате $\{1\}$.
2. $\{a^n b^n \mid n \in \mathbb{N} = \{\varepsilon, ab, aabb, aaabbb, \dots\}\}$ (множеството от думи над азбуката $\{a, b\}$ с дължина $2n$, които започват с n на брой a-та и завършват с n на брой b-та за някое $n \in \mathbb{N}$) като за базово множество използвате $\{\varepsilon\}$.

Задача 15. Намерете 2^A, ако:

1. $A = \emptyset$.

2. $A = \{\{1, 2\}\}$.
3. $A = \{\emptyset, \{\emptyset\}\}$.
4. $A = \{\emptyset, \{1, 2\}, 7\}$.
5. $A = \{1, 2, 3, 4\}$.

Задача 16.

1. Докажете, че $A \subseteq B \Rightarrow 2^A \subseteq 2^B$.
2. Докажете, че $2^{A \cap B} = 2^A \cap 2^B$.
3. Вярно ли е, че $2^{A \cup B} = 2^A \cup 2^B$.

Глава 2

Релации

Досега намерихме формален начин да изразим и работим със съвкупност от елементи. Светът е по-сложен и често се налага да говорим за връзки между елементи: едно момче, което е влюбено в едно момиче, едно дърво по-сенчесто от друго, едно естествено число, което дели друго.

За да можем да опишем формално една такава по-сложна конструкция, трябва първо да можем да опишем обект от две части, на който да можем винаги да разпознаваме коя е първа част и коя - втора част.

Множества от елементи не биха могли да ни послужат директно, защото $\{7, 9\} = \{9, 7\}$ - наредбата се загубва.

2.1 Наредени двойки, декартово произведение

Определение 2.1. Наредена двойка на елементите a и b, която означаваме с (a, b), е двойка елементи, в която a е първи елемент, а b е втори елемент.

Един начин за дефиниция на наредена двойка, предложен от Куратовски е:

$$(a, b) = \{a, \{a, b\}\}.$$

Забележка! Една наредена двойка (a_1, a_2) е равна на друга наредена двойка (b_1, b_2) тогава и само тогава, когато $a_1 = b_1$ и $a_2 = b_2$. Например $(5, 7) \neq (7, 5)$.

Понятието за наредена двойка се обобщава по естествен начин до наредена n-торка за произволно естествено $n \geq 2$. Наредена n-торка означаваме с $(a_1, a_2, \ldots a_n)$. Един начин за дефиниция на наредена n-торка е:

$$(a_1, a_2, \ldots, a_n) = (a_1, (a_2, (\ldots, a_n))).$$

Сега $(a_1, a_2 \ldots a_n) = (b_1, b_2 \ldots b_n)$ тогава и само тогава, когато $a_1 = b_1$, $a_2 = b_2$,... и $a_n = b_n$.

Определение 2.2. Нека A и B са множества. Декартово произведение на A и B наричаме множеството:

$$A \times B = \{(a, b) \mid a \in A \ \& \ b \in B\}.$$

Забележка! Операцията декартово произведение не е комутативна. Формално операцията не е и асоциативна, но ние ще си позволим да не изписваме скоби в декартово произведение на повече от две множества, като предварително се уговорим, че $A \times B \times C$ винаги означава $(A \times B) \times C$.

Теорема 2.3. Нека A и B са множества, $|A| = n$, $|B| = m$. Тогава

$$|A \times B| = n \cdot m.$$

Доказателство. Ще докажем твърдението с индукция по n - броя на елементите на множеството A.

i) Ако $n = 0$, то $A = \emptyset$. Но тогава $\emptyset \times B = \emptyset$ и следователно

$$|\emptyset \times B| = 0 = 0 \cdot m.$$

ii) Нека твърдението е в сила за множества с n елемента, т.е. ако $A = \{a_1, a_2, \ldots, a_n\}$ и $B = \{b_1, \ldots, b_m\}$, където m е произволно, то е изпълнено:

$$|A \times B| = n \cdot m.$$

iii) Ще докажем твърдението за множества с $n + 1$ елемента, т.е. нека

$$A = \{a_1, a_2, \ldots a_n, a_{n+1}\} \text{ и } B = \{b_1, b_2, \ldots b_m\},$$

където m е произволно число. Да разпишем какво представлява множеството $A \times B$.

$$\begin{aligned} A \times B &= \{a_1, a_2, \ldots a_n, a_{n+1}\} \times \{b_1, b_2, \ldots b_m\} \\ &= \{a_1, a_2, \ldots a_n\} \times \{b_1, b_2, \ldots b_m\} \cup \{a_{n+1}\} \times \{b_1, b_2, \ldots b_m\}. \end{aligned}$$

Съгласно индукционното предположение,

$$|\,\{a_1, a_2, \ldots a_n\} \times \{b_1, b_2, \ldots b_m\}\,| = n \cdot m.$$

Броят на елементите в множеството

$$\{a_{n+1}\} \times \{b_1, b_2, \ldots b_m\} = \{(a_{n+1}, b_1), (a_{n+1}, b_2), \ldots (a_{n+1}, b_m)\}$$

е m. Множествата $\{a_1, a_2, \ldots a_n\} \times \{b_1, b_2, \ldots b_m\}$ и $\{a_{n+1}\} \times \{b_1, b_2, \ldots b_m\}$ са непресичащи се, защото елементите на първото множество са наредени двойки, с пръв елемент различен от a_{n+1}, елементите на първото множество са наредени двойки, с пръв елемент a_{n+1}. Съгласно принципа за събирането,

$$|A \times B| = n \cdot m + m = (n + 1) \cdot m$$

$\square$

2.2 Релации

Определение 2.4. Нека A и B са множества. Всяко подмножество R на декартовото произведение на A и B ($R \subseteq A \times B$) наричаме (бинарна) релация над A и B.

Когато $A = B$, релация $R \subseteq A \times A$ наричаме (бинарна) релация над A. Понятието релация може да се обобщи естествено по следния начин. Ако $A_1, A_2, \dots, A_n$ са множества и $R \subseteq A_1 \times \dots A_n$, то R наричаме n-местна релация над $A_1, A_2, \dots, A_n$.

С всяка релация свързваме две множества дефиниционна област (домейн) и област от стойности (рейндж):

Определение 2.5. Нека $R \subseteq A \times B$ е релация над A и B.

$$\begin{aligned} dom(R) &= \{a \in A \mid (\exists b)[(a, b) \in R]\} \\ range(R) &= \{b \in B \mid (\exists a)[(a, b) \in R]\}. \end{aligned}$$

2.2.1 Представяне на релации

Когато работим с крайни релации, бихме могли да използваме представяния, с които се работи по лесно. Ще илюстрираме две представяния с пример. Нека T е релация над $\{1, 2, 3\}$ и $\{a, b, c, d\}$, дефинирана чрез

$$T = \{(1, a), (1, c), (1, d), (2, b), (3, a), (3, d)\}.$$

Нека S е релация над $\{1, 2, 3, 4\}$, дефинирана чрез

$$S = \{(1, 2), (1, 3), (1, 4), (2, 2), (3, 4), (4, 2), (4, 4)\}.$$

Таблично представяне

Нека R е релация над $A = \{a_1, \dots, a_n\}$ и $B = \{b_1, \dots, b_m\}$. Представяме релацията R с помощта на таблица (матрица) с n реда и m стълба, като позицията на i-ти ред, j-ти стълб е 0, ако $(a_i, b_j) \notin R$ и 1, ако $(a_i, b_j) \in R$.

Например табличното представяне на T е:

$$\begin{pmatrix} * & a & b & c & d \\ 1 & 1 & 0 & 1 & 1 \\ 2 & 0 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 & 1 \end{pmatrix}$$

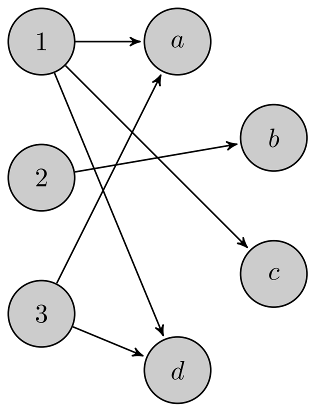
Табличното представяне на S е:

$$\begin{pmatrix} * & 1 & 2 & 3 & 4 \\ 1 & 0 & 1 & 1 & 1 \\ 2 & 0 & 1 & 0 & 0 \\ 3 & 0 & 0 & 0 & 1 \\ 4 & 0 & 1 & 0 & 1 \end{pmatrix}$$

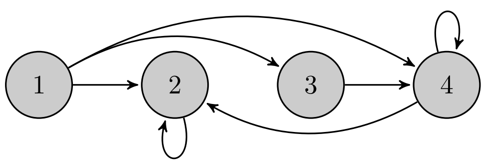
Графично представяне на релация

Нека R е релация над $A = \{a_1, \dots, a_n\}$ и $B = \{b_1, \dots, b_m\}$. Представяме релацията R с помощта на ориентиран граф $G(A \cup B, R)$. За всеки елемент от $A \cup B$ имаме по един връх, а за всеки елемент $(a, b) \in R$ поставяме стрелка от a към b.

Графичното представяне на T е:



Графичното представяне на S е:



2.2.2 Операции над релации

Релациите са множества и над тях могат да се прилагат булевите операции, които разгледахме в предишната тема. Допълнително ще дефинираме още две операции, специфично за релации.

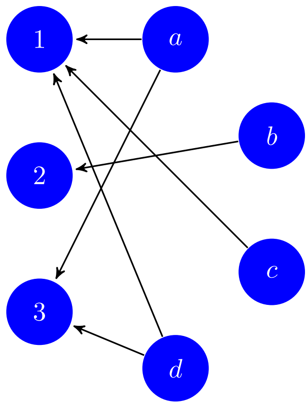
Определение 2.6. Нека R е релация над множествата A и B. Обратната релация на R е релацията над B и A:

$$R^{-1} = \{(b, a) \mid (a, b) \in R\}.$$

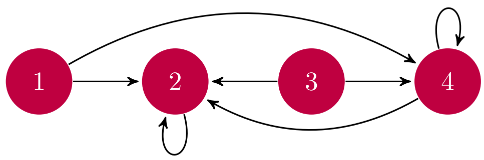
Определение 2.7. Нека R е релация над множествата A и B и S е релация над множествата B и C. Композицията на релациите R и S е релацията над A и C:

$$R \circ S = \{(a, c) \mid \exists b\ ((a, b) \in R \ \&\ (b, c) \in S)\}.$$

Пример. Нека T и S са както в предния пример. Графичното представяне на T^{-1} е:



Графичното представяне на $S \circ S$ е:



2.2.3 Видове релации

Нека е множество и R е релация над .

Рефлексивност

Определение 2.8. Релацията R наричаме рефлексивна, ако за всеки елемент $a \in A$, двойката (a, a) е в релацията R:

$$(\forall a \in A)[(a, a) \in R].$$

Например релацията $\leq$ над естествените числа, релацията $\subseteq$ над множества от естествени числа, са рефлексивни релации.

Възможно е релацията R да не е рефлексивна: за някой елемент $a \in A$ наредената двойка $(a, a) \notin R$. Възможно е да е изпълнено нещо много по-силно:

Определение 2.9. Релацията R наричаме антирефлексивна, ако **за всеки** елемент $a \in A$, двойката (a, a) **не** е в релацията R:

$$(\forall a \in A)[(a, a) \notin R].$$

Например релацията $<$ над естествените числа, релацията $\subset$ над множества от естествени числа, са антирефлексивни релации.

Релацията $R = \{(n, m) \mid n \text{ е прост делител на } m\}$ не е нито рефлексивна, нито антирефлексивна. Не е рефлексивна, защото например $(4, 4) \notin R$. Не е антирефлексивна, защото например $(3, 3) \in R$.

Транзитивност

Определение 2.10. Релацията R наричаме транзитивна, ако за всяка тройка елементи $a, b, c \in A$, ако $(a, b) \in R$ и $(b, c) \in R$, то $(a, c) \in R$:

$$\forall a \in A \forall b \in A \forall c \in A \ ((a, b) \in R \ \& \ (b, c) \in R \rightarrow (a, c) \in R).$$

Например релациите $\leq$ и $<$ над естествените числа, релациите $\subseteq$ и $\subset$ над множества от естествени числа, са транзитивни релации.

Релацията $R = \{(n, m) \mid n \text{ и } m \text{ имат обща прост делител}\}$ не е транзитивна. Например $(3, 6) \in R$, $(6, 2) \in R$, но $(3, 2) \notin R$.

Твърдение 2.11. Релацията R е транзитивна тогава и само тогава, когато $R \circ R \subseteq R$.

Доказателство. Нека R е транзитивна. Нека (a, c) е произволен елемент от $R \circ R$. Съгласно дефиницията на операцията композиция на релации, можем да намерим междинен елемент $b \in A$, такъв че $(a, b) \in A$ и $(b, c) \in A$. От транзитивността на R следва, че $(a, c) \in R$. Така $R \circ R \subseteq R$.

Нека сега $R \circ R \subseteq R$. Да вземем произволна тройка елементи $a, b, c \in A$ такива, че $(a, b) \in R$ и $(a, c) \in R$. Съгласно дефиницията на операцията композиция на релации, $(a, c) \in R \circ R$. Но $R \circ R \subseteq R$, следователно $(a, c) \in R$ и R е транзитивна. □

Симетричност

Определение 2.12. Релацията R наричаме симетрична, ако за всяка двойка елементи $a, b \in A$, ако $(a, b) \in R$, то $(b, a) \in R$:

$$\forall a \in A \forall b \in A \ ((a, b) \in R \rightarrow (b, a) \in R).$$

Например релацията $R = \{(n, m) \mid n \text{ и } m \text{ имат обща прост делител}\}$ и релацията $=$ над естествените числа са симетрични. Релациите $\leq$ и $<$ над естествените числа, релациите $\subseteq$ и $\subset$ над множества от естествени числа, не са симетрични релации. За тях отново можем да кажем нещо много по-силно, те са антисиметрични.

Определение 2.13. Релацията R наричаме антисиметрична, ако за всяка двойка елементи $a, b \in A$, ако $(a, b) \in R$ и $a \neq b$, то $(b, a) \notin R$:

$$\forall a \in A \forall b \in A \ ((a, b) \in R \ \& \ a \neq b \rightarrow (b, a) \notin R).$$

Забележка! Тук отново е възможно да има релация, която не нито симетрична, нито антисиметрична. Например релацията $R = \{(A, B) \mid A \setminus B \neq \emptyset\} \subseteq 2^{\mathbb{N}} \times 2^{\mathbb{N}}$ не е симетрична защото например $(\{1, 2, 3\}, \{1, 2\}) \in R$, но $(\{1, 2\}, \{1, 2, 3\}) \notin R$. Релацията не е антисиметрична защото $(\{1, 2, 3\}, \{4, 5, 6\}) \in R$, $\{1, 2, 3\} \neq \{4, 5, 6\}$, но $(\{4, 5, 6\}, \{1, 2, 3\}) \in R$.

Твърдение 2.14. Релацията R е симетрична тогава и само тогава, когато $R^{-1} \subseteq R$.

Доказателство. Нека R е симетрична. Нека $(b, a) \in R^{-1}$. Съгласно дефиницията на обратна релация $(a, b) \in R$. Но щом R е симетрична, $(b, a) \in R$. Така $R^{-1} \subseteq R$.

Нека сега $R^{-1} \subseteq R$. Нека $a, b \in A$ са произволни елементи такива, че $(a, b) \in R$. Съгласно дефиницията на обратна релация $(b, a) \in R^{-1}$. Но $R^{-1} \subseteq R$, следователно $(b, a) \in R$ и R е симетрична. □

2.3 Релация на еквивалентност

Определение 2.15. Нека е непразно множество. Релация R над A наричаме релация на еквивалентност, ако R е рефлексивна, симетрична и транзитивна.

Пример за релация на еквивалентност е $\{(n, m) \mid n \equiv m(mod\ 4)\} \subseteq \mathbf{N}^2$. Тази релация се състои от всички двойки естествени числа, които дават един и същ остатък, при деление на 4.

Интуицията зад понятието релация на еквивалентност, е че тя групира елементите елементите на A по отношение на някакво сходство. Групата в която попада конкретен елемент се нарича негов клас на еквивалентност.

Определение 2.16. Нека A е множество, $a \in A$ и $R \subseteq A^2$ е релация на еквивалентност над A. Класът на еквивалентност на a по отношение на релацията R е множеството:

$$[a]_R = \{b \in A \mid (a, b) \in R\}.$$

Всяка релация на еквивалентност над множество поражда разбиване на множеството .

Определение 2.17. Нека A е непразно множество, I е индексно множество и $\{A_i\}_{i \in I}$ е фамилия от множества, индексирана с I. Фамилията $\{A_i\}_{i \in I}$ е разбиване на A ако:

1. $\forall i \in I(A_i \neq \emptyset)$;
2. $\bigcup_{i \in I} A_i = A$;
3. $\forall i \in I \forall j \in (A_i \cap A_j \neq \emptyset \to A_i = A_j)$.

Теорема 2.18.
1. Нека A е множество, а $R \subseteq A^2$ е релация на еквивалентност над A. Фамилията $\{[a]_R\}_{a \in A}$ е разбиване на множеството A.
2. Нека A е множество, I е индексно множество и $\{A_i\}_{i \in I}$ е разбиване на A. Релацията:

$$R = \{(a, b) \mid \exists i \in I(a \in A_i \ \& \ b \in A_i)\}$$

е релация на еквивалентност над A и всеки клас на еквивалентност по отношение на R съвпада с A_i за някое $i \in I$.

Доказателство.

1. Всеки клас на еквивалентност е непразен, защото R е рефлексивна релация и следователно $(a, a) \in R$, $a \in [a]_R$. Всеки клас на еквивалентност е по дефиниция подмножество на A, и всеки елемент $a \in A$ попада в поне един клас на еквивалентност - своя, така $\bigcup_{a \in A}[a]_R = A$. Нека $a, b \in A$ са такива, че $[a]_R \cap [b]_R \neq \emptyset$. Нека $c \in [a]_R \cap [b]_R$. Тогава $(a, c) \in R$, $(b, c) \in R$ и понеже R е симетрична $(c, b) \in R$. Сега от транзитивността на R следва, че $(a, b) \in R$, а следователно и $(b, a) \in R$.

Ще покажем, че $[a]_R = [b]_R$. Нека $x \in [a]_R$. Тогава $(b,a) \in R$ и $(a,x) \in R$ и следователно от транзитивността на R, $(b,x) \in R$ и $x \in [b]_R$. Така $[a]_R \subseteq [b]_R$.

Нека сега $x \in [b]_R$. Тогава $(a,b) \in R$ и $(b,x) \in R$ и следователно от транзитивността на R, $(a,x) \in R$ и $x \in [a]_R$. Така получаваме и второто включване: $[b]_R \subseteq [a]_R$.

С това доказахме, че фамилията $\{[a]_R\}_{a \in A}$ изпълнява и трите условия, необходими за да е разбиване на множеството .

2. Нека сега $\{A_i\}_{i \in I}$ е разбиване на A. Релацията:

$$R = \{(a,b) \mid \exists i \in I(a \in A_i \ \& \ b \in A_i)\}$$

е рефлексивна, защото $\bigcup_{i \in I} A_i = A$ следователно за всеки елемент $a \in A$ има индекс $i \in I$, такъв че $a \in A_i$. Релацията е симетрична, защото логическата връзка & е комутативна. Остава да покажем, че R е транзитивна. Нека $a, b, c \in A$ са такива, че $(a,b) \in R$ и $(b,c) \in R$. Тогава съществуват индекси i и j такива, че $a, b \in A_i$ и $b, c \in A_j$. Така $b \in A_i \cap A_j$. От третото условие в дефиницията на разбиване на множество следва, че $A_i = A_j$. Така $a, c \in A_i$ и следователно $(a,c) \in R$.

Нека a е произволен елемент от A и нека $i \in I$ е такова, че $a \in A_i$. Твърдим, че $[a]_R = A_i$. Наистина, ако $b \in A_i$ то $(a,b) \in R$ и следователно $b \in R_i$. От друга страна, ако $b \in [a]_R$, то $(a,b) \in R$ и има $j \in I$ такова, че $\in A_j$ и $b \in A_j$. Но от третото свойство на разбиване и фактът, че $a \in A_i \cap A_j$, следва, че $A_i = A_j$. Така показахме, че $b \in A_i$. □

2.4 Частична наредба

Вторият вид релации, които ще разгледаме се наричат частични наредби и интуитивно сравняват елементи по някакъв признак. Ако $(a,b) \in R$ - считаме, че a е по-малък, предхожда, b. В зависимост дали релацията, която разглеждаме е рефлексивна или антирефлексивна имаме два вида частични наредби.

Определение 2.19. Нека A е непразно множество.

1. Релация R над A наричаме (нестрога) частична наредба, ако R е рефлексивна, антисиметрична и транзитивна.

2. Релация R над A наричаме строга частична наредба, ако R е антирефлексивна, антисиметрична и транзитивна.

Примери за нестроги частични наредби са релацията $\leq$ над естествените числа, релацията $\subseteq$ над множества от естествени числа.

Примери за строги частични наредби са релацията $<$ над естествените числа, релацията $\subset$ над множества от естествени числа.

Макар релациите $\leq$ $(<)$ и $\subseteq$ $(\subset)$ да имат едни и същи характеристики по отношение на рефлексивност, симетричност, транзитивност, те са съществено различни от друга гледна точка. Каквато и двойка различни естествени числа да вземем n, m, те са винаги сравними: или $n \leq m$ или $m \leq n$. За двойки множество, това съвсем не важи. Например двойката множества $2\mathbb{N}$ и $2\mathbb{N}+1$ са несравними по отношение на релацията $\subseteq$: нито $2\mathbb{N} \subseteq 2\mathbb{N}+1$, нито $2\mathbb{N}+1 \subseteq 2\mathbb{N}$.

Определение 2.20. Нека R е частична наредба (строга или нестрога) над множество A. Казваме, че R е линейна (пълна), ако всеки два различни елемента от A са сравними по отношение на R:

$$\forall a \in A \forall b \in A \ (a \neq b \rightarrow ((a,b) \in R \ \vee \ (b,a) \in R)).$$

Така релациите $\leq$ и $<$ над естествените числа, са примери за линейни частични наредби, докато релациите $\subseteq$ и $\subset$ над множества от естествени числа са примери за частични наредба, които не са линейни.

Интуицията, че $(a,b) \in R$ означава, че a е по-малък от b е залегнала и във следващата дефиниция:

Определение 2.21. Нека R е частична наредба (строга или нестрога) над множество A.

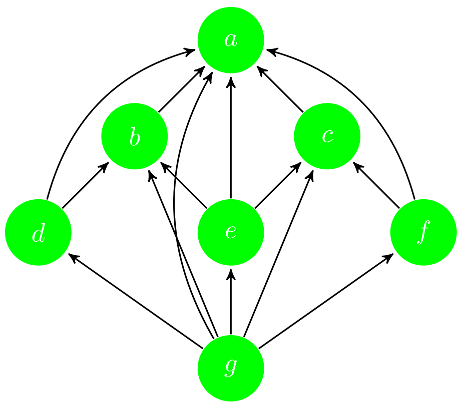
- Казваме, че $a \in A$ е най-малък по отношение на R, ако е по-малък от всеки друг елемент на A:

$$\forall b \in A(a \neq b \rightarrow (a,b) \in R).$$

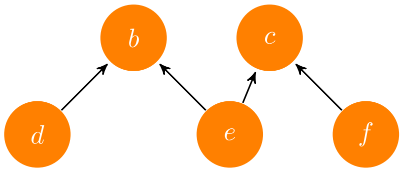
- Казваме, че $a \in A$ е най-голям по отношение на R, ако е по-голям от всеки друг елемент на A:

$$\forall b \in A(a \neq b \rightarrow (b,a) \in R).$$

Например в следната релация, представена графично a е най-голям елемент, а g е най-малък.



Съществуването на най-голям и най-малък елемент съвсем не е задължително. Например ако разгледаме $\mathbb{Z}$ и наредбата $\leq$ над $\mathbb{Z}$, не съществува нито най-голям, нито най-малък елемент. Възможно е дори в крайна частична наредба да няма най-малък или най-голям елемент, както се случва в следния пример:



Определение 2.22. Нека R е частична наредба (строга или нестрога) над множество A.

- Казваме, че $a \in A$ е минимален елемент по отношение на R, ако не съществува друг елемент $b \in A$, който е по-малък от него:
$$\forall b \in A (a \neq b \rightarrow (b, a) \notin R).$$
- Казваме, че $a \in A$ е максимален елемент по отношение на R, ако не съществува друг елемент $b \in A$, който е по-голям от него:
$$\forall b \in A (a \neq b \rightarrow (a, b) \notin R).$$

Така в горе изобразената релация, елементите d, e и f са минимални, а b и c са максимални.

Теорема 2.23. Всяка частична наредба R над крайно непразно множество A притежава минимален и максимален елемент.

Доказателство. За определеност ще приемем, че R е нестрога частична наредба. Теоремата е в сила и за строга частична наредба. Доказателството ще извършим с индукция по $|A|$.

Ако $A = \{a\}$ има само един елемент, то a минимален и максимален елемент.

Нека твърдението е в сила за крайни множества с n елемента. Нека $A = \{a_1 \dots a_n, a_{n+1}\}$ и R е частична наредба над A. Да разгледаме множеството $A_1 = \{a_1, \dots, a_n\} = A \setminus \{a_{n+1}\}$ и релацията $R_1 = R \cap (A_1 \times A_1)$. Лесно се проверява, че R_1 е частична наредба над A_1. A_1 е множество с n елемента и съгласно индукционното предположение A_1 има минимален a_i и максимален елемент a_j по отношение на R_1, $i, j \leq n$.

Ако $(a_{n+1}, a_i) \notin R$, то a_i е минимален елемент на по отношение на R. Наистина ако допуснем, че съществува $b \in A$, такъв че $b \neq a_i$ и $(b, a_i) \in R$, то $b \neq a_{n+1}$ и следователно $b \in A_1$, а $(b, a_i) \in R_1$, което противоречи на минималността на a_i.

Ако $(a_{n+1}, a_i) \in R$, то a_{n+1} е минимален елемент на по отношение на R. Наистина ако допуснем, че съществува $b \in A$, такъв че $b \neq a_{n+1}$ и $(b, a_{n+1}) \in R$, от транзитивността на R, следва, че $(b, a_i) \in R$, отново $b \in A_1$, и следователно $(b, a_i) \in R_1$, което пак противоречи на минималността на a_i.

Съществуването на максимален елемент се доказва по аналогичен начин: ако $(a_j, a_{n+1}) \notin R$, то a_j е максимален елемент; ако $(a_j, a_{n+1}) \in R$, то a_{n+1} е максимален елемент. □

Като използваме предишната теорема ще покажем, че всяка частична наредба над крайно непразно множество A може да се продължи до пълна (линейна). Методът, който ще използваме в доказателството е известен като метод на топологическата сортировка.

Теорема 2.24. Нека A е непразно крайно множество и R е частична наредба над A. Съществува линейна наредба S над A такава, че $R \subseteq S$.

Доказателство. Отново за определеност ще приемем, че R е нестрога частична наредба. Теоремата е в сила и за строга частична наредба.

Нека A е множество с n елемента. Ще подредим елементите на A в редица. Съгласно предишната теорема, A притежава минимален елемент по отношение на R. Нека a_1 е един такъв минимален елемент на A.

Нека сме построили елементите $a_1, \dots a_i$ - i-на брой различни елементи на A. Ако $i = n$, конструкцията е готова и $A = \{a_1, \dots a_n\}$. Иначе множеството $A_i = A \setminus \{a_1, \dots a_i\}$ е непразно, а $R \cap (A_i \times A_i)$ е частична наредба над A_i. Отново прилагаме предишната теорема за да изберем a_{i+1} като минимален елемент на A_i по отношение на $R \cap (A_i \times A_i)$.

След като сме подредили елементите на A, като $a_1, \dots a_n$, дефинираме релацията $S = \{(a_i, a_j) \mid 1 \leq i \leq j \leq n\}$. Релацията S е линейна частична наредба. Всеки елемент $a \in A$ присъства някъде в редицата, $a = a_i$ за някое i. Понеже $i \leq i$, $(a_i, a_i) \in S$ и S е рефлексивна. Антисиметричност и транзитивност на S, следват от антисиметричност и транзитивност на релацията $\leq$ над естествените числа. Нека $a, b \in A$. Тогава $a = a_i$ и $b = a_j$ за някои i и j. Ако $i \leq j$, то $(a, b) \in S$. Иначе $j \leq i$ и $(b, a) \in S$.

Остана да видим, че $R \subseteq S$. Нека $(a, b) \in R$. Тогава отново $a = a_i$ и $b = a_j$ за някои i и j. Да допуснем, че $j < i$ да се върнем на стъпка j от конструкцията. Елементът b е избран като минимален елемент на A_j по отношение на $R \cap (A_j \times A_j)$. Елементът не се среща сред $a_1 \dots a_{j-1}$, защото съгласно допускането $i > j$. Тогава $a \in A_j = A \setminus \{a_1, \dots a_{j-1}\}$. Така $(a, b) \in R \cap (A_j \times A_j)$, но това противоречи на минималността на R. Противоречието се дължи на грешното ни допускане, следователно $i \leq j$ и $(a, b) \in S$. □

Определение 2.25. Нека R е частична наредба над A (строга или нестрога). Казваме, че R е фундирана, ако всяко непразно подмножество $B \subseteq A$ има минимален елемент по отношение на R.

Алтернативна характеризация на фундираните наредби е следната:

Твърдение 2.26. Нека A е непразно крайно множество и R е частична наредба над A. R е фундирана, тогава и само тогава когато не съществува безкрайна редица от различни елементи на A, $\{a_i\}_{i \in \mathbb{N}}$, със свойството $\forall i (a_{i+1}, a_i) \in R$.

Доказателство. Нека R е фундирана. Да допуснем, че има безкрайна редица от елементи на A, $\{a_i\}_{i \in \mathbb{N}}$, със свойството $\forall i (a_{i+1}, a_i) \in R$. Тогава множеството $\{a_i\}_{i \in \mathbb{N}}$ трябва да има минимален елемент $b = a_j$ за наякое j. Но тогава $a_{j+1} \neq b$ и $(a_{j+1}, b) \in R$, което противоречи на дефиницията на минимален елемент.

Нека сега допуснем, че R не е фундирана. Нека $B \subseteq A$ е непразно множество, което няма минимален елемент. Ще построим редица със исканите свойства. Взимаме произволен елемент $b \in R$ и полагаме $a_0 = b$. Да допуснем че сме построили $a_0 \dots a_k$ различни елементи, такива че $(a_{i+1}, a_i) \in R$ за всяко $i < k$. Избираме $a_{k+1} \in B$ като нов елемент със свойството $(a_{k+1}, a_k) \in R$. Такъв елемент има, защото ако допуснем противното: за всеки елемент $b \in B$, ако $b \neq a_k$ то $(b, a_k) \notin R$, получаваме, че a_k е минимален елемент на

B по отношение на R. Така с индукция по k пострихме безкрайна редица от елементи на A с исканото свийство. $\square$

Пример за фундирана наредба е наредбата на естествените числа. Фундираността е свойството на тази наредба, което ни позволява да използваме метода на математическата индукция.

Теорема 2.27 (Метод на структурната индукция)**.** Нека A е непразно множество и R е фундирана наредба над A. Ако $P \subseteq A$ има следното свойство:

> За всички $b \in A$ е вярно следното: ако всяко $a \in A$, такова че $a \neq b$ и $(a, b) \in R$, имаме че $a \in P$, то тогава и $b \in P$.

Тогава $P = A$.

Доказателство. Нека $P \subseteq A$ има това две свойства. Да допуснем, че $P \subset A$. Тогава $A \setminus P$ е непразно множество. Понеже R е фундирана, можем да изберем b като минимален елемент на $A \setminus P$ по отношение на R. Нека $a \in A$ е произволен елемент, такъв че $a \neq b$ и $(a, b) \in R$. От минималността на b следова, че $a \notin A \setminus P$. Така $a \in P$. От свойството на P, следва, че $b \in P$, което противоречи на избора на b. Така допускането ни е грешно и следователно $A = P$. $\square$

2.5 Задачи за упражнение

Задача 1. Нека $A = \{John, Mary\}$, $B = \{1, 2, 3\}$, $C = \emptyset$. Намерете $A \times B$, $B \times A$, $A \times C$, $C \times A$, $A \times A = A^2$, $B \times B \times B = B^3$.

Задача 2. Докажете, че:

1. Ако $A \subseteq A_1$ и $B \subseteq B_1$, то $A \times B \subseteq A_1 \times B_1$.
2. Ако $A \neq \emptyset$ и $B \neq \emptyset$, то $A \times B = B \times A \Leftrightarrow A = B$.

Задача 3. Вярно ли е, че:

1. $A \times (B \cup C) = A \times B \cup A \times C$.
2. $A \times (B \cap C) = A \times B \cap A \times C$.
3. $A \times (B \setminus C) = A \times B \setminus A \times C$.

Задача 4. Нека A и B са както в Задача 1.

1. Кои от следните множества са релации над A и B: $\{(John, 1), (John, 2)\}$, $\{(Mary, 3), (John, Mary)\}$, $\{(John, 1), (2, John)\}$, $(\{Mary, 1\}, \{Mary, 2\})$.
2. Коя е най- голямата релация над A и B? А най-малката?
3. Колко са всички релации над A и B?

Задача 5. Определете $dom(R)$ и $range(R)$, за:

1. $R = \{(1,7),(3,3),(13,11),(3,12),(2,15)\}$.
2. $R = \{(7,1),(3,3),(11,13),(12,3),(15,2)\}$.
3. $R = Id_A = \{(a,a) \mid a \in A\}$.

Задача 6. Нека $A = \{1,2,3,4\}$. Представете таблично и графично релациите: "$<$ "$\leq$ "$=\emptyset$ и ^{2}.

Задача 7. Намерете обратната релация R^{-1} и $R \circ R$, ако R е:

1. $\{(0,1),(1,3),(4,0)\}$.
2. $\{(n,n+1) \mid n \in \mathbb{N}\}$.
3. $\{(n,m) \mid n,m \in \mathbb{N} \;\&\; n < m\}$.

Как можем по табличното (графичното) представяне на R да намерим табличното (графичното) представяне на R^{-1}? А на $R \circ R$?

Задача 8. Докажете, че:

1. $dom(R^{-1}) = range(R)$ и $range(R^{-1}) = dom(R)$.
2. $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$ и $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$.

Задача 9. Как може по табличното (графичното) представяне на релацията R да се разбере дали тя е:

1. рефлексивна, антирефлексивна или нито едно от двете?
2. симетрична, антисиметрична или нито едно от двете?.

Задача 10. Нека R е релация над A. Докажете, че

1. Ако R е транзитивна и рефлексивна, то $R \circ R = R$.
2. Възможно ли е $R \circ R = R$, ако R не е рефлексивна.

Задача 11. Нека R е релация над A. Докажете, че следните три условия са еквивалентни:

1. R е симетрична.
2. $R^{-1} \subseteq R$.
3. $R = R^{-1}$.

Задача 12. Една релация $R \subseteq A^2$ наричаме а-цикилична, ако не съществуват елементи $a_1, a_2, \ldots a_n \in A$ $(n \geq 2)$ такива, че $a_1 = a_n$ и за всяко i, $1 \leq i < n$, $(a_i, a_{i+1}) \in R$. Докажете, че

1. Всяка транзитивна, антирефлексивна релация е а-циклична.

2. Ако R е а-циклична, то R е антирефлексивна.

3. Дайте пример за а-циклична релация, която не е транзитивна.

Задача 13. Покажете, че за всяко множество A, релацията id_A е релация на еквивалентност. Покажете, че това е най-малката релация на еквивалентност над A по отношение на релацията $\subseteq$. Коя е най-голямата? Как изглежда графичното представяне на релация на еквивалентност?

Задача 14. Проверете дали следните релации са релации на еквивалентност:

а) $\{(n, m) \mid n \equiv m(\mod k)\} \subseteq \mathbb{N} \times \mathbb{N}$, където k е някакво фиксирано положително естествено число.

б) $\{(x, y) \mid x + y = 0\} \subseteq \mathbb{R} \times \mathbb{R}$.

в) $\{(n, m) \mid n + m \text{ е четно число.}\} \subseteq \mathbb{N} \times \mathbb{N}$.

г) $\{(a, b) \mid a.b \geq 0\} \subseteq \mathbb{Z} \times \mathbb{Z}$.

д) $\{(a, b) \mid a.b > 0\} \subseteq \mathbb{Z} \times \mathbb{Z}$.

е) $\{(p, r) \mid p - r \text{ е цяло число}\} \subseteq \mathbb{Q} \times \mathbb{Q}$.

ж) $\{((a, b), (c, d)) \mid a.d = b.c\} \subseteq \mathbb{N}^2 \times \mathbb{N}^2$.

Задача 15. Кое от следните множества е разбиване на множеството $\{1, 2, 3, 4\}$:

- $\{\{1, 2\}, \{3\}\}$.
- $\{\{1, 2\}, \{2, 3\}, \{4\}\}$.
- $\{\{1, 2\}, \{3, 4\}, \emptyset\}$
- $\{\{1, 4\}, \{2, 3\}\}$

Задача 16. Опишете класовете на еквивалентност, породени от тези от релациите в Задача 14, които са релации на еквивалентност.

Задача 17. Нека $A = \{n \in \mathbb{N} \mid 2 \leq n \leq 20\}$. Нека $R \subseteq A^2$ се състои от всички двойки числа, които имат еднакви прости делители. Например $(6, 12) \in R$, защото простите делители на 6 и 12 са $2, 3$, но $(6, 9) \notin R$, защото 2 е прост делител на 6, но не и на 9. Докажете, че R е релация на еквивалентност и определете класовете на еквивалентност породени от R.

Задача 18. Нека α е равнина. С $P(\alpha)$ означаваме множеството от точките в равнината, а с $L(\alpha)$ множеството от правите в равнината. Кои от следните релации са релации на еквивалентност? Определете класовете на еквивалентност.

1. $\{(a, b) \mid a||b\} \subseteq L(\alpha) \times L(\alpha)$.
2. $\{(a, b) \mid a \perp b\} \subseteq L(\alpha) \times L(\alpha)$.

3. $\{((A,B,C),(A',B',C')) \mid \ \triangle\, ABC \sim\triangle\, A'B'C'\} \subseteq P(\alpha)^3 \times P(\alpha)^3$.

Задача 19. Кои от следните релации са частични наредби:

1. $\{(n,m) \mid \exists k \in \mathbb{N}(m = k.n)\} \subseteq \mathbb{N} \times \mathbb{N}$.
2. $\{(A,B) \mid A \cap B = B\} \subseteq 2^{\mathbb{N}} \times 2^{\mathbb{N}}$.
3. $\{(x,y) \mid x^3 - 1 \geq y^3 - 1\} \subseteq \mathbb{R} \times \mathbb{R}$.
4. $\{(a,b) \mid a = b \ \vee \ a + 1 = b\} \subseteq \mathbb{N} \times \mathbb{N}$.

В следващите няколко задачи, ще разглеждаме множеството от думи на азбуката $\{a,b\}$.

Определение 2.28. Празната дума има дължина 0 и се означава с ε. Ако α е дума с дължина n, то αa и αb са думи с дължина $n+1$. Множеството на всички думи над азбуката $\{a,b\}$ означаваме с $\{a,b\}^*$.

Дефинираме операция конкатенация, ., на думи.

Определение 2.29. Нека α и β са думи над $\{a,b\}$. Конкатенацията на α и β е думата

$$\alpha.\beta = \begin{cases} \varepsilon, & \text{ако } \beta = \varepsilon; \\ (\alpha.\beta')a, & \text{ако } \beta = \beta' a; \\ (\alpha.\beta')b, & \text{ако } \beta = \beta' b. \end{cases}$$

Задача 20. Нека α и β са думи над азбуката $\{a,b\}$. Ще казваме, че α е начало на β, $(\alpha \subseteq \beta)$, ако съществува дума γ, такава че $\beta = \alpha.\gamma$. Докажете, че $\{(\alpha,\beta) \mid \alpha \subseteq \beta\} \subseteq \{a,b\}^* \times \{a,b\}^*$ е частична наредба. Линейна наредба ли е?

Задача 21. Нека α и β са думи над азбуката $\{a,b\}$. Ще казваме, че α е наляво от β, $(\alpha <_L \beta)$, ако съществува дума γ, такава че $\gamma a \subseteq \alpha$ и $\gamma b \subseteq \beta$. Докажете, че $\{(\alpha,\beta) \mid \alpha <_L \beta\} \subseteq \{a,b\}^* \times \{a,b\}^*$ е строга частична наредба. Линейна наредба ли е?

Задача 22. Нека α и β са думи над азбуката $\{a,b\}$. Ще казваме, че α е лексикографски по-малка от β, $(\alpha \preccurlyeq \beta)$, ако $\alpha \subseteq \beta$ или $\alpha <_L \beta$. Докажете, че $\{(\alpha,\beta) \mid \alpha \preccurlyeq \beta\} \subseteq \{a,b\}^* \times \{a,b\}^*$ е линейна частична наредба.

Задача 23. Дайте пример за частична наредба R с

1. два минимални елемента и три максимални елемента.
2. два минимални елемента и най-голям елемент.
3. един максимален елемент, без минимален елемент.

Задача 24. Нека R е линейна частична наредба над множеството A. Нека $a \in A$ е минимален елемент по отношение на R. Докажете, че a е най-малък елемент.

Задача 25. Нека разгледаме множеството $\mathbb{N}_* = \mathbb{N} \cup \{*\}$. Нека $R = \{(a, b) \mid a = b \ \vee \ a = *\} \subseteq \mathbb{N}_* \times \mathbb{N}_*$. Докажете, че R е частична наредба и определете минималните, максималните, най-малкия и най-големия елемент в $\mathbb{N}_*$ по отношение на R, ако такива има.

Глава 3

Функции

3.1 Дефиниция

Определение 3.1. Нека A и B са множества. Релацията $f \subseteq A \times B$ наричаме функция от A към B, ако за всеки елемент $a \in A$ съществува единствен елемент $b \in B$, такъв че $(a, b) \in f$.

Забележка! Дефиницията на понятието функция включва две изисквания:

1. За всеки елемент $a \in A$ трябва да има елемент $b \in B$ такъв, че $(a, b) \in f$, което записано формално има следния вид:

$$(\forall a \in A)(\exists b \in B)[(a, b) \in f].$$

   По друг начин казано дефиниционната област $dom(f) = A$.

2. За всеки елемент $a \in A$ **няма** два различни елемента $b_1, b_2 \in B$ такива, че $(a, b_1) \in f$ и $(a, b_2) \in f$, т.е.

$$(\forall a \in A)(\exists b_1, b_2 \in B)[(a, b_1) \in f \ \& \ (a, b_2) \in f \rightarrow b_1 = b_2].$$

Пример за функция е множеството $f \subseteq \mathbb{N} \times \mathbb{N}$, дефинирано чрез:

$$f = \{(n, m) \mid m = 2n\}.$$

Ако f е функция и $(a, b) \in f$, елементът b означаваме с $f(a)$. Така ако множеството f е дефинирано с помощта за аксиома за отделянето:

$$f = \{(a, b) \in A \times B \mid b = P(a)\},$$

където P е правило, по което на елемент $a \in A$ съпоставя неговият единствен $f(a) \in B$, ще използваме кратък запис:

$$f : A \rightarrow B \ \ f(x) = P(x).$$

Тук x е променлива, която може да се замести с произволен елемент от A, която ще наричаме аргумент на f.

Така функцията от горния пример можем да изпишем като:

$$f : \mathbb{N} \to \mathbb{N} \;\; f(x) = 2x.$$

Бихме могли да обобщим понятието функция по няколко начина. Първо бихме могли да позволим функция да има произволен краен аргументи:

$$f : A_1 \times A_2 \dots A_n \to B \;\; f(x_1, x_2, \dots x_n) = P(x_1, x_2, \dots x_n).$$

Тогава за всяка n-торка $(a_1, \dots a_n) \in A_1 \times \dots A_n$ съществува единствен елемент $b \in B$ такъв, че $(a_1, \dots a_n, b) \in f$. Елементът b означаваме с $f(a_1, \dots a_n)$.

Друго обобщение на понятието функция получаваме като отслабим изискването $dom(f) = A$, до $dom(f) \subseteq A$. Такива релации се наричат частични функции. Например релацията:

$$f : \mathbb{R} \to \mathbb{R} \;\; f(x) = \frac{1}{x^2 - 3x + 2}$$

не е дефинирана при $x = 1$ и при $x = 2$ и е частична функция.

3.2 Операции над функции

Всяка функция $f : A \to B$ е релация над A и B. С нея свързваме множествата $dom(f)$, $range(f)$, обратната релация f^{-1}. Знаем и какво представлява композицията на две функции. В този параграф ще видим какви специфични свойства имат тези операции, когато се прилагат към специалния вид релации: функции. Ще разгледаме и някои операции специфични за функциите.

Първо нека обърнем внимание на факта, че макар и $dom(f)$ винаги е цялото множество A, за $range(f)$ такова изискване няма.

3.2.1 Образ, първообраз, рестрикция и затваряне

Определение 3.2. Нека $f : A \to B$ е функция.

- Нека $X \subseteq A$. *Образ на множеството* X под действието на функцията f, наричаме множеството:

$$f(X) = \{f(a) \in B \mid a \in X\}.$$

- Нека $Y \subseteq B$. *Първообраз на множеството* Y под действието на функцията f, наричаме множеството:

$$f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}.$$

Например, ако функцията $f : \mathbb{N} \to \mathbb{N}$ е определна като $f(x) = 2x$ и имаме множествата

$$X = \{0, 1, 2, 3, 4, 5\}$$
$$Y = \{0, 1, 2, 3, 4, 5\},$$

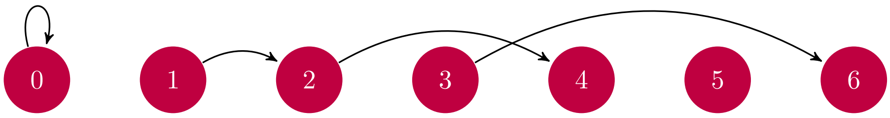
тогава:

$$f(X) = \{0, 2, 4, 6, 8, 10\},$$
$$f^{-1}(Y) = \{0, 1, 2\}.$$

Определение 3.3. Нека $f : A \to B$ е функция. Нека $X \subseteq A$. Рестрикция на f до множеството X, наричаме множеството:

$$f \upharpoonright X = f \cap X \times B.$$

Лесно се вижда, че рестрикцията на функция до множество, също е функция. Например рестрикцията на функцията f от предишния пример до множеството $\{0, 1, 2, 3\}$ може да се представи графично по следния начин:



Когато разглеждахме различни методи за задаване на множество в първа глава, една от възможностите беше да дефинираме множество по индукция от базово множество с помощта на някакви правило. Сега вече можем да опишем този метод с по голяма прецизност.

Определение 3.4. Нека $f : A \to A$ е функция, а $A_0 \subseteq A$ е базово множество. Нека за всяко $n \geq 0$, $A_{n+1} = A_n \cup f(A_n)$. Затваряне на множеството A_0 по отношение на функцията f наричаме множеството:

$$f[A] = \bigcup_{n \in \mathbb{N}} A_n.$$

Твърдение 3.5. Нека $f : A \to A$ е функция, а $A_0 \subseteq A$ е базово множество. $f[A_0]$ е най-малкото множество по отношение на релацията $\subseteq$, което съдържа A и е затворено по отношение на f: ако $a \in f[A^0]$, то и $f(a) \in f[A^0]$.

Доказателство. Вижте доказателството на Твърдение 1.25. $\square$

Например, ако f е както в предния пример ($f(x) = 2x$), затварянето на множеството $\{0\}$ по отношение на f е $f[\{0\}] = \{0\}$. Но затварянето на $\{1\}$ е $f[\{1\}] = \{1, 2, 4, 8, \dots\} = \{2^n \mid n \in \mathbb{N}\}$.

3.2.2 Композиция на функции

Дефиницията за композиция на две функции $f : A \to B$ и $g : B \to C$ вече ни е позната от предишната глава. Това е релация $f \circ g$ над A и C, дефинирана чрез:

$$f \circ g = \{(a, c) \mid \exists b \in B((a, b) \in f \ \& \ (b, c) \in g)\}.$$

Операцията композиция приложена към функции винаги дава функция.

Твърдение 3.6. Нека $f : A \to B$ и $g : B \to C$ са функции. Тогава $f \circ g$ също е функция.

Доказателство.

Нека $a \in A$. Тогава понеже f е функция, има елемент $b \in B$ такъв, че $(a, b) \in f$. От друга страна понеже g е функция, има елемент $c \in C$ такъв, че $(b, c) \in g$. Така $(a, c) \in f \circ g$ и следователно $dom(f \circ g) = A$.

Нека допуснем , че (a, c_1) и (a, c_2) са елементи на $f \circ g$. Тогава съгласно дефиницията на операция композиция има елементи $b_1, b_2 \in B$ такива, че $((a, b_1) \in f \ \& \ (b_1, c_1) \in g)$ и $((a, b_2) \in f \ \& \ (b_2, c_2) \in g)$. Но f е функция, следователно $b_1 = b_2 = b$. Сега $(b, c_1) \in g$ и $(b, c_2) \in g$, но g също е функция, следователно $c_1 = c_2$. $\square$

Така получаваме лесен начин да получим правило за $f \circ g$ от правила за f и g: $f \circ g(x) = g(f(x))$.

Операцията композиция може да се обобщи, когато разглеждаме функции на повече аргументи.

Определение 3.7. Нека е множество, $n, k \in \mathbb{N}$. Нека $g : A^n \to A$ и $f_1 \dots f_n : A^k \to A$ са функции. Тогава функцията $h : A^k \to A$, дефинирана чрез

$$h(a_1, \dots a_k) = g(f_1(a_1 \dots a_k), \dots f_n(a_1 \dots a_k)),$$

наричаме суперпозиция на g с $f_1, \dots f_n$.

Забележете, че при $n = k = 1$ получаваме точно дефиницията за композицията $f \circ g$.

3.2.3 Инекция, сюрекция, биекция

За разлика от операцията композиция на функции, която винаги дава функция, обратната релация на функция не винаги е функция. Нека $f : A \to B$ е функция. Какви свойства трябва да има f за да бъде релацията $f^{-1} = \{(b, a) \mid (a, b) \in f\}$ функция от B към A? Първото изискване е, за всеки елемент $b \in B$ да има елемент $a \in A$ такъв, че $(b, a) \in f^{-1}$, а следователно $(a, b) \in f$.

Определение 3.8. Нека $f : A \to B$ е функция. f е сюрекция ако:

$$\forall b \in B \exists a \in A((a, b) \in f).$$

Друго наименование за сюрекция е "върху", а еквивалентен начин да формулираме условието за сюрекция е $range(f) = B$. Композиция на сюрекции е сюрекция.

Твърдение 3.9. Нека $f : A \to B$ и $g : B \to C$ са сюрекции. Тогава $f \circ g$ също е сюрекция.

Доказателство. Нека $c \in C$. Трябва да намерим елемент $a \in A$ такъв, че $f \circ g(a) = c$. g е сюрекция, следователно има елемент $b \in B$ такъв, че $g(b) = c$. Сега $b \in B$ и f е сюрекция, следователно има елемент $a \in A$ такъв, че $f(a) = b$. Тогава $f \circ g(a) = g(f(a)) = g(b) = c$. $\square$

Функцията над естествените числа $f(x) = 2x$, не е сюрекция, защото например за $b = 1$ не съществува $a \in \mathbb{N}$, такова, че $2 = 1$.

Пример за сюрекция е функцията $g : \mathbb{N} \to \mathbb{N}$ дефинирана чрез $g(x) =$ най-голямото n такова, че 2^n дели x. Наистина за всяко естествено число n $g(2^n) = n$, следователно g е сюрекция. Въпреки това обратната релация

g^{-1} отново не е функция. Причината е, при фиксирано естествено число n има много различни естествени числа m такива, че $(n, m) \in g$. Например $g(12) = g(20) = g(28) = 4$. Така достигаме до второ изискване, което трябва да наложим към една функция, за да бъде нейната обратна релация също функция: на различни стойности, функцията трябва да съпоставя различни стойности.

Определение 3.10. Нека $f : A \to B$ е функция. f е инекция ако:

$$\forall a_1, a_2 \in A(a_1 \neq a_2 \to f(a_1) \neq f(a_2)).$$

Твърдение 3.11. Нека $f : A \to B$ и $g : B \to C$ са инекции. Тогава $f \circ g$ също е инекция.

Доказателство. Нека $a_1 \neq a_2$ са елементи на A. Трябва да покажем, че $f \circ g(a_1) = g(f(a_1)) \neq g(f(a_2)) = f \circ g(a_2)$. f е инекция, следователно $f(a_1) \neq f(a_2)$. Сега $f(a_1)$ и $f(a_2)$ са два различни елементи от множеството B и g е инекция, следователно $g(f(a_1)) \neq g(f(a_2))$. □

Определение 3.12. Нека $f : A \to B$ е функция. f е биекция, ако f е инекция и f е сюрекция.

Следствие 3.13. Нека $f : A \to B$ е функция. Следните условия са еквивалентни:

1. f е биекция.
2. f^{-1} е функция.
3. f^{-1} е биекция.

Доказателство. Методът, по който въведохме понятията инекция и сюрекция, беше точно да разгледаме необходимите и достатъчни условия за това f^{-1} да е функция. Следователно (1) $\Leftrightarrow$ (2). Обратната релация на f^{-1} е f. Тъй като f е функция, f^{-1} е биекция и (2) $\Leftrightarrow$ (3). □

Следствие 3.14. Нека $f : A \to B$ и $g : B \to C$ са биекции. Тогава $f \circ g$ също е биекция.

Доказателство. Това е директно следствие от Твърдение 3.9 и Твърдение 3.11. □

3.3 Някои по-важни функции

3.3.1 Идентитет

Нека A е множество. Функцията $id_A : A \to A$, $id_A(a) = a$, наричаме идентитет над множеството A.

Идентитетът винаги е биекция и $id_A^{-1} = id_A$. Идентитетът е единствената релация над множеството A, която е едновременно функция, релация на еквивалентност и частична наредба.

Ако $f : A \to B$ е функция, то $id_A \circ f = f \circ id_B$.

3.3.2 Характеристична функция

Нека U е множество. С всяко подмножество $A \subseteq U$ свързваме по една функция $\chi_A : U \to \{0, 1\}$, дефинирана чрез следното равенство:

$$\chi_A(x) = \begin{cases} 1, & \text{ако } x \in A; \\ 0, & \text{ако } x \notin A. \end{cases}$$

Характеристичната функция на множество кодира информацията, затова кои елементи от U му принадлежат и кои не. Всъщност това дефинира взаимно еднозначно съответствие (или биекция) между подмножествата на U и функциите $f : U \to \{0, 1\}$. Нека с $\mathcal{F}_U$ означим множеството от всички функции $f : U \to \{0, 1\}$. Тогава:

Твърдение 3.15. Функцията $F : 2^U \to \mathcal{F}_U$, дефинирана чрез:

$$F(A) = \chi_A$$

е биекция.

Доказателство. Ще покажем, че F е сюрекция и инекция. Нека $f \in \mathcal{F}_U$. Да разгледаме множеството $A = f^{-1}(\{1\})$. Твърдим, че характеристичната функция на A е точно f. За да проверим дали двете функции са равни, трябва да видим че са всеки възможен аргумент $x \in U$, $\chi_A(x) = f(x)$. Нека $x \in U$. Имаме две възможности: $\chi_A(x) = 1$ и $\chi_A(x) = 0$.

$$\chi_A(x) = 1 \Rightarrow x \in A \Rightarrow x \in f^{-1}(\{1\}) \Rightarrow f(x) = 1.$$

От друга страна:

$$\chi_A(x) = 0 \Rightarrow x \notin A \Rightarrow x \notin f^{-1}(\{1\}) \Rightarrow f(x) \neq 1 \Rightarrow f(x) = 0.$$

Така $\chi_A = f$ и следователно $F(A) = f$.

Нека сега A_1 и A_2 са две различни подмножества на U. Трябва да покажем, че техните характеристични функции са различни, т.е. поне за един аргумент $x \in U$, $\chi_{A_1}(x) \neq \chi_{A_2}(x)$. Щом $A_1 \neq A_2$, то има елемент $x \in U$ такъв, че или $x \in A_1 \setminus A_2$, или $x \in A_2 \setminus A_1$. Тъй като двата случая са симетрични и доказателството в единия случай се получава буквално като разменим индексите 1 и 2 в доказателството на другия случай, без ограничени на общността можем да предположим, че е налице първия случай: $x \in A_1 \setminus A_2$. Но тогава $\chi_{A_1}(x) = 1$, а $\chi_{A_2}(x) = 0$ и следователно $F(A_1) = \chi_{A_1} \neq \chi_{A_2} = F(A_2)$. Така F е инекция. □

3.3.3 Фамилии от множества, редици от множества

Понятието функция ни позволява да уточним още две понятия.

Вече разгледахме понятието фамилия от множества, индексирана с някакво индексно множество I. Там казахме, че на всеки индекс i е съпоставено множество A_i. Сега можем да дефинираме понятието по точно:

Нека I е непразно множество, а $\mathcal{A}$ е множество от множества. Нека $f : I \to \mathcal{A}$ е функция. Тогава с всяко $i \in I$ сме свързали множеството $A_i = f(i)$. Фамилията индексирана с I е просто $\{f(i) \mid i \in I\} = range(f)$.

Аналогично разсъждение може да се проведе за понятието редица от елементи $\{a_i\}_{i \in \mathbb{N}}$. Когато дефинираме редица от елементи, всъщност дефинираме функция $f : \mathbb{N} \to A$, и $a_i = f(i)$.

3.4 Мощност на множество

Когато разглеждаме крайни множества една от основните характеристики на едно крайно множество A е броят на неговите елементи $|A|$.

С помощта на функции лесно можем да сравняваме брой елементи на крайни множества. Броят на елементите на множество A е по-малък или равен на броя на елементите на множество B тогава и само тогава, когато съществува инекция $f : A \to B$. Този принцип се нарича принцип на Дирихле и е известен още като принцип на чекмеджетата: Ако трябва да приберем n предмета в m чекмеджета (да построим функция, която на всеки предмет съпоставя чекмедже, в което да бъде прибран) и $n > m$, то поне в едно чекмедже, ще трябва да приберем поне два предмета (няма как тази функция да е инекция).

Твърдение 3.16 (Принцип на Дирихле)**.** Нека A и B са крайни множества. $|A| \leq |B|$ тогава и само тогава, когато съществува инекция $f : A \to B$.

Доказателство. Нека $A = \{a_1 \dots a_n\}$ и $B = \{b_1 \dots b_m\}$. Ако $n \leq m$, то функцията $f : A \to B$, дефинирана чрез: $f(a_i) = b_i$ за $1 \leq i \leq n$ е инекция.

Нека сега $f : A \to B$ е инекция. Да разгледаме множеството $\{f(a_1), \dots f(a_n)\} = range(f)$. Тъй като f е инекция, за $i \neq j$, $f(a_i) \neq f(a_j)$. Така $|range f| = n$. Тъй като $range f \subseteq B$, B съдържа поне n на брой елемента и $|B| \geq n$. □

Като следствие от този принцип получаваме принцип за биекцията:

Теорема 3.17 (Принцип за биекцията)**.** Нека A и B са крайни множества. $|A| = |B|$ тогава и само тогава, когато съществува биекция $f : A \to B$.

Доказателство. Нека $A = \{a_1 \dots a_n\}$ и $B = \{b_1 \dots b_n\}$.

Функцията $f : A \to B$, дефинирана чрез: $f(a_i) = b_i$ за $1 \leq i \leq n$ е биекция.

Нека сега $f : A \to B$ е биекция. Тогава f и инекция и съгласно принципа на Дирихле $|A| \leq |B|$. Функцията $f^{-1} : B \to A$ също е инекция и следователно $|B| \leq |A|$. Така $|A| = |B|$. □

Когато говорим за безкрайни множества, понятието брой елементи вече няма ясен смисъл. Все пак интуитивно бихме могли да считаме, че две множества A и B имат еднакво количество елементи, ако съществува еднозначно съответствие между техните елементи, т.е. ако съществува биекция между тях.

Определение 3.18. Нека A и B са множества. Ще казваме, че A е равномощно с B, $A \sim B$, ако съществува биекция $f : A \to B$.

Нека ограничим разглежданията си до свят, който се състои от всички подмножества на някакво фиксирано множество U. Тогава релацията A е равномощно на B е релация на еквивалентност над множеството от всички подмножества на U.

Твърдение 3.19. Нека U е множество. $R = \{(A, B \mid A \sim B\}$ е релация на еквивалентност над 2^U.

Доказателство. Всяко множество A е равномощно на себе си, защото $id_A : A \to A$ е биекция. Следователно релацията е рефлексивна.

Нека $A \sim B$ и нека $f : A \to B$ е биекция. Тогава $f^{-1} : B \to A$ е биекция. Следователно $B \sim A$ и релацията е симетрична.

Нека $A \sim B$ и $B \sim C$ и нека $f : A \to B$ и $g : B \to C$ са биекции. Тогава $f \circ g : A \to C$ също е биекция. Така $A \sim C$ и релацията е транзитивна. $\square$

Множества, които са крайни или равномощни с $\mathbb{N}$ наричаме изброими множества.

Пример за изброимо безкрайно множество е $2\mathbb{N}$, защото функцията $f : \mathbb{N} \to 2\mathbb{N}$, дефинирана чрез $f(n) = 2n$ е биекция. За да покажем, че едно безкрайно множество е изброимо, достатъчно е да подредим елементите му в редица без повторения. Наистина вече видяхме, че дефиницията на редица $a_0, a_1, \dots a_n, \dots$ с елементи от множество A означава, че дефинираме функция $f : \mathbb{N} \to A$, като $f(i) = a_i$. За да бъде тази функция биекция, трябва допълнително за различни индекси да имаме различни елементи $(i \neq j \to a_i \neq a_j)$ и всеки елемент от A да се появи някъде в редицата $(\forall a \in A \exists i(a = a_i)$. Така например можем да покажем, че множеството от целите числа е изброимо, защото можем да подредим елементите му така:

$$0, 1, -1, 2, -2, 3, -3 \dots n, -n, \dots$$

Малко по-трудно е да се убедим, че $\mathbb{N} \times \mathbb{N}$ също е изброимо множество. Елементите на $\mathbb{N} \times \mathbb{N}$ могат да се подредят в безкрайна таблица:

$$\begin{pmatrix} (0,0) & (0,1) & (0,2) & \dots & (0,n) & \dots \\ (1,0) & (1,1) & (1,2) & \dots & (1,n) & \dots \\ (2,0) & (2,1) & (2,2) & \dots & (2,n) & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \\ (n,0) & (n,1) & (n,2) & \dots & (n,n) & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix}$$

Твърдение 3.20. Множеството $\mathbb{N} \times \mathbb{N}$ е изброимо.

Доказателство. Друга биекция между множеството $\mathbb{N} \times \mathbb{N}$ и $\mathbb{N}$ е следната функция:

$$\pi(x, y) = 2^x(2y + 1) - 1.$$

За да докажем, че това е биекция ще се възползваме от основната теорема на аритметиката, която гласи, че:

Теорема 3.21 (Основна теорема на аритметиката)**.** Всяко естествено число $n \geq 2$ се представя по единствен начин с точност до реда на множителите като произведение от прости множители.

Нека $(x_1, y_1) \neq (x_2, y_2)$ са две различни двойки естествени числа. Ако $x_1 \neq x_2$, то $2^{x_1} \neq 2^{x_2}$ и съгласно основната теорема на аритметиката, тъй като $2y_1 + 1$ и $2y_2 + 1$ са числа в чието представяне като произведение на прости множители не участва 2, трябва $2^{x_1}(2y_1+1) \neq 2^{x_2}(2y_2+1)$. Ако $x_1 = x_2$ то $y_1 \neq y_2$ и отново $2^{x_1}(2y_1 + 1) \neq 2^{x_2}(2y_2 + 1)$. Така $\pi(x_1, y_1) \neq \pi(x_2, y_2)$ и следователно π инекция.

Нека сега n е произволно естествено число. Ако $n = 0$, то $\pi(0, 0) = 1$. Нека сега $n \geq 1$, тогава $n + 1 \geq 2$ и $n + 1$ се представя по единствен начин като произведение $2^x.z$, където $x \geq 0$, а z е произведение от прости числа, различни от 2. Така z е нечетно число и следователно $z = 2y + 1$. Сега $\pi(x, y) = n$. $\square$

Съществуването на биекция $f : A \to B$ се доказва трудно. В много случаи по-лесно е да се докаже, че съществуват две инекции $g_1 : A \to B$ и $g_2 : B \to A$. Ако A и B са крайни множества, това е равносилно на съществуването на биекция между двете множества. Наистина от принципа на Дирихле и съществуването на две инекции получаваме, че $|A| = |B|$, а от принципа на биекцията, че има биекция между тях. Тази еквивалентност е обобщена за произволни множества в следващата теорема, известна като теорема на Кантор-Шрьодер-Бернщайн.

Теорема 3.22 (Кантор-Шрьодер-Бернщайн)**.** Нека A и B са множества. $A \sim B$ тогава и само тогава, когато съществуват инекции $f : A \to B$ и $g : B \to A$.

Доказателство. Едната посока на тази теорема е лесна: ако $A \sim B$, нека $f : A \to B$ е биекция (следователно инекция), тогава $g = f^{-1}$ е втората търсена инекция. Затова нека $f : A \to B$ и $g : B \to A$ са инекции. Ще построим биекция $h : A \to B$.

С индукция по n дефинираме следната редица редица от множества C_n. Нека $C_0 = A \setminus g(B)$. За всяко $n \geq 0$, $C_{n+1} = g(f(C_n))$. Нека $C = \bigcup_{n\in\mathbb{N}} C_n$.

Сега за всяко $a \in A$, дефинираме $h(a)$ по следния начин:

- Ако $a \in C$, то $h(a) = f(a)$.
- Ако $a \notin C$, то в частност $a \notin C_0$. Следователно $a \in g(B)$ и понеже g е инекция съществува единствен елемент $b \in B$ такъв че $g(b) = a$. Нека $h(a) = b$.

Така функцията h е дефинирана за всяко $a \in A$. Остава да покажем, че h е инекция и сюрекция.

Нека $a_1 \neq a_2$. Ако $a_1, a_2 \in C$ то $h(a_1) \neq h(a_2)$ следва от инективността на f. Ако $a_1, a_2 \notin C$ то $h(a_1) \neq h(a_2)$ следва от това, че g е функция. Остава възможността единия елемент да е от C а другия от $A \setminus C$. Без ограничение на общността да предположим, че $a_1 \in C$ и $a_2 \notin C$. Да допуснем, че $h(a_1) = h(a_2)$, тогава $g(f(a_1)) = a_2$. Тъй като $a_1 \in C = \bigcup_{n\in\mathbb{N}} C_n$, съществува n такова, че $a_1 \in C_n$, но тогава $a_2 = f(g(a_1)) \in C_{n+1} \subseteq C$, което противоречи на $a_2 \notin C$. Така h е инективна функция.

Нека сега $b \in B$. Ако $g(b) \notin C$ то съгласно дефиницията на h, $h(g(b)) = b$. Ако $g(b) \in C$, то съществува n такова, че $g(b) \in C_n$. При това $g(b) \notin C_0 = A \setminus g(B)$, значи $n \geq 1$ и $g(b) \in g(f(C_{n-1}))$. Така $g(b) = g(z)$ за някое $z \in f(C_{n-1})$. Но g е инекция, следователно $b = z$. В крайна сметка $b \in f(C_{n-1})$, следователно $b = f(a)$, за някое $a \in C_{n-1} \subseteq C$. Съгласно дефиницията на h, $h(a) = b$. Така h е сюрекция и следователно биекция. □

Като използваме тази теорема ще покажем необходимо и достатъчно условие за изброимост на множество.

Твърдение 3.23 (Критерий за изброимост)**.** Нека е множество. A е изброимо тогава и само тогава, когато съществува инекция $f : A \to \mathbb{N}$.

Доказателство. Нека A е изброимо. Ако $A = \{a_1, \ldots a_n\}$ е крайно, то функцията $f : A \to \mathbb{N}$, дефинирана чрез $f(a_i) = i$ е инекция. Ако A е безкрайно то по дефиниция има биекция $f : A \to \mathbb{N}$. Така условието е необходимо.

Нека $f : A \to \mathbb{N}$ е инекция. Ако A е крайно - то A е изброимо. Нека A е безкрайно. Ще дефинираме инекция $g : \mathbb{N} \to A$. Тогава съгласно теоремата на Кантор-Шрьодер-Бернщайн, $A \sim \mathbb{N}$ и A е изброимо.

Ще дефинираме $g(n)$ на стъпки.

- $n = 0$: Понеже A не е крайно, $A \neq \emptyset$ и следователно има поне един елемент. Нека $g(0)$ е произволен елемент $a \in A$.
- $n \to n+1$. Нека сме дефинирали $\{g(0), \dots g(n)\}$. Понеже A не е крайно $A \nsubseteq \{g(0), \dots g(n)\}$. Нека $g(n+1)$ е произволен елемент $a \in A \setminus \{g(0), \dots g(n)\}$.

Така показахме, че условието е достатъчно. $\square$

Теорема 3.24. Изброимо обединение на изброими множества е изброимо множество.

Доказателство. Нека I е изброимо множество и нека $\{A_i\}_{i \in I}$ е фамилия от множества индексирана с I, такава, че за всяко $i \in I$, A_i е изброимо. Ще покажем, че $\bigcup_{i \in I} A_i$ е изброимо множество.

Съгласно критерия за изброимост има инекция $f : I \to \mathbb{N}$ и за всяко $i \in I$ инекция $g_i : A_i \to \mathbb{N}$. Да разгледаме функцията $h : \bigcup_{i \in I} A_i \to \mathbb{N} \times \mathbb{N}$, дефинирана така:

За всяко $a \in \bigcup_{i \in I} A_i$ нека i_a е индексът с най-малка стойност на $f(i_a)$ измежду всички $\{j \in I \mid a \in A_j\}$. Тогава $h(a) = (f(i_a), g_{i_a}(a))$. Така дефинираната функция h е инекция защото ако $a \neq b$ са два различни елемента от $\bigcup_{i \in I} A_i$, то или $i_a \neq i_b$ и следователно $f(i_a) \neq f(i_b)$, или $i_a = i_b = i$ и тогава $g_i(a) \neq g_i(b)$.

Окончателно функцията $h \circ \pi$, където $\pi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ е биекцията дефинирана в доказателството на Твърдение 3.20 е търсената инекция от $\bigcup_{i \in I} A_i$ в $\mathbb{N}$. $\square$

Не всички множества са изброими. Множеството от всички подмножества на $\mathbb{N}$ например е неизброимо. Методът за доказателство на това твърдение е известен като диагонален метод на Кантор.

Теорема 3.25. Множеството $2^{\mathbb{N}}$ е неизброимо.

Доказателство. $2^{\mathbb{N}}$ не е крайно множество например, защото за всяко $n \in \mathbb{N}$ съдържа елементът $\{n\}$. Да допуснем, че съществува биекция $f : \mathbb{N} \to 2^{\mathbb{N}}$. Това означава, че всички подмножества на $\mathbb{N}$ могат да бъдат подредени в редица: $A_0 = f(0), A_1 = f(1) \dots A_n = f(n), \dots$. Като използваме характеристичните функции на множествата A_i, да разгледаме следната таблица:

$$\begin{pmatrix} \chi_{A_0}(0) & \chi_{A_0}(1) & \chi_{A_0}(2) & \dots & \chi_{A_0}(n) & \dots \\ \chi_{A_1}(0) & \chi_{A_1}(1) & \chi_{A_1}(2) & \dots & \chi_{A_1}(n) & \dots \\ \chi_{A_2}(0) & \chi_{A_2}(1) & \chi_{A_2}(2) & \dots & \chi_{A_2}(n) & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \chi_{A_n}(0) & \chi_{A_n}(1) & \chi_{A_n}(2) & \dots & \chi_{A_n}(n) & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix}$$

Напомняме, че характеристичната функция на множество A се дефинира като:

$$\chi_A(x) = \begin{cases} 1, & \text{ако } x \in A; \\ 0, & \text{ако } x \notin A. \end{cases}$$

Така таблицата съдържа пълна информация за всички множества от естествени числа. Ще достигнем до противоречие като посочим множество от естествени числа, която не би могло да фигурира в тази таблица. Взимаме главния диагонал на тази таблица. Той съдържа информация за по една стойност на всяка от посочените характеристични функции:

$$\chi_{A_0}(0), \chi_{A_1}(1), \chi_{A_2}(2), \ldots, \chi_{A_n}(n), \ldots$$

Ако дефинираме функцията $d : \mathbb{N} \to \{0, 1\}$ като: $d(i) = 1 - \chi_{A_i}(i)$, то d ще е функция, различна от всички характеристични функции в таблицата. Тогава $D = \{i \mid d(i) = 1\}$ е множество от естествени числа с характеристична функция $\chi_D = d$, което се различава от всяко от множествата $A_0, \ldots A_n, \ldots$. Но това противоречи на допускането, че редицата $\{A_0, A_1, A_2, \ldots A_n, \ldots\}$ съдържа всички елементи от $2^{\mathbb{N}}$.

Следователно допускането е грешно и $2^{\mathbb{N}}$ е неизброимо. □

Горното твърдение може да се обобщи за произволно множество. Доказателството макар и кратко скрива интуицията, която получаваме от доказателството на предишната теорема, затова предпочетохме да изложим и двете доказателства.

Теорема 3.26. Нека е множество. Тогава $2^A \nsim A$.

Доказателство. Да допуснем, че има биекция $f : A \to 2^A$. Нека $D = \{a \in A \mid a \notin f(a)\}$. Тогава $D \subseteq A$ и следователно $D = f(a_0)$ за някое $a_0 \in A$. Но тогава:

$$a_0 \in D \Leftrightarrow a_0 \notin f(a_0) \Leftrightarrow a_0 \notin D$$

Това е противоречие, следователно $2^A \nsim A$. □

3.5 Задачи за упражнение

Задача 1. Нека $A = \{a, b, c, d\}$ и $B = \{1, 2, 3, 4, 5\}$. Кое от следните релации е функция от A към B. Напишете графичното представяне на всяка от релациите. Как можем по графичното представяне на релация да разберем, дали тя е функция?

1. $\{(a, 1), (b, 2), (c, 3)\}$.
2. $\{(a, 1), (b, 2), (c, 3), (d, 4), (d, 5)\}$.
3. $\{(a, 1), (b, 2), (c, 3), (d, 5)\}$.
4. $\{(a, 1), (b, 2), (c, 2), (d, 5)\}$.
5. $\{(a, 5), (b, 5), (c, 5), (d, 5)\}$.

Задача 2. Кое от следните множества е функция над $\mathbb{Z}$?

1. $\{(a, |a|) \mid a \in \mathbb{Z}\}$.
2. $\{(|a|, a) \mid a \in \mathbb{Z}\}$.
3. $\{(a, a + 1) \mid a \in \mathbb{Z}\}$.

4. $\{(a+1, a) \mid a \in \mathbb{Z}\}$.

5. $\{(a, 2a) \mid a \in \mathbb{Z}\}$.

6. $\{(2a, a) \mid a \in \mathbb{Z}\}$.

Задача 3. За всяка от функциите f от Задача 2. определете:

1. $f(\mathbb{N})$, $f^{-1}(\mathbb{N})$, $f \restriction \mathbb{N}$.

2. $f(\{-2, -1, 0, 1, 2\})$, $f^{-1}(\{-2, -1, 0, 1, 2\})$, $f \restriction \{-2, -1, 0, 1, 2\}$.

Задача 4. Нека $f : A \to B$, $X, Y \subseteq B$. Вярно ли е, че:

1. $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$.

2. $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$.

3. $f^{-1}(X \setminus Y) = f^{-1}(X) \setminus f^{-1}(Y)$.

Задача 5. Нека $f : \mathbb{R} \to \mathbb{N}$, е функцията дефинирана чрез $f(x) = \lfloor x \rfloor$, най-голямото естествено число, по-малко или равно на x. Определете $f([0, 5])$, $f((0, 5])$, $f([0, 5))$ и $f((0, 5))$.

Задача 6. Нека $f, g, h : \mathbb{R} \to \mathbb{R}$, са дефинирани чрез $f(x) = x + 1$, $g(x) = x^2 + 3x + 1$ и

$$h(x) = \begin{cases} x - 1, & \text{ако } \ x > 0; \\ \frac{x}{2}, & \text{ако } x \leq 0. \end{cases}$$

Намерете $f \circ g$ и $g \circ f$. Комутативна ли е операцията композиция на функции?

Намерете $(f \circ g) \circ h$ и $f \circ (g \circ h)$. Асоциативна ли е операцията композиция на функции?

Задача 6. Нека и B са множества от естествени числа с характеристични функции χ_A и χ_B. С помощта на операцията суперпозиция на функциите χ_A, χ_B, $+, -, *, min, max$ изразете характеристичните функции на $A \cap B$, $A \cup B$, $A \setminus B$, $A \Delta B$.

Задача 7. За всяка функция f от Задача 2. определете дали f е инекция, сюрекция или биекция.

Задача 8. За всяка от следните функции f определете дали f е инекция, сюрекция или биекция.

1. $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x + 3$.

2. $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2 - 4x + 2$.

3. $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^3 + 7$.

4. $f : \mathbb{N} \to \mathbb{N}$, $f(x) = \begin{cases} x + 1, & \text{ако } x \text{ е четно;} \\ x - 1, & \text{ако } x \text{ е четно.} \end{cases}$.

5. $f : \mathbb{N} \to \mathbb{N}$, $f(x) = rem(x, 3)$ (остатък при делене на 3).

6. $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $f(x, y) =$нод(x, y) (най-голям общ делител).

7. $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $f(x, y) = 3x + 2y$.

8. $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $f(x, y) = x^2 + y^2$.

9. $f : \mathbb{Q} \to \mathbb{Q}$, $f(x) = \begin{cases} 0, & \text{ако } x = 0; \\ \frac{1}{x}, & \text{ако } x \neq 0. \end{cases}$.

10. $f : \mathbb{R} \to \mathbb{R}$, $f(x) = |x| + 1$.

11. $f : (-\frac{\pi}{2}, \frac{\pi}{2}) \to \mathbb{R}$, $f(x) = tgx$.

12. $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $f(x, y) = 3^x.5^y$.

13. $f : \mathbb{R}^+ \to \mathbb{N}$, $f(x) = \lfloor x \rfloor$. (най-голямото естествено число, по-малко или равно на x.)

14. $f : \mathbb{N} \to \mathbb{N}$, $f(x) = (x + 1)$-вото просто число.

Задача 9. Нека $f : A \to B$, $g : B \to C$ са функции. Вярно ли е, че:

1. Ако f не е инекция, то $f \circ g$ не е инекция?

2. Ако g не е инекция, то $f \circ g$ не е инекция?

3. Ако f не е сюрекция, то $f \circ g$ не е сюрекция?

4. Ако g не е сюрекция, то $f \circ g$ не е сюрекция?

Задача 10. Като използвате принципа на Дирихле, покажете, че ако $|A| > k|B|$, то за всяка функция $f : A \to B$ има елемент $b \in B$ и елементи $seta_1 \dots a_{k+1}$, такива, че $f(a_1) = f(a_2) = \cdots = f(a_k) = b$.

Задача 11. В едно село има 400 жители. Докажете, че поне двама имат един и същ рожден ден и поне 34 са родени в един и същ месец.

Задача 12. Докажете, че за всяко ≥ 2, $\mathbb{N}^k$ е изброимо.

Задача 13. Докажете, че $\mathbb{Q}$ е изброимо.

Задача 14. Докажете, че ако $A \sim B$, то $2^A \sim 2^B$.

Задача 15. Докажете, че следните множества са равномощни:

1. $\mathbb{R}$;

2. $(-\frac{\pi}{2}, \frac{\pi}{2})$;

3. $(0, 1)$;

4. (a, b), където $a, b \in \mathbb{R}$ и $a < b$;

5. $2^{\mathbb{N}}$.

6. $\{f \mid f : \mathbb{N} \to \mathbb{N}\}$

Задача 16. Докажете, че множеството от всички думи над азбуката $\{a, b\}$ ($\{a, b\}^*$) е изброимо. Докажете, че множеството от всички безкрайни редици от букви a и b е неизброимо.

Глава 4

Комбинаторика

Досега разглеждахме множествата като абстрактни обекти и изследвахме техните общи характерситики и свойства. В тази глава ще се спрем на крайните множества, като основната задаче, която ще си посртавим е да намерим начин да преброим техните елементи. За целта ще са ни нужни две помощни средства: комбинаторни принципи, които ни помага да свеждаме нови задачи към множество по-прости задачи, и комбинаторни конфигурации, които ни помагат да различим между 4 основни начина за избиране на k предмета измежду n.

4.1 Основни комбинаторни принципи

Основните комбинаторни принципи са вече разгледани и доказани. Тук ще ги съберем накуп и ще ги доразвием.

4.1.1 Принцип за биекцията

Принципът за биекцията гласи, че ако A и B са крайни множества, $|A| = |B|$ тогава и само тогава, когато съществува биекция $f : A \to B$. Доказателство на този принцип се основава на принципа на Дирихле (принципа за чекмеджетата) и е посочено в Теорема 3.17. Този принцип ни позволява да свеждаме нови задачи към стари, но които вече знаем решението.

4.1.2 Принцип за събирането

Принципът за събирането гласи, че ако A и B са крайни непресичащи се множества, то броят на елементите на $A \cup B$ е сумата от броя на елементите на A и броя на елементите на B:

$$A \cap B = \emptyset \Rightarrow |A \cup B| = |A| + |B|.$$

Макар и лесен, този принцип има важни следствия. Въз основа на този принцип ще изведем четири негови обобщения: принцип за разликата, принцип за разбиването, принцип за обединението и принцип за крайните разлики.

Принципът за разликата има широко приложение. Интуитивно - ако видим, че задачата да преброим елементите на дадено множество е много сложна, например включва разглеждането на твърде много случаи, винаги трябва да проверим дали не е по-лесно да пресметнем броя на елементите на допълнението на това множество.

Твърдение 4.1 (Принцип за разликата)**.** Нека A и U са крайни множества и $A \subseteq U$. Тогава $|U \setminus A| = |U| - |A|$.

Доказателство. Това е директно приложение на принципа за събирането: $A \cap U \setminus A = \emptyset$, следователно $|U| = |A \cup U \setminus A| = |A| + |U \setminus A|$. Така $|U \setminus A| = |U| - |A|$. □

Принципът за разбиването ни позволява да разбием една задача на много подслучаи.

Твърдение 4.2 (Принцип за разбиването)**.** Нека $A_1 \dots A_n$ са взаимно непресичащи се крайни множества и $n \geq 2$. Тогава $|A_1 \cup A_2 \cup \dots A_n| = |A_1| + \dots + |A_n|$, т.е. $|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i|$.

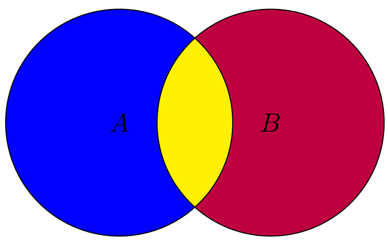
Доказателство. Доказателството е с индукция по n. При $n = 2$ получаваме точно принципа за събирането. Нека твърдението е вярно за n на брой непресичащи се множества и нека $A_1 \dots A_n, A_{n+1}$ са непресичащи се множества. Тогава $A_{n+1} \cap (A_1 \dots A_n) = \emptyset$ и съгласно принципа за събирането $|(A_1 \cup \dots \cup A_n) \cup A_{n+1}| = |(A_1 \cup \dots \cup A_n)| + |A_{n+1}|$. Съгласно индукционното предположение $|A_1 \cup A_2 \cup \dots A_n| = |A_1| + \dots + |A_n|$. Така $|\bigcup_{i=1}^{n+1} A_i| = \sum_{i=1}^{n+1} |A_i|$. □

Следващото обобщение ни позволява да пресмятаме броят елементи на обединението на произволни множества.

Твърдение 4.3 (Принцип за обединението)**.** Нека A и B са крайни множества. $|A \cup B| = |A| + |B| - |A \cap B|$.

Доказателство. Ще представим обединението на множествата A и B като обединение на три непресичащи се множества:

$$A \cup B = A \setminus (A \cap B) \cup (A \cap B) \cup B \setminus (A \cap B)$$



Съгласно принципа за разбиването:

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

Съгласно принципа за разликата:

$$|A \setminus (A \cap B)| = |A| - |A \cap B| \quad |B \setminus (A \cap B)| = |B| - |A \cap B|.$$

Така получаваме, че:

$$|A \cup B| = |A| - |A \cap B| + |A \cap B| + |B| - |A \cap B| = |A| + |B| - |A \cap B|.$$

□

Последният принцип се нарича принцип за включването и изключването и е възможно най-широкото обобщение на принципа за събиране. Той ни позволява да намираме броя на елементите на обединението на произволен n на брой множества.

Теорема 4.4 (Принцип за включването и изключването)**.** Нека $A_1 \dots A_n$ са n на брой крайни множества и $n \geq 2$. Тогава

$$|A_1 \cup A_2 \cup \dots \cup A_n| = \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i_1 < i_2 \leq n} |A_{i_1} \cap A_{i_2}| + \sum_{1 \leq i_1 < i_2 < i_3 \leq n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| - \dots + (-1)^{n-1} |A_1 \cap A_2 \dots \cap A_n|.$$

Доказателство. Доказателството е с индукция по n. При $n = 2$ имаме точно принципа за обединението. За да илюстрираме идеята на доказателството ще докажем принципа и за $n = 3$. Нека A_1, A_2, A_3 са множества. Първо групираме $_1$ с A_2 и прилагаме принципа за обединението:

$$|A_1 \cup A_2 \cup A_3| = |(A_1 \cup A_2) \cup A_3| = |A_1 \cup A_2| + |A_3| - |(A_1 \cup A_2) \cap A_3|.$$

Съгласно принципа за обединението $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$. Съгласно дистрибутивния закон $(A_1 \cup A_2) \cap A_3 = (A_1 \cap A_3) \cup (A_2 \cap A_3)$. Отново прилагаме принципа за обединението: $|(A_1 \cap A_3) \cup (A_2 \cap A_3)| = |A_1 \cap A_3| + |A_2 \cap A_3| - |A_1 \cap A_2 \cap A_3|$. Така получаваме:

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|.$$

Нека твърдението е в сила за n. Нека $A_1 \dots A_n, A_{n+1}$ са $n+1$ на брой крайни множества.

$$|A_1 \cup A_2 \cup \dots \cup A_n \cup A_{n+1}| = |(A_1 \cup A_2 \cup \dots \cup A_n) \cup A_{n+1}| =$$

$$|A_1 \cup A_2 \cup \dots \cup A_n| + |A_{n+1}| - |(A_1 \cup A_2 \cup \dots \cup A_n) \cap A_{n+1}| =$$

$$\sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i_1 < i_2 \leq n} |A_{i_1} \cap A_{i_2}| + \sum_{1 \leq i_1 < i_2 < i_3 \leq n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| - \dots + (-1)^{n-1} |A_1 \cap A_2 \dots \cap A_n| +$$

$$+ |A_{n+1}| - |(A_1 \cap A_{n+1}) \cup (A_2 \cap A_{n+1}) \cup \dots \cup (A_n \cap A_{n+1})| =$$

$$\sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i_1 < i_2 \leq n} |A_{i_1} \cap A_{i_2}| + \sum_{1 \leq i_1 < i_2 < i_3 \leq n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| - \dots + (-1)^{n-1} |A_1 \cap A_2 \dots \cap A_n| +$$

$$+ |A_{n+1}| - \sum_{1 \leq i_1 \leq n} |A_{i_1} \cap A_{n+1}| + \sum_{1 \leq i_1 < i_2 \leq n} |A_{i_1} \cap A_{i_2} \cap A_{n+1}| - \dots + (-1)^n |A_1 \cap A_2 \dots \cap A_n \cap A_{n+1}| =$$

$$\sum_{1 \leq i \leq n+1} |A_i| - \sum_{1 \leq i_1 < i_2 \leq n+1} |A_{i_1} \cap A_{i_2}| + \sum_{1 \leq i_1 < i_2 < i_3 \leq n+1} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| - \dots + (-1)^n |A_1 \cap A_2 \dots \cap A_n \cap A_{n+1}|.$$

□

4.1.3 Принцип за умножението

Принципът за умножението гласи, че ако A и B са крайни множества, то $|A \times B| = |A|.|B|$. Доказателство на този принцип е посочено в Теорема 2.3.

Този принцип също може да се обобщи по естествен начин.

Твърдение 4.5. Нека $A_1 \dots A_n$ са крайни множества и $n \geq 2$. Тогава $|A_1 \times A_2 \times \dots A_n| = |A_1|.|A_2| \dots .|A_n|$.

Доказателство. Доказателството е с индукция по n като се използва, че $A \times B \times C = (A \times B) \times C$.

4.2 Основни комбинаторни конфигурации

В този раздел ще разгледаме четири начина да изберем k предмета измежду n. За да онагледим задачата ще започнем с един пример. В местния клуб по бридж членуват 5 души. Трябва да се изберат измежду тях двама доброволци, които да отговарят за двете месечни сбирки на клуба. По колко начина могат да се изберат тези двама доброволци?

Преди да отговорим този въпрос трябва да уточним две неща. Има ли значение редът? С други думи за различни избори ли ще считаме Иван отговаря за първата среща, Петър за втората и Петър отговаря за първата, Иван за втората? Вторият уточнителен въпрос е възможни ли са повторения: може ли Иван да отговаря и за двете срещи. В зависимост от отговорите на тези уточнителни въпроси получаваме различен брой възможности за избор на доброволци. Ако са възможни повторения и редът има значение, бихме могли да илюстрираме един възможен избор: Иван за първа среща, Петър за втора среща, като наредена двойка (Иван, Петър). Нека за по-просто считаме, че членовете на клуба са a, b, c, d, e. Така можем да организираме всички възможности в следната таблица:

$$\begin{pmatrix} (a,a) & (a,b) & (a,c) & (a,d) & (a,e) \\ (b,a) & (b,b) & (b,c) & (b,d) & (b,e) \\ (c,a) & (c,b) & (c,c) & (c,d) & (c,e) \\ (d,a) & (d,b) & (d,c) & (d,d) & (d,e) \\ (e,a) & (e,b) & (e,c) & (e,d) & (e,e) \end{pmatrix}$$

Общо възможностите са 25.

В случай, че редът има значение, но не е позволено един и същ човек да отговаря и за двете срещи възможните избори са 20 - всички без тези по главния диагонал.

$$\begin{pmatrix} & (a,b) & (a,c) & (a,d) & (a,e) \\ (b,a) & & (b,c) & (b,d) & (b,e) \\ (c,a) & (c,b) & & (c,d) & (c,e) \\ (d,a) & (d,b) & (d,c) & & (d,e) \\ (e,a) & (e,b) & (e,c) & (e,d) & \end{pmatrix}$$

Ако не са позволени повторения и редът няма значение, достатъчно е да преброим изборите над главния диагонал: общо 10.

$$\begin{pmatrix} & (a,b) & (a,c) & (a,d) & (a,e) \\ & & (b,c) & (b,d) & (b,e) \\ & & & (c,d) & (c,e) \\ & & & & (d,e) \\ & & & & \end{pmatrix}$$

Ако редът няма значение, но пък може да повтаряме доброволци, прибавяме и главния диагонал и получаваме 15 възможности:

$$\begin{pmatrix} (a,a) & (a,b) & (a,c) & (a,d) & (a,e) \\ & (b,b) & (b,c) & (b,d) & (b,e) \\ & & (c,c) & (c,d) & (c,e) \\ & & & (d,d) & (d,e) \\ & & & & (e,e) \end{pmatrix}$$

Така получаваме четири основни конфигурации.

4.2.1 Конфигурации с повторение, с наредба

Професор X, след успешно завършване на кратко работно посещение на факултета по математическа ловкост и изобретателност в градчето Y, решил да изпрати поздравителни картички на своите приятели A, B, C, D и E. Разхождайки се един слънчев следобед из историческия център на Y, минал покрай една малка книжарница и видял на витрината изложени 26 вида картички с изгледи от близката планина Z. Професор X се спрял пред витрината и започнал да се чуди за кой приятел, да избере кой вид картичка. Колко са възможните избори за професор X?

Така професорът трябва да избере 5 елемента от 26 възможни, като редът има значение, защото първата е за A, втората е за B ... петата е за E. Възможни са и повторения - дори съвсем вероятно е професорът, от съображения за справедливост, да избере една и съща картичка за всичките си приятели.

Всъщност професор X трябва да построи една функция, която на всеки приятел от множеството $\{A, B, C, D, E\}$ съпоставя един от 26-те вида картички, значи елемент от множеството $\{I, II, III, \ldots, XXVI\}$.

Теорема 4.6. Нека A и B са множества, $|A| = k$, $|B| = n$. Броят на функциите $f : A \to B$ е n^k.

Доказателство. Ако $k = 0$, то $A = \emptyset$ има една единствена функция $f = \emptyset : A \to B$.

Нека $k \geq 1$ и нека $A = \{a_1 \ldots a_k\}$. Всяка функция $f : A \to B$ можем да представим еднозначно чрез вектора от нейните стойности

$$f = (f(a_1), \ldots f(a_k)) \in B^k.$$

Съгласно принципа на биекцията броят на различните функции е същият като броя на елементите на B^k. Съгласно принципа за умножението $|B^k| = |B|^k = n^k$ □

Така получаваме, че броят на конфигурациите на k елемента измежду n, с наредба и с повторение е:

$$K_{\text{нп}}(k, n) = n^k.$$

4.2.2 Конфигурации с наредба, без повторение

Когато професор X най-сетне направил своя избор, влезнал в книжарницата. Там за жалост разбрал от продавача, че от всеки вид картички е останала само по една бройка. Сега професорът бил изправен пред един съвсем различен избор. Колко са възможностите при тези обстоятелства?

Професорът трябва отново да избере 5 елемента от 26 възможни, като редът има значение, но вече не са възможни повторения. Сега професор X трябва да построи не каква да е функция, която на всеки приятел от множеството $\{A, B, C, D, E\}$ съпоставя елемент от множеството $\{I, II, III, \dots, XXVI\}$. Функцията трябва да е инекция - защото вече не е позволено един и същи вид да се повтаря.

Теорема 4.7. Нека A и B са множества, $|A| = k$, $|B| = n$. Броят на инекциите $f : A \to B$ е $n(n-1)\dots(n-k+1) = \prod_{i=0}^{k-1}(n-i)$.

Доказателство. Ако $k > n$ съгласно принципа на Дирихле няма инекции $f : A \to B$. Ще отбележим, че формулата остава вярна защото в $\prod_{i=0}^{k-1}(n-i)$ един от множителите ще е 0.

Ако $k = 0$, то $A = \emptyset$ има една единствена функция $f = \emptyset : A \to B$. Тази функция е инекция по тривиални съображения. Дефиницията на инекция е във формата на импликация, чиято предпоставка не би могла да е изпълнена за $\emptyset$.

Нека $k \geq 1$ и нека $A = \{a_1 \dots a_k\}$. Всяка инекция $f : A \to B$ можем да представим еднозначно отново чрез вектора от нейните стойностите

$$f = (f(a_1), f(a_2) \dots f(a_k)).$$

Сега обаче $f(a_1)$ е произволен елемент от B, но $f(a_2)$ е елемент на B, различен от $f(a_1)$, т.е елемент на $B \setminus \{f(a_1)\}$. Така $f(a_3) \in B \setminus f(a_1), f(a_2)$ ... $f(a_k) \in B \setminus \{f(a_1), f(a_2) \dots f(a_{k-1})\}$.

Съгласно принципа за умножението получаваме $\prod_{i=0}^{k-1}(n-i)$ възможности. $\square$

Така получаваме, че броят на конфигурациите на k елемента измежду n, с наредба и без повторение е:

$$K_{\text{н}}(k, n) = \prod_{i=0}^{k-1}(n-i).$$

В случая, когато $k = n$ конфигурацията с наредба, без повторение се нарича пермутация. Броят на различните пермутации на n елемента отговаря на броя на начините по които можем да подредим n различни елемента. Броят им се означава с $n!$ - факториел.

$$n! = \begin{cases} 1, & \text{ако } n = 0; \\ \prod_{i=0}^{n-1}(n-i) = n.(n-1), \dots .1 = \prod_{i=1}^{n} i, & \text{ако } n > 0. \end{cases}$$

4.2.3 Конфигурации без повторение, без наредба

Професор X прекарал цели 2 часа в книжарницата без успех. Накрая продавачът, който бързал за вкъщи, за да не изпусне приятелския футболен мач между университетските отбори на града Y и вражеския град P, подканил професора просто да избере 5-те картички, които му харесват най-много и по-късно да ги разпределя на своите приятели. Професорът, макар и малко недоволен от обслужването, се съгласил и бързо напуснал книжарницата с петте най-хубави картички. Колко са били възможните избори за професора сега?

Професорът отново избира 5 картички измежду 26, без право на повторение, но редът вече няма значение. Неговата цел е да избере едно 5-елементно подмножество от множество с 26 елемента (при това най-хубавото).

За да пресметнем броя на възможностите можем да разсъждаваме така. За да избере проф X 5 картички за своите приятели ще извърши две стъпки: първо ще подбере 5 картички, после ще ги разпредели на своите 5 приятеля. Общо това може възможностите са, както видяхме в предишната част, 26.25.24.23.22. Всеки избор на 5 картички води до 5! различни разпределения на картички. Така възможностите за избор на 5 картички остава да бъдат $\frac{26.25.24.23.22}{5!}$. Това число се нарича "26 над 5"и се означава с $\binom{26}{5}$.

За произволни n и k:

$$\binom{n}{k} = \frac{\prod_{i=0}^{k-1}(n-i)}{k!} = \begin{cases} 0, & \text{ако } n < k; \\ \frac{n!}{k!(n-k)!}, & \text{ако } n \geq k. \end{cases}$$

Теорема 4.8. Броят на k-елементните подмножества на множество с n елемента е $\binom{n}{k}$.

Доказателство. Ако $k > n$ няма k-елементи подмножества на множество с n елемента и формулата е вярна. Нека $k \leq n$ и A е множество.

Доказателството ще извършим с индукция по n. Ако $n = 0$, $A = \emptyset$ и единствената възможност за k е $k = 0$. ма едно единствено подмножество на A с 0 елемента - $\emptyset$. $1 = \frac{n!}{0!(n-0)!} = \binom{n}{0}$.

Нека твърдението е в сила за n. Тук индукционното предположение е по силно от обичайно: предполагаме че за всяко $k \leq n$, броят на k елементните подмножества на множество с n елемента е $\binom{n}{k}$. Нека $A = \{a_1 \dots a_n, a_{n+1}\}$ и $k \leq n+1$.

Отново, ако $k = 0$, има едно единствено подмножество на A с 0 елемента - $\emptyset$, и $1 = \frac{(n+1)!}{0!((n+1)-0)!} = \binom{n+1}{0}$.

Ако $k = n+1$, то също има едно единствено подмножество на A с n+1 елемента - A, и $1 = \frac{(n+1)!}{(n+1)!((n+1)-(n+1))!} = \binom{n+1}{n+1}$.

Ако $1 \leq k \leq n$ то можем да разделим k-елементните подмножества на A на две непресичащи се групи: група 1, на тези, които не съдържат елемента a_{n+1}, и група 2, на тези, които съдържат елемента a_{n+1}.

Елементите от група 1 са k-елементни подмножества на множеството с n елемента $\{a_1 \dots a_n\}$. Съгласно индукционното предположение, те са $\binom{n}{k}$ на брой.

Елементите от група 2 са от вида $\{a_{k+1}\} \cup B$, където B е $k-1$-елементно подмножество на множеството с n елемента $\{a_1 \dots a_n\}$. Следователно броят на елементите от група 2 са колкото са различните възможности за B. Съгласно индукционното предположение, те са $\binom{n}{k-1}$ на брой.

Съгласно принципа за събирането общо получаваме

$$\binom{n}{k} + \binom{n}{k-1} = \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} =$$

$$= \frac{n!}{(k-1)!(n-k!)(\frac{1}{k} + \frac{1}{n-k+1})} = \frac{(n+1)!}{k!(n+1-k)!} = \binom{n+1}{k}.$$

□

Така получаваме, че броят на конфигурациите на k елемента измежду n, без наредба и без повторение е:

$$K(k,n) = \binom{n}{k}.$$

Формулата от последния ред на доказателството се нарича формула на Паскал. С помощта на тази формула можем по индуктивно да намираме стойностите $\binom{n}{k}$ от предишно стойности. Пресмятането се организира най лесно с така наречения триъгълник на Паскал:

$$\begin{array}{ccccccccc}
 & & & & \binom{0}{0} & & & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4}
\end{array}$$

Крайните точки в триъгълника попълваме с 1, защото както вече видяхме $\binom{n}{0} = \binom{n}{n} = 1$ за всяко n. Останалите стойности $\binom{n}{k}$ попълваме като съберем стойностите на предишния ред точно над търсената: $\binom{n-1}{k-1} + \binom{n-1}{k}$.

$$\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & & 2 & & 1 & & \\
 & 1 & & 3 & & 3 & & 1 & \\
1 & & 4 & & 6 & & 4 & & 1
\end{array}$$

Числата $\binom{n}{k}$ са известни също и като биномни коефициенти. Причина за това е следната теорема на Нютон.

Теорема 4.9 (Нютон)**.** Нека $x, y \in \mathbb{R}$, $n \in \mathbb{N}$.

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k.y^{n-k}$$

Доказателство. Доказателството ще извършим с индукция по n.

$$(x+y)^0 = 1 = \binom{0}{0} x^0.y^{0-0}.$$

Нека твърдението е в сила за n.

$$(x+y)^{n+1} = (x+y)^n.(x+y) = (\sum_{k=0}^{n} \binom{n}{k} x^k.y^{n-k})(x+y) =$$

$$= \sum_{k=0}^{n} \binom{n}{k} x^{k+1}.y^{n-k} + \sum_{k=0}^{n} \binom{n}{k} x^{k}.y^{n-k+1} =$$

$$= \binom{n}{0} x.y^n + \binom{n}{1} x^2.y^n + \dots + \binom{n}{k-1} x^k.y^{n+1-k} + \dots \binom{n}{n} x^{n+1} +$$

$$+ \binom{n}{0} y^{n+1} + \binom{n}{1} x.y^n \dots + \binom{n}{k} x^k.y^{n+1-k} + \dots \binom{n}{n} x^n.y =$$

$$= \binom{n+1}{0} y^{n+1} + (\binom{n}{0} + \binom{n}{1}) x.y^n + \dots (\binom{n}{k-1} + \binom{n}{k}) x^k y^{n+1-k} + \dots \binom{n+1}{n+1} x^{n+1} =$$

$$= \sum_{k=0}^{n+1} \binom{n+1}{k} x^k.y^{n+1-k}.$$

□

Като следствие от тази теорема получаваме алтернативно доказателство на следната теорема:

Теорема 4.10. Нека A е крайно множество.

$$|2^A| = 2^{|A|}.$$

Доказателство. Подмножествата на A можем да разделим на следните непресичащи се групи:
Група 0: 0-елементните подмножества, които са 1 на брой.
Група 1:1-елементните подмножества, които са $\binom{n}{1}$ на брой.
Група 2: 2-елементните подмножества, които са $\binom{n}{2}$ на брой.
...
Група k: k-елементните подмножества, които са $\binom{n}{k}$ на брой.
...
Група n: n-елементните подмножества, които са $\binom{n}{n}$ на брой.

Съгласно принципа за разбиването получаваме общо:

$$1 + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{k} + \dots \binom{n}{n} = \sum_{k=1}^{n} \binom{n}{k}.$$

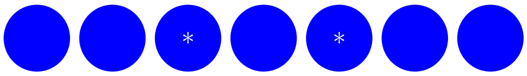
Съгласно теоремата на Нютон това е точно $(1+1)^n = 2^n$. □

4.2.4 Конфигурации без наредба, с повторение

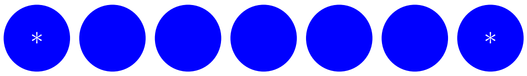
Цяла нощ професор X избирал и разпределял петте картички на своите петима приятели. На сутринта вече всичко било готово, картичките били надписани и професорът се отправил към пощата за да ги изпрати. Там го уведомили, че за всяка картичка трябва да закупи марки на стойност 1 лев. Те разполагали, с три вида марки - всяка от по 20 стотинки. Професорът вече твърдо решил, че на всяка картичка ще залепи едни и същи марки и все пак оставало да реши - по колко марки от всеки вид да си купи.

Сега въпросът е по колко начина могат да се изберат 5 предмета измежду 3 възможни, като наредбата няма значение, но са позволени (и се налагат) повторения.

Отговорът на този въпрос ще изведем като сведем тази задача до друга, вече позната конфигурация. Всеки възможен избор на марки ще кодираме по следния начин: в поредица от 7 кутийки ще поставим две звездички. Празните кутийки преди първата звездичка ще отговарят на броя марки от първи вид. Празните кутийки между двете звездички ще отговарят на марките от втори вид, а празните кутийки след втората звездичка ще отговарят на марките от трети вид. Така например следната картина отговаря на 2 марки от първи вид, 1 от втори и 2 от трети вид:



Ако искам да изберем всички марки от втори вид, избора ще се кодира така:



На всеки избор от марки съответства разпределяне на две звездички в 7-те кутийки и на всяко разпределяне на двете звездички в кутийки съответства избор на марки. Така съгласно принципа за биекцията, задачата се свежда до начините по които можем да изберем две от кутийките, в които да поставим 2 звездички: общо по $\binom{7}{2}$ начина.

В общия случай трябва да изберем k предмета измежду n вида, като наредбата няма значение но имаме право на повторения, ще ни трябват $k+n-1$ кутийки и $n-1$ звездички. Броят на конфигурациите на k елемента измежду n, без наредба и с повторение е:

$$K_{\text{п}}(k,n) = \binom{n+k-1}{n-1}.$$

4.3 Задачи за упражнение

Задача 1. Компютърна програма представя целите числа в двоичен запис. Първият бит представя знака на числото, а останалите - абсолютната стойност. Колко цели числа могат да се изпишат в регистър с n бита.

Задача 2. Искате да вземете 2 книги с вас на екскурзия. Имате 3 книги по дискретна математика, 2 книги по логика и 3 новели. Искате книгите, които ще вземете с вас да са на различна тематика. Колко са възможните избора.

Задача 3. В щата Юта всяка радиостанция се обозначава с идентификатор от 3 или 4 букви, като всеки идентификатор започва с K или N. Колко най-много радиостанции може да има?

Задача 4. Намираме се в Париж. Искаме да направим екскурзия като трябва да минем през Лондон и Брюксел, и обратно в Париж. Колко различни възможности за полети имаме ако всеки ден има 5 полета Париж -

Брюксел, Брюксел - Париж, 13 полета Париж - Лондон, Лондон Париж, 3 полета Лондон - Брюксел и 2 полета Брюксел - Лондон.

Задача 5. В телевизионно състезание първият играч трябва да отговори на 7 въпроса с или . Вторият играч трябва да отговори на 2 въпроса с по седем възможни отговора. Кой от двамата играчи има предимство?

Задача 6. В ресторант за десерт могат да се сервират 1, 2 или 3 топки сладолед. ма 5 вида сладолед - шоколад, ванилия, ягода, карамел и ментов сладолед. Колко различни десерта се предлагат?

Задача 7. Колко различни думи могат да се получат като се разместят буквите в думата:

1. “ релация"
2. “ наредба"
3. “ алабаланица"
4. “ непротивоконституционствувателствувайте"

Задача 8. По колко начина могат да седнат:

1. n човека на една пейка?
2. n мъже и n жени на една пейка като мъж седи само до жени, а жена само до мъже?
3. n човека на кръгла маса?
4. n мъже и n жени на кръгла маса като мъж седи само до жени, а жена само до мъже?

Задача 9. Имаме 10 задачи. Трябва да разпределим тези задачи измежду Алберт, Бети и Деби.

1. Искаме първо да решим колко задачи да изпълни Алберт, колко задачи да изпълни Деби и колко Бети. По колко начина можем да разпределим тези бройки?
2. По колко начина можем да разпределим задачите, ако Алберт трябва да изпълни 3, Бети 5, а Деби 2?

Задача 10. В игра с 52 карти едно раздаване са състои от 13 карти.

1. Колко са всички раздавания?
2. Колко са всички раздавания, при които се пада точно едно асо?
3. Колко са всички раздавания, при които се падат поне две валета?
4. Колко са всички раздавания, при които се падат 2 аса и 4 кари?

Задача 11. Дадена е шахматна дъска 8×8. Една фигура е позиционирана в най-долното най ляво квадратче и трябва да стигне до най-горното най-дясно квадратче. Може да извършва следните два вида хода: едно квадратче нагоре или едно квадратче надясно. По колко различни пътища може фигурата да достигне целта?

Задача 12. Колко цели числа име между 0 и 999, в които:

1. ма точно една цифра 5?
2. ма поне една цифра 5?
3. ма не повече от две цифри 5?

Задача 13. Колко решения в естествените числа има уравнението:

1. $x_1 + x_2 + x_3 + x_4 = 15$?
2. $x_1 + x_2 + x_3 + x_4 = 15$, ако $x_2 \geq 3$?
3. $x_1 + x_2 + x_3 + x_4 = 15$, ако $x_2 \geq 3$ и $x_3 \geq 5$?
4. $x_1 + x_2 + x_3 + x_4 = 15$, ако $x_2 < 7$?
5. $x_1 + x_2 + x_3 + x_4 = 15$, ако $x_2 < 7$ и $x_3 < 6$?
6. $x_1 + x_2 + x_3 + x_4 = 15$, ако $x_2 < 7$ и $x_3 < 6$ и $x_4 < 5$?

Задача 14. Колко числа има между 0 и 1001, които се делят:

1. на 3?
2. на 3 или на 5?
3. на 3 или на 5 или на 2?
4. на 3 или на 5 или на 2 или на 6?

Задача 15. Колко различни числа има между 0 и 9999

1. със сума на цифрите равна на 16?
2. имат цифрата 3 и цифрата 6, но няма цифрата 8?

Задача 16. Колко са 20-буквените думи в латинската азбука, които:

1. са палиндроми?
2. имат две последователни еднакви букви?
3. всяка буква в думата се среща точно два пъти?

Задача 17. Нека U е множество с n елемента. Колко са:

1. Двойките (X, Y), където $X, Y \subseteq U$?
2. Двойките (X, Y), където $X, Y \subseteq U$ и $|X| = 1$?
3. Двойките (X, Y), където $X, Y \subseteq U$ и $|X| = k$?
4. Двойките (X, Y), където $X, Y \subseteq U$ и $X \cap Y = \emptyset$?
5. Двойките (X, Y), където $X, Y \subseteq U$, $X \cap Y = \emptyset$ и $X \cup Y = U$?
6. Двойките (X, Y), където $X, Y \subseteq U$, $X \cap Y = \emptyset$ и $|X| \geq 2$ и $|Y| \geq 2$?

Глава 5

Дискретни функции

Определение 5.1. Нека A е крайно множество и $n \in \mathbb{N}$. Всяка функция $f : A^n \to A$ наричаме n-местна дискретна функция.

Твърдение 5.2. Нека A е крайно множество и $|A| = m$. Броят на различните n-местни дискретни функции $f : A^n \to A$ е m^{m^n}.

Доказателство. От Теорема 4.6 знаем, че броят на функциите $f : A^n \to A$ е $|A|^{|A^n|}$. От принципа за умножението получаваме, че $|A^n| = |A|^n$. Така броят на различните n-местни дискретни функции $f : A^n \to A$ е m^{m^n}. $\square$

5.1 Булеви функции.Представяния.

Ние ще се занимаваме предимно с двоични (булеви) функции, дискретни функции, при които множеството A е $\{0,1\}$. Множеството на n-местните булеви функции, ще означаваме с $\mathcal{F}_2^n = \{f \mid f : \{0,1\}^n \to \{0,1\}\}$. Множеството на всички булеви функции ще означаваме с $\mathcal{F}_2 = \bigcup_{n \in \mathbb{N}} \mathcal{F}_2^n$. Така $|\mathcal{F}_2^n| = 2^{2^n}$.

Да разгледаме няколко примера. Булевите функции на един аргумент са описани в следната таблица:

x	g_1	g_2	g_3	g_4
0	0	0	1	1
1	0	1	0	1

Функцията $g_1(x) = o(x)$ наричаме константа нула. Функцията $g_4(x) = 1(x)$ наричаме константа единица. Функцията $g_2(x) = I_1^1(x) = x$ наричаме идентитет. Функцията $g_3(x) = \overline{x}$ наричаме константа отрицание.

При $n = 2$ функциите вече са $2^{2^2} = 16$:

x	y	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

В края на таблицата имаме отново двете константи, но те сега са вече функции на два аргумента. Функция, която прилича на идентитета също се появява два пъти $f_4(x, y) = x$ и $f_6(x, y) = y$. Сега обаче не е уместно да говорим за идентитет, защото аргументите са два и трябва да уточним допълнително, стойността на кой от двата аргумента връщаме като резултат. Затова тук по-правилно е да говорим за проектиращи функции: $f_4(x, y) = I_1^2(x, y)$, $f_6(x, y) = I_2^2(x, y)$. Проектиращите функции могат да се дефинират за произволен брой аргументи. Те ще играят съществена роля в нашите разглеждания.

Определение 5.3. Нека $1 \leq k \leq n$. Функцията $I_k^n : \{0, 1\}^n \to \{0, 1\}$, дефинираме чрез:

$$I_k^n(x_1, \dots x_n) = x_k.$$

Имаме и две представяния на отрицанието: $f_{13}(x, y) = \overline{x}$, $f_{11}(x, y) = \overline{y}$.

Други основни функции получаваме като направим аналогия с основните логическите връзки, като считаме, че 0 представя лъжа, а 1 - истина. Така $f_2(x, y) = x.y$ е конюнкцията на x и y, $f_8(x, y) = x \vee y$ е дизюнкцията на x и y, $f_{10}(x, y) = x \leftrightarrow y$ е еквиваленцията между x и y, $f_{14}(x, y) = x \to y$ е импликацията от x към y. Нови функции, които също ще означим със специални символи са: $f_7(x, y) = x \oplus y$, събиране по модул две; $f_9(x, y) = f \downarrow y$, стрелката на Пийрс, $f_{15}(x, y) = x|y$, чертата на Шефер.

Останалите функции: f_3, f_5, f_{12} нямат собствени имена. Те мога да се изразят чрез останалите с помощта на операцията суперпозиция. Напомняме дефиницията на операция суперпозиция за случая на булевите функции.

Определение 5.4. Нека $n, k \in \mathbb{N}$. Нека $f : \{0, 1\}^n \to \{0, 1\}$ и $g_1 \dots g_n : \{0, 1\}^k \to \{0, 1\}$ са функции. Тогава функцията $h : \{0, 1\}^k \to \{0, 1\}$, дефинирана чрез

$$h(a_1, \dots a_k) = f(g_1(a_1 \dots a_k), \dots g_n(a_1 \dots a_k)),$$

наричаме суперпозиция на f с $g_1, \dots g_n$.

Така $f_3(x, y) = \overline{x \to y} = g_3(f_{14}(x, y))$, а

$$f_5(x, y) = \overline{y \to x} = g_3(f_{14}(I_2^2(x, y), I_1^2(x, y))).$$

Така получаваме два различни начина за представяне на булеви функции - чрез суперпозиция на някои от основните функции, или чрез описание на всички техни стойности в таблица. Когато $n = 2$ таблицата е сравнително малка и може да се изпише лесно: 4 реда и 3 стълба:

x	y	$f(x, y)$
0	0	$f(0, 0)$
0	1	$f(0, 1)$
1	0	$f(1, 0)$
1	1	$f(1, 1)$

Но с нарастване на аргументите, размера на таблицата нараства експоненциално. При $n = 3$ таблицата вече е с 8 реда и 4 стълба:

x	y	z	$f(x,y,z)$
0	0	0	$f(0,0,0)$
0	0	1	$f(0,0,1)$
0	1	0	$f(0,1,0)$
0	1	1	$f(0,1,1)$
1	0	0	$f(1,0,0)$
1	0	1	$f(1,0,1)$
1	1	0	$f(1,1,0)$
1	1	1	$f(1,1,1)$

При това първите три стълба на всяка таблица, представяща булева функция с три аргумента, са едни и същи. За да опишем една такава функция, ако отнапред сме се разбрали в какъв ред описваме възможните стойности на аргументите достатъчно е да знаем как се попълва само четвъртия стълб:

$$(f(0,0,0), f(0,0,1), f(0,1,0), f(0,1,1), f(1,0,0), f(1,0,1), f(1,1,0), f(1,1,1)).$$

Затова ще въведем стандартна наредба на булевите вектори:

Определение 5.5. Стандартната наредба на едномерните булеви вектори е: $0, 1$.

Нека $\alpha_1, \alpha_2 \dots \alpha_{2^n}$ е стандартната наредба на n-мерните булеви вектори. Стандартната наредба на $n+1$-мерните булеви вектори е:

$$0\alpha_1, 0\alpha_2 \dots 0\alpha_{2^n}, 1\alpha_1, 1\alpha_2 \dots 1\alpha_{2^n}.$$

Забележка! Стандартната наредба на n-мерните булеви вектори отговаря на стандартната наредба на естествените числа представени в двоичен запис с n цифри и водещи нули.

Така една n-местна булева функция f може да се зададе чрез своя вектор от стойности:

$$(f(\alpha_1), f(\alpha_2) \dots f(\alpha_{2^n})).$$

Например функцията $f(x,y,z) = (01101011)$ е функцията със следната таблица:

x	y	z	$f(x,y,z)$
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	1

Една функция може да има много различни представяния с помощта на суперпозиции на други функции. Например

$$x \downarrow y = \overline{x \vee y} = \overline{x}.\overline{y}.$$

Следващата теорема описва по-важните такива връзки:

Теорема 5.6. В сила са следните равенства:

1. Константи: $x \vee 1 = x \to 1 = 0 \to x = x \vee \overline{x} = 1$,$x \wedge 0 == x\overline{x} = 0$, $x \vee 0 = x.1 = 1 \leftrightarrow x = x \oplus 0 = x$, $x \to 0 = x \leftrightarrow 0 = x \oplus 1 = \overline{x}$.
2. Комутативност: $xy = yx$, $x \vee y = y \vee x$, $x \oplus y = y \oplus x$, $x \leftrightarrow y = y \leftrightarrow x$
3. Асоциативност: $(xy)z = x(yz)$, $(x \vee y) \vee z = x \vee (y \vee z)$, $(x \oplus y) \oplus z = x \oplus (y \oplus z)$.
4. Отрицание: $\overline{\overline{x}} = x$, $\overline{xy} = \overline{x} \vee \overline{y}$, $\overline{x \vee y} = \overline{x}\overline{y}$.
5. Дистрибутивност: $x(y \vee z) = xy \vee xz$, $x(y \oplus z) = xy \oplus xz$, $x \vee yz = (x \vee y)(x \vee z)$.
6. Поглъщане: $x.x = x$, $x \vee x = x$, $x \oplus x = 0$, $x(x \vee y) = x \vee xy = x$.
7. Представяне чрез $\{., \vee, \bar{}\}$: $x \to y = \overline{x} \vee y$, $\overline{x \to y} = x\overline{y}$, $x \leftrightarrow y = xy \vee \overline{x}\overline{y}$, $x \oplus y = x\overline{y} \vee \overline{x}y$, $x|y = \overline{xy} = \overline{x} \vee \overline{y}$, $x \downarrow y = \overline{x \vee y} = \overline{x}\overline{y}$.
8. Представяне чрез $\{., \oplus, 1\}$: $x \vee y = xy \oplus x \oplus y$,$\overline{x} = x \oplus 1$, $x \to y = xy \oplus x \oplus 1$, $x \leftrightarrow y = x \oplus y \oplus 1$, $x|y = xy \oplus 1$, $x \downarrow y = xy \oplus x \oplus y \oplus 1$.

Доказателство. Всяко от тези равенства може да се докаже чрез директна проверка. Например равенството $x \to y = x.y \oplus x \oplus 1$ се доказва чрез следната проверка:

x	y	$x \to y$	$xy \oplus (x \oplus 1)$
0	0	1	$0.0 \oplus (0 \oplus 1) = 0 \oplus 1 = 1$
0	1	1	$0.1 \oplus (0 \oplus 1) = 0 \oplus 1 = 1$
1	0	0	$0.1 \oplus (1 \oplus 1) = 0 \oplus 0 = 0$
1	1	1	$1.1 \oplus (1 \oplus 1) = 1 \oplus 0 = 1$

$\square$

5.2 Пълни множества булеви функции

Определение 5.7. Нека $F \subseteq \mathcal{F}^2$ е множество от булеви функции. С индукция дефинираме следната редица.
$F_0 = F \cup \{I_k^n \mid 1 \leq k \leq n\}$. За всяко $n \geq 0$,

$$F_{n+1} = F_n \cup \{h \mid \exists f, g_1 \dots g_n \in F_n(h(x_1 \dots x_k) = f(g_1(x_1 \dots a_k), \dots g_n(x_1 \dots x_k)))\}$$

Затварянето на F по отношение на суперпозиция наричаме множеството:

$$[F] = \bigcup_{n \in \mathbb{N}} F_n.$$

Така множеството $[F]$ се задава с индукция от базово множество $F \cup \{I_k^n \mid 1 \leq k \leq n\}$ по правилото суперпозиция. От Тема 1, знаем, че това е най-малкото множество X, което съдържа базовото множество и е затворено относно суперпозиция.

Определение 5.8. Нека $F \subseteq \mathcal{F}^2$ е множество от булеви функции. F е пълно множество или базис, ако $[F] = \mathcal{F}^2$.

Като пример за пълно множество ще докажем теоремата на Бул, която доказва, че множеството $\{f_1(x,y) = x.y, f_2(x,y) = x \vee y, f_3(x) = \overline{x}\}$ е пълно. За целта ще въведем специално означение.

Определение 5.9. Нека $a \in \{0,1\}$. С x^a означаваме x, ако $a = 1$ и $\overline{x}$, ако $a = 0$. Функция от вида

$$f(x_1, x_2 \dots x_n) = x_1^{a_1}.x_2^{a_2} \dots x_n^{a_n},$$

където $a_i \in \{0,1\}$, за $i = 1 \dots n$, наричаме пълна елементарна конюнкция.

Забележка! Функция от вида

$$f(x_1, x_2 \dots x_n) = x_{i_1}^{a_1}.x_2^{a_2} \dots x_{i_k}^{a_k},$$

където $a_i \in \{0,1\}$, за $i = 1 \dots k$, наричаме елементарна конюнкция. Функцията от дефиницията е пълна, защото в нея участват всички променливи.

Пълната елементарна конюнкция е полезна функция, защото тя има стойност 1 само в един единствен случай:

Лема 5.10. Нека $f(x_1, x_2 \dots x_n) = x_1^{a_1}.x_2^{a_2} \dots x_n^{a_n}$, където $a_i \in \{0,1\}$, за $i = 1 \dots n$.

1. $f(x_1, \dots x_n) \in [F]$, където $F = \{f_1(x,y) = x.y, f_2(x,y) = x \vee y, f_3(x) = \overline{x}\}$
2. Нека $(b_1 \dots b_n) \in \{0,1\}^n$. Тогава:

$$f(b_1 \dots b_n) = 1 \Leftrightarrow b_1 = a_1 \ \&\ b_2 = a_2 \ \&\ b_n = a_n.$$

Доказателство. Ще докажем и двете твърдения с индукция по n. Ако $n = 1$ твърдението следва директно от дефиницията на $x_1^{a_1}$. Ако $a_1 = 1$, то $f(x_1) = x_1 = I_1^1(x) \in [F]$ и $f(b_1) = 1 \Leftrightarrow b_1 = 1$. Ако $a_1 = 0$, то $f(x_1) = \overline{x}_1 \in [F]$ и $f(b_1) = 1 \Leftrightarrow b_1 = 0$.

Нека твърдението е в сила за n. Нека $f(x_1 \dots x_n, x_{n+1}) = x_1^{a_1}.x_2^{a_2} \dots x_n^{a_n}.x_{n+1}^{a_{n+1}}$. Тогава $f(x_1 \dots x_n, x_{n+1}) =$

$$(x_1^{a_1}.x_2^{a_2} \dots x_n^{a_n}).x_{n+1}^{a_{n+1}}$$

е суперпозиция на $f_1 \in F$, конюнкцията, с

$$g(x_1 \dots x_n) = x_1^{a_1}.x_2^{a_2} \dots x_n^{a_n}$$

елементарна конюнкция с дължина n, разширена до функция на $n+1$ променливи чрез добавяне на една фиктивна променлива (виж забележката по-горе) и проектиращата функция $I_{n+1}^{n+1}(x_1 \dots x_n) \in [F]$. Съгласно индукционното предположение $g \in [F]$, следователно $f \in [F]$.

Нека $(b_1 \dots b_n, b_{n+1}) \in \{0,1\}^{n+1}$.

Представяме $f(b_1, \dots b_{n+1})$ като

$$f(b_1 \dots b_n, b_{n+1}) = (b_1^{a_1}.b_2^{a_2} \dots b_n^{a_n}).b_{n+1}^{a_{n+1}}.$$

Съгласно дефиницията на функцията конюнкция,

$$(b_1^{a_1}.b_2^{a_2} \dots b_n^{a_n}).b_{n+1}^{a_{n+1}} = 1 \Leftrightarrow b_1^{a_1}.b_2^{a_2} \dots b_n^{a_n} = 1 \ \&\ b_{n+1}^{a_{n+1}} = 1.$$

Съгласно индукционното предложение

$$b_1^{a_1}.b_2^{a_2}\dots b_n^{a_n} = 1 \Leftrightarrow b_1 = a_1 \ \& \ b_2 = a_2 \ \& \ b_n = a_n.$$

Съгласно базовия случай

$$b_{n+1}^{a_{n+1}} = 1 \Leftrightarrow b_{n+1} = a_{n+1}.$$

□

Сега сме готови да докажем теоремата на Бул.

Теорема 5.11 (Теорема на Бул)**.** Множеството

$$F = \{f_1(x,y) = x.y, f_2(x,y) = x \vee y, f_3(x) = \overline{x}\}$$

е пълно.

Доказателство. Нека $f \in \mathcal{F}_2^n$. Ако $f(x_1\dots x_n) = \mathbf{0}$, константата нула, то $f(x_1\dots x_n) = x_1.\overline{x}_1 = f_1(I_1^n(x_1\dots x_n), I_1^n(x_1\dots x_n))$.

Нека f не е константата нула. Разглеждаме следната функция:

$$g(x_1,\dots x_n) = \bigvee_{(a_1\dots a_n)\in\{0,1\}^n \& f(a_1,\dots a_n)=1} x_1^{a_1}.x_2^{a_2}\dots x_n^{a_n}.$$

Така g е дизюнкция от пълни елементарни конюнкции. Ще покажем, че $g \in [F]$ и че $f = g$.

Всяка елементарна конюнкция е от съгласно предишната лема $[F]$.

Така $g(x_1\dots x_n) =$

$$f_2(h_{i_1}(x_1\dots x_n), f_2(h_{i_2}(x_1\dots x_n),\dots, h_{i_k}(x_1\dots x_n))).$$

Където $h_{i_1}\dots h_{i_k}$ са елементарните конюнкции за всеки от векторите $\alpha_i = (a_1,\dots a_n)$, за който $f(\alpha_i) = 1$. Следователно $g \in [F]$.

Сега нека $(b_1\dots b_n) \in \{0,1\}^n$. Ако $f(b_1\dots b_n) = 1$ то съгласно предишната лема $g(b_1\dots b_n) =$

$$\bigvee_{(a_1\dots a_n)\in\{0,1\}^n \& f(a_1,\dots a_n)=1} b_1^{a_1}.b_2^{a_2}\dots b_n^{a_n} = 1.$$

Ако $g(b_1,\dots b_n) = 1$, то поне една от елементарните конюнкции в g има стойност единица, т.е за някой $(a_1,\dots a_n) \in \{0,1\}^n$, за който $f(a_1\dots a_n) = 1$, имаме, че:

$$b_1^{a_1}.b_2^{a_2}\dots b_n^{a_n} = 1.$$

Отново съгласно предишната лема $a_1 = b_1 \ \& \ a_2 = b_2 \ \& \ \dots a_n = b_n$, следователно $f(b_1\dots b_n = 1)$. Така $f = g$ и $f \in [F]$. □

Определение 5.12. Нека $f \in \mathcal{F}_2^n$ и f не е константата нула. Представянето на f във вида:

$$f(x_1,\dots x_n) = \bigvee_{(a_1\dots a_n)\in\{0,1\}^n \& f(a_1,\dots a_n)=1} x_1^{a_1}.x_2^{a_2}\dots x_n^{a_n}$$

наричаме свършена дизюнктивна нормална форма.

Следващата лема ще ни даде възможност да дадем много други примери за базиси:

Твърдение 5.13. Нека $F, G \subseteq \mathcal{F}_2$ са такива, че $F \subseteq [G]$. Тогава $[F] \subseteq [G]$.

Доказателство. Нека $[F] = \bigcup_{n \in \mathbb{N}} F_n$, където $F_0 = F \cup \{I_k^n \mid 1 \leq k \leq n\}$ и

$F_{n+1} = F_n \cup \{h \mid \exists f, g_1 \dots g_k \in F_n(h(x_1 \dots x_n) = f(g_1(x_1 \dots x_n), \dots g_k(x_1 \dots x_n)))\}$.

Нека $[G] = \bigcup_{n \in \mathbb{N}} G_n$, където $G_0 = G \cup \{I_k^n \mid 1 \leq k \leq n\}$ и

$G_{n+1} = G_n \cup \{h \mid \exists f, g_1 \dots g_k \in G_n(h(x_1 \dots x_n) = f(g_1(x_1 \dots x_n), \dots g_k(x_1 \dots x_n)))\}$.

Ще докажем, че за всяко n $F_n \subseteq [G]$.

$F \subseteq [G]$ по условие. $\{I_k^n \mid 1 \leq k \leq n\} \in G_0 \subseteq [G]$. Следователно $F_0 \subseteq [G]$. Нека $F_n \subseteq [G]$. Нека $h(x_1 \dots x_n) = f(g_1(x_1 \dots x_n), \dots g_k(x_1 \dots x_n))$, където $f, g_1 \dots g_k \in F_n$. Съгласно индукционното предположение $f \in [G] = \bigcup_{n \in \mathbb{N}} G_n$. Следователно съществува m_0 такова, че $f \in G_{m_0}$. Аналогично $g_1 \dots g_k \in [G]$, следователно съществуват $m_1, \dots m_k$, такива че $g_i \in G_{m_i}$, за $i = 1 \dots k$. Нека $m = \max(m_0, m_1 \dots m_k)$. Тогава $f, g_1 \dots g_k \in G_m$ и $h \in G_{m+1}$. Следователно $h \in [G]$ и следователно $F_{n+1} \subseteq [G]$. $\square$

Като следствие от това твърдение и теоремата на Бул получаваме, че следните множества са пълни:

1. $\{x.y, \overline{x}\}$ е пълно, защото $x \vee y = \overline{\overline{x}.\overline{y}}$.

2. $\{x \oplus y, x.y, \mathbf{1}\}$ е пълно, защото $\overline{x} = x \oplus 1$ и $x \vee y = x.y \oplus x \oplus y$.

Вторият пример за пълно множество задава друг вид представяне на булевите функции:

Определение 5.14. Функция от вида:

$$f(x_1 \dots x_n) = a_0 \oplus \bigoplus_{1 \leq i \leq n} a_i x_i \oplus \bigoplus_{1 \leq i < j \leq n} a_{ij} x_i . x_j \oplus \dots \oplus a_{12\dots n} x_1 x_2 \dots x_n,$$

където $a_i \in \{0, 1\}$, наричаме полином на Жегалкин.

Съгласно предишното ни наблюдение всяка функция може да се представи чрез полином на Жегалкин, защото множеството $\{x \oplus y, x.y, \mathbf{1}\}$ е пълно.

Например полиномите на Жегалкин за основните ни функции са:

$\mathbf{0}$	0
$\mathbf{1}$	1
x	x
x	$x \oplus 1$
$x.y$	$x.y$
$x \vee y$	$x.y \oplus x \oplus y$
$x \to y$	$x.y \oplus x \oplus 1$
$x \leftrightarrow y$	$x \oplus y \oplus 1$
$x \oplus y$	$x \oplus y$
$x \mid y$	$x.y \oplus 1$
$x \downarrow y$	$x.y \oplus x \oplus y \oplus 1$

В общия случай, полином на Жегалкин за функция на две променливи има следният вид:

$$f(x, y) = a_0 \oplus a_1x_1 \oplus a_2x_2 \oplus a_{12}x_1x_2.$$

Възможните различни полиноми получаваме от различните възможни стойности за параметрите $(a_0, a_1, a_2, a_{1,2}) \in \{0, 1\}^4$. Така различните полином на Жегалкин са 2^4, точно толкова, колкото са булевите функции на 2 аргумента. От тук следва, че всяка функция на две променливи има единствен полином на Жегалкин.

Това разсъждение може да се обобщи за всяка функция:

Теорема 5.15 (Теорема на Жегалкин)**.** Всяка булева функция може да се представи по единствен начин във вида:

$$f(x_1 \dots x_n) = a_0 \oplus \bigoplus_{1\leq i\leq n} a_ix_i \oplus \bigoplus_{1\leq i<j\leq n} a_{ij}x_ix_j \oplus \dots \oplus a_{12\dots n}x_1x_2 \dots x_n.$$

където $a_i \in \{0, 1\}$.

Доказателство. Вече видяхме, че всяка функция има такова представяне, затова достатъчно е да докажем, че то е единствено.

I Начин (Комбинаторно доказателство): Нека разгледаме общия вид на полином на Жегалкин на n променливи:

$$a_0 \oplus \bigoplus_{1\leq i\leq n} a_ix_i \oplus \bigoplus_{1\leq i<j\leq n} a_{ij}x_ix_j \oplus \dots \oplus a_{12\dots n}x_1x_2 \dots x_n$$

Различните функции на n аргумента имат различни представяния чрез полином на Жегалкин. Различните полиноми на Жегалкин се получават от различните стойности на коефициентите. Броят на коефициентите е: 1 - свободен член, n - коефициента пред линейните събираеми, $\binom{n}{2}$ коефициента, по един за всяка двойка променливи, $\binom{n}{3}$ коефициента, по един за всяка тройка променливи,..., $\binom{n}{k}$ коефициента, по един за всяка k-орка променливи, ..., $\binom{n}{n} = 1$ коефициент, пред $x_1x_2 \dots x_n$. Общо:

$$\sum_{i=0}^{k} \binom{n}{k} = 2^n,$$

съгласно теоремата на Нютон. Всеки коефициент може да има стойност 0 или 1. Общо различните полиноми на Жегалкин са 2^{2^n}, точно толкова колкото са и булевите функции. Следователно всяка булева функция има единствен полином на Жегалкин.

II Начин. Да допуснем, че f има две различни представяния:

$$f(x_1 \dots x_n) = a_0 \oplus \bigoplus_{1\leq i\leq n} a_ix_i \oplus \bigoplus_{1\leq i<j\leq n} a_{ij}x_ix_j \oplus \dots \oplus a_{12\dots n}x_1x_2 \dots x_n =$$

$$= b_0 \oplus \bigoplus_{1\leq i\leq n} b_ix_i \oplus \bigoplus_{1\leq i<j\leq n} b_{ij}x_ix_j \oplus \dots \oplus b_{12\dots n}x_1x_2 \dots x_n$$

Нека $a_{i_1 \dots i_k}$ и $b_{i_1 \dots i_k}$ са първата двойка различни коефициенти. Заместваме в двете представяния с вектора $(c_1 \dots c_n)$, където

$$c_j = \begin{cases} 1, & \text{ако } j \in \{i_1 \dots i_k\}; \\ 0, & \text{ако } j \notin \{i_1 \dots i_k\}. \end{cases}$$

Събираемите до това с индекс $i_1 \dots i_k$ и в двете представяния са еднакви, нека те са с обща стойност C. Всички събираеми след това с индекс $i_1 \dots i_k$ се нулират, защото в тях участва като множител c_j за някое $j \notin \{i_1 \dots i_k\}$. Така $f(c_1 \dots c_n) = C \oplus a_{i_1 \dots i_k} = C \oplus a_{i_1 \dots i_k}$, което противоречи на допускането, че $a_{i_1 \dots i_k} \neq b_{i_1 \dots i_k}$. □

5.3 Затворени множества булеви функции

Определение 5.16. Нека $F \subseteq \mathcal{F}_2$ е множество от булеви функции. F е затворено множество, ако $[F] = F$.

Твърдение 5.17 (Критерий за затвореност)**.** Нека $F \subseteq \mathcal{F}_2$ е множество от булеви функции. F е затворено множество, ако:

1. $\forall n, k \in \mathbb{N}(1 \leq k \leq n \Rightarrow I_k^n \in F)$.
2. $\forall f, g_1 \dots g_k \in F(h(x_1 \dots x_n) = f(g_1(x_1 \dots x_n), \dots g_k(x_1 \dots x_n)) \in F))$.

Доказателство. Ще докажем, че за всяко n, $F_n \subseteq F$, където $[F] = \bigcup F_n$. $F_0 = F \cup \{I_k^n \mid 1 \leq k \leq n\} \subseteq F$ от първата точка в условието. Нека допуснем, че $F_n \subseteq F$. Тогава $F_{n+1} = F_n \cup \{h \mid \exists f, g_1 \dots g_k \in F(h(x_1 \dots x_n) = f(g_1(x_1 \dots x_n), \dots g_k(x_1 \dots x_n)))\} \subseteq F$ от индукционното предположение и втората точка от условието. □

5.3.1 Булеви функции запазващи константите

Определение 5.18. Нека $f \in \mathcal{F}_2^n$ и $\alpha_1, \dots \alpha_{2^n}$ е стандартната подредба на булевите вектори. Казваме, че f запазва константата нула, ако $f(\alpha_1) = f(0, 0, \dots 0) = 0$. Множеството на всички булеви функции, които запазват нулата означаваме с T_0.

Казваме, че f запазва константата единица, ако $f(\alpha_{2^n}) = f(1, 1, \dots 1) = 1$. Множеството на всички булеви функции, които запазват единицата означаваме с T_1.

Например $x.y, x \vee y \in T_0 \cap T_1$ $x \oplus y \in T_0 \backslash T_1$, $x \leftrightarrow y \in T_1 \backslash T_0$, $x|y, x \downarrow \notin T_0 \cup T_1$.

Твърдение 5.19. T_0 и T_1 са затворени множества.

Доказателство. Ще използваме критерий за затвореност. Нека $k \leq n$. $I_k^n(\alpha_1) = I_k^n(0, 0 \dots 0) = 0$, следователно $I_k^n \in T_0$. Нека $f, g_1 \dots g_k \in T_0$ и нека $h(x_1 \dots x_n) = f(g_1(x_1 \dots x_n), \dots g_k(x_1 \dots x_n))$. Тогава $h(\alpha_1) = h(0, 0, \dots 0) = f(g_1(0 \dots 0), \dots g_k(0 \dots 0)) = f(0, 0, \dots 0) = 0$. Така $h \in T_0$ и $_0$ е затворено. Аналогично се проверява, че и T_1 е затворено. □

5.3.2 Самодвойнствени булеви функции

Определение 5.20. Нека $f \in \mathcal{F}_2^n$. Двойнствена на f наричаме функцията:

$$f^*(x_1 \dots x_n) = \overline{f}(\overline{x}_1, \dots \overline{x}_n).$$

В следващата таблица са изброени някои основни примери за двойки функция и нейната двойнствена.

f	f^*
$\mathbf{0}$	$\mathbf{1}$
$\mathbf{1}$	$\mathbf{0}$
x	x
$\overline{x}$	$\overline{x}$
$x.y$	$x \vee y$
$x \vee y$	$x.y$
$x \oplus y$	$x \leftrightarrow y$
$x \leftrightarrow y$	$x \oplus y$
$x \vert y$	$x \downarrow y$
$x \downarrow y$	$x \vert y$

Твърдение 5.21. Нека $f \in \mathcal{F}_2^n$. $(f^*)^* = f$

*Доказателство. Доказателство.*Доказателството следва директно от дефиницията:

$$(f^*)^*(x_1 \dots x_n) = \overline{f}^*(\overline{x}_1, \dots \overline{x}_n) = \overline{\overline{f}}(\overline{\overline{x}_1}, \dots \overline{\overline{x}_n}) = f(x_1 \dots x_n).$$

□

Твърдение 5.22 (Принцип за двойнственост)**.** Нека $f \in \mathcal{F}_2^k$ и $g_1 \dots g_k \in \mathcal{F}_2^n$. Нека h е суперпозицията на f и $g_1 \dots g_k$. Тогава

$$h^*(x_1 \dots x_n) = f^*(g_1^*(x_1 \dots x_n) \dots g_k^*(x_1 \dots x_n)).$$

Доказателство. Отново твърдението следва от дефиницията.

$$\begin{gathered} h^*(x_1 \dots x_n) = \overline{f}(g_1(\overline{x}_1 \dots \overline{x}_n) \dots g_k(\overline{x}_1 \dots \overline{x}_n)) = \\ = \overline{f}(\overline{\overline{g}_1(\overline{x}_1 \dots \overline{x}_n)} \dots \overline{\overline{g}_k(\overline{x}_1 \dots \overline{x}_n)}) = \\ = \overline{f}(\overline{g_1^*(x_1 \dots x_n)} \dots \overline{g_k^*(x_1 \dots x_n)}) = f^*(g_1^*(x_1 \dots x_n) \dots g_k^*(x_1 \dots x_n)). \end{gathered}$$

□

Определение 5.23. Нека $f \in \mathcal{F}_2^n$. f наричаме самодвойнствена, ако $f = f^*$. С S означаваме множеството на всички самодвойнствени функции.

Пример за самодвойнствена функция е функцията $m(x, y, z) = x.y \oplus y.z \oplus z.x = x.y \vee y.z \vee z.x$, която се нарича медиана.

Твърдение 5.24. S е затворено множества.

Доказателство. Ще използваме критерий за затвореност. Нека $k \leq n$.

$$(I_k^n(x_1 \dots x_n))^* = \overline{I_k^n}(\overline{x}_1, \dots \overline{x}_n) = \overline{\overline{x_k}} = x_k = I_k^n(x_1 \dots x_n).$$

Следователно $I_k^n \in S$.

Нека $f, g_1 \dots g_k \in S$ и нека $h(x_1 \dots x_n) = f(g_1(x_1 \dots x_n), \dots g_k(x_1 \dots x_n))$. Тогава съгласно принципа за двойнственост:

$$h^*(x_1 \dots x_n) = f^*(g_1^*(x_1 \dots x_n) \dots g_k^*(x_1 \dots x_n)) =$$

$$= f(g_1(x_1 \dots x_n), \dots g_k(x_1 \dots x_n)) = h(x_1 \dots x_n).$$

Така $h \in S$ и S е затворено. □

5.3.3 Линейни булеви функции

Определение 5.25. Нека $f \in \mathcal{F}_2^n$. Казваме, че f е линейна, ако f има линеен полином на Жегалкин. Т.е. f може да се представи като

$$f(x_1 \dots x_n) = a_0 \oplus a_1 x_1 \oplus \dots a_n x_n,$$

където $a_i \in \{0, 1\}$. С L означаваме множеството на всички линейни функции.

Например $x, \overline{x} = x \oplus 1, x \oplus y, x \leftrightarrow y = x \oplus y \oplus 1 \in L$, $x.y, x \vee y = x.y \oplus x \oplus y \notin L$.

Твърдение 5.26. L е затворено множество.

Доказателство. Ще използваме критерий за затвореност. Нека $k \leq n$. $I_k^n(x_1 \dots x_n) = x_k$. Това е линеен полином на Жегалкин ($a_k = 1$ и $a_i = 0$ за $i \neq k$), следователно $I_k^n \in L$.

Нека $f, g_1 \dots g_k \in L$, $f(x_1 \dots x_k) = b_0 \oplus \bigoplus_{j=1}^k b_j x_j$ и $g_j(x_1 \dots x_n) = a_0^j \oplus \bigoplus_{i=1}^n a_i^j x_i$. Тогава

$$h(x_1 \dots x_n) = f(g_1(x_1 \dots x_n), \dots g_k(x_1 \dots x_k)) =$$

$$= b_0 \oplus \bigoplus_{j=1}^{k} b_j (a_0^j \oplus \bigoplus_{i=1}^{n} a_i^j x_i) =$$

$$= (b_0 \oplus \bigoplus_{j=1}^{k} b_j a_0^j) \oplus (\bigoplus_{j=1}^{k} b_j a_1^j) x_1 \oplus \dots (\bigoplus_{j=1}^{k} b_j a_n^j) x_n$$

.

Така $h \in L$ и L е затворено. □

5.3.4 Монотонни булеви функции

За да дефинираме монотонните булеви функции, дефинираме наредба между n-мерните вектори. Обърнете внимание, че наредбата е частична, не е линейна.

Определение 5.27. Нека $\alpha = (a_1, \dots a_n)$ и $\beta = (b_1, \dots b_n)$ са n-мерни булеви вектори.

$$\alpha \leq \beta \Leftrightarrow a_1 \leq b_1 \ \& \ a_2 \leq b_2 \ \& \ \dots a_n \leq b_n.$$

Нека $f \in \mathcal{F}_2^n$. Казваме, че f е монотонна, ако за всяка двойка аргументи $\alpha, \beta \in \{0,1\}^n$

$$\alpha \leq \beta \Rightarrow f(\alpha) \leq f(\beta).$$

С M означаваме множеството на всички монотонни функции.

Например $x, x.y, x \vee y \in M$, а $\overline{x}, x \oplus y, x \leftrightarrow y \notin M$.

Проверката, дали една функция е монотонна, е в общия случай сложна. За да опростим тази проверка в случая на булевите функции, ще докажем едно свойство на наредбата.

Твърдение 5.28. Нека $\alpha, \beta \in \{0,1\}^n$ и $\alpha \leq \beta$, $\alpha \neq \beta$. Тогава съществува верига

$$\alpha = \alpha_1 \leq \alpha_2 \leq \dots \leq \alpha_k = \beta$$

такава, че α_i се различава от α_{i+1} само в една позиция.

Доказателство. Нека $\alpha = (a_1 \dots a_n)$ и $\beta = (b_1 \dots b_n)$ и нека $i_1, \dots i_k$ са позициите, за които $a_{i_j} \neq b_{i_j}$. Тъй като $\alpha \leq \beta$, $a_{i_j} = 1$ и $b_{i_j} = 0$ за $j = 1 \dots k$. Ще докаже твърдението с индукция по броя на разликите, k.

Ако $k = 1$, то твърдението е в сила, веригата е $\alpha = \alpha_1 \leq \alpha_2 = \beta$. Нека твърдението е в сила за вектори с k разлики и нека α и β се различават в $k+1$ точки. Нека i е индексът на първата разлика. Разглеждаме вектора $\gamma = (c_1 \dots c_n)$, където:

$$c_j = \begin{cases} a_j, & \text{ако } j \neq i; \\ b_j, & \text{ако } j = i. \end{cases}$$

Така γ се различава от α само в една позиция, и от β в k позиции (всички, в които се различава и α, с изключение на i-тата). По индукция има верига

$$\gamma = \alpha_1 \leq \alpha_2 \leq \dots \leq \alpha_{k+1} = \beta$$

такава, че α_i се различава от α_{i+1} само в една точка. Така търсената верига е:

$$\alpha \leq \gamma = \alpha_1 \leq \alpha_2 \leq \dots \leq \alpha_{k+1} = \beta.$$

□

С помощта на това свойство получаваме лесен критерий за разпознаване, дали една функция е монотонна.

Лема 5.29. Нека $f \in \mathcal{F}_2^n$ и $f \notin M$. Тогава съществуват вектори $\alpha, \beta \in \{0,1\}^n$ такива, че $\alpha \leq \beta$, α и β се различават в точно една позиция и $f(\alpha) \not\leq f(\beta)$.

Доказателство. Щом $f \notin M$ съществуват α' и β' такива, че $\alpha' \leq \beta'$ и $f(\alpha') \not\leq f(\beta')$. От предишното твърдение следва, че има верига

$$\alpha' = \alpha_1 \leq \alpha_2 \leq \dots \leq \alpha_k = \beta'$$

такава, че α_i се различава от α_{i+1} само в една точка. Нека i е първият индекс такъв, че $f(\alpha_i) \not\leq f(\alpha_{i+1})$. Такъв съществува, защото $f(\alpha_1) \not\leq f(\alpha_k)$. Тогава търсените вектори са $\alpha = \alpha_i$, $\beta = \alpha_{i+1}$. □

Твърдение 5.30. M е затворено множество.

Доказателство. Ще използваме критерий за затвореност. Нека $k \leq n$. $I_k^n(x_1 \dots x_n) = x_k$ е монотонна функция, защото ако $(a_1 \dots a_n) \leq (b_1 \dots b_n)$, то $I_k^n(a_1 \dots a_n) = a_k \leq b_k = I_k^n(b_1 \dots b_n)$. Следователно $I_k^n \in M$.

Нека $f, g_1 \dots g_k \in$ и $(a_1 \dots a_n) \leq (b_1 \dots b_n)$. Тогава $g_i(a_1 \dots a_n) \leq g_i(b_1 \dots b_n)$ и следователно,

$$h(a_1 \dots a_n) = f(g_1(a_1 \dots a_n), \dots g_k(a_1 \dots a_n)) \leq f(g_1(b_1 \dots b_n), \dots g_k(b_1 \dots b_n)) = h(b_1 \dots b_n)$$

Така $h \in M$ и M е затворено. □

5.4 Теорема на Пост-Яблонски

Теорема 5.31. Нека $F \subseteq \mathcal{F}_2^n$. Множеството F е пълно, тогава и само тогава, когато

$$F \not\subseteq T_0 \;\&\; F \not\subseteq T_1 \;\&\; F \not\subseteq S \;\&\; F \not\subseteq M \;\&\; F \not\subseteq L.$$

Доказателство. Нека първо F е пълно. Всяко от множествата T_0, T_1, S, L, M са затворени множества. Нека $K \in \{T_0, T_1, S, L, M\}$, ако допуснем, че $F \subseteq K$, то $\mathcal{F}_2 = [F] \subseteq [K] = K$. Така достатъчно е да посочим функция $f_k \notin K$, за достигнем до противоречие. $\overline{x} \notin T_0 \cup T_1 \cup M$, $x.y \notin S, L$. Така ако F е пълно, то $F \not\subseteq T_0 \;\&\; F \not\subseteq T_1 \;\&\; F \not\subseteq S \;\&\; F \not\subseteq M \;\&\; F \not\subseteq L$.

Нека сега $F \not\subseteq T_0 \;\&\; F \not\subseteq T_1 \;\&\; F \not\subseteq S \;\&\; F \not\subseteq M \;\&\; F \not\subseteq L$. Нека $f_0 \in F \setminus T_0$, $f_1 \in F \setminus T_1$, $f_s \in F \setminus S$, $f_l \in F \setminus L$ и $f_m \in F \setminus M$.

Първо, ще покажем че константите $\mathbf{0}, \mathbf{1} \in [F]$. Да разгледаме функцията $g_0(x) = f_0(x \dots x) = f_0(I_1^1(x), \dots I_1^1(x))$ и $g_1(x) = f_1(x \dots x) = f_1(I_1^1(x), \dots I_1^1(x))$. $f_0 \notin T_0$, следователно $g_0(0) = f_0(0 \dots 0) = 1$. Аналогично $f_1 \notin T_1$, следователно $g_1(1) = f_1(1 \dots 1) = 0$. Имаме следните възможности за стойността на другия аргумент:

1. $g_0(1) = 0$, $g_1(0) = 0$. Тогава $g_0(x) = \overline{x}$, $g_1(x) = \mathbf{0}(x)$ и $g_0(g_1(x)) = \mathbf{1}(x)$.

2. $g_0(1) = 1$, $g_1(0) = 0$. Тогава $g_0(x) = \mathbf{1}(x)$, $g_1(x) = \mathbf{0}(x)$.

3. $g_0(1) = 1$, $g_1(0) = 1$. Тогава $g_0(x) = \mathbf{1}(x)$, $g_1(x) = \overline{x}$ и $g_1(g_0(x)) = \mathbf{0}(x)$.

4. $g_0(1) = 0$, $g_1(0) = 1$. Тогава $g_0(x) = g_1(x) = \overline{x}$. Да разгледаме функцията $f_s \notin S$. За нея има вектор $(a_1 \dots a_n)$ такава, че $f_s(a_1 \dots a_n) \neq f_s^*(a_1 \dots a_n)$. Но $f_s^*(a_1 \dots a_n) = \overline{f_s}(\overline{a}_1 \dots \overline{a}_n)$. Следователно $f_s(a_1 \dots a_n) = f_s(\overline{a}_1 \dots \overline{a}_n)$. Да разгледаме функцията

   $$h(x) = f_s(x^{a_1}, \dots x_n^{a_n}).$$

   Функцията h е суперпозиция на f_s и $h_1 \dots h_n$, където

   $$h_i = \begin{cases} I_1^1(x), & \text{ако } a_i = 1; \\ g_0(x), & \text{ако } a_i = 0. \end{cases}$$

   Така $h \in [F]$ и

   $$h(1) = f_s(a_1 \dots a_n) = f_s(\overline{a}_1 \dots \overline{a}_n) = h(0).$$

   Следователно h е константа. Тогава $g_0(h(x))$ е другата константа.

Така във всеки от случаите доказахме, че $\mathbf{0}, \mathbf{1} \in [F]$.

Втората ни цел е да докажем, че $\overline{x} \in [F]$, като използваме константите. Да разгледаме $f_m \notin M$. От Лема 5.29 следва, че има вектори $(a_1 \dots a_n) \leq (b_1 \dots b_n)$, различаващи се само в една позиция, за които $f_m(a_1 \dots a_n) = 1$ и $f_m(b_1 \dots b_n) = 0$. Нека $a_i \neq b_i$. Да разгледаме суперпозицията на f_m и $h_1 \dots h_n$, където

$$h_j(x) = \begin{cases} a_j, & \text{ако } j \neq i; \\ I_1^1(x), & \text{ако } i = j. \end{cases}$$

Така $h \in [F]$ и $h(0) = 1$, $h(1) = 0$, следователно $h(x) = \overline{x}$.

Накрая ще използваме нелинейната функция, константите и $\overline{x}$, за да покажем, че $x.y \in [F]$. Нека

$$f_l(x_1 \dots x_n) = a_0 \oplus a_1 x_1 \dots a_n x_n \oplus x_{i_1} x_{i_2} \dots x_{i_k} \oplus \dots,$$

където $x_{i_1} x_{i_2} \dots x_{i_k}$ е първият нелинеен елемент от полинома на Жегалкин на f_l. Да разгледаме суперпозицията на f_l с $h_1 \dots h_n$, където:

$$h_j(x_1, x_2) = \begin{cases} I_1^2(x_1, x_2), & \text{ако } j = i_1; \\ I_2^2(x_1, x_2), & \text{ако } j = i_2; \\ \mathbf{1}(I_1^2(x_1, x_2)), & \text{ако } j \in \{i_3 \dots i_k\}; \\ \mathbf{0}(I_1^2(x_1, x_2), & \text{ако } j \notin \{i_1 \dots i_k\}. \end{cases}$$

Така $h \in [F]$ и $h(x, y) = c_0 \oplus c_1 x \oplus c_2 y \oplus x.y$. Ако $c_0 = 1$, $\overline{h(x, y)} = h(x, y) \oplus 1 = c_1 x \oplus c_2 x \oplus x.y$. Така БОО можем да предположим, че $c_0 = 0$. Имаме следните възможности за c_1 и c_2:

1. $c_1 = 0$, $c_2 = 0$, тогава $h(x, y) = x.y$.

2. $c_1 = 1$, $c_2 = 0$, тогава $h(x, \overline{y}) = x \oplus x.(y \oplus 1) = x.y$.

3. $c_1 = 0$, $c_2 = 1$, тогава $h(\overline{x}, y) = y \oplus (x \oplus 1).y = x.y$.

4. $c_1 = 1$, $c_2 = 1$, тогава $\overline{h(\overline{x}, \overline{y})} = x \oplus y \oplus (x \oplus 1).(y \oplus 1) \oplus 1 = x.y$.

Така във всеки от случаите $x.y \in [F]$. От теоремата на Бул следва, че $\mathcal{F}_2 = [\{\overline{x}, x.y\}] \subseteq [F]$ и следователно $[F]$ е пълно множество.

□

Определение 5.32. Една функция $f \in \mathcal{F}_2$ наричаме Шеферова, ако $\{f\}$ е пълно множество.

Пример за Шеферова функция е чертата на Шефер $x|y$. Наистина, $x|y \notin T_0$, $x|y \notin T_1$, $x|y \notin S$, $x|y \notin M$, $x|y \notin L$, така от теоремата на Пост-Яблонски следва, че $\{x|y\}$ е пълно.

Твърдение 5.33. Нека $f \in \mathcal{F}_2^n$. f е Шеферова тогава и само тогава, когато $f \notin T_0 \cup T_1 \cup S$.

Доказателство. Едната посока следва от теоремата на Пост-Яблонски. Нека $f \notin T_0 \cup T_1 \cup S$. Тогава $f(0, \dots 0) = 1$, $f(1, \dots 1) = 0$, и тъй като $(0 \dots 0) \leq (1 \dots 1)$, $f \notin M$.

Нека допуснем, че $f \in L$. Тогава $f(x_1 \dots x_n) = a_0 \oplus a_1x_1 \oplus \dots \oplus a_nx_n$. $f(0 \dots 0) = 1$, следователно $a_0 = 1$. $f(1, \dots 1) = 0$, следователно $a_0 \oplus a_1 \oplus \dots \oplus a_n = 0$. Но тогава

$$f^*(x_1 \dots x_n) = \overline{f}(\overline{x}_1, \dots \overline{x}_n) = 1 \oplus a_0 \oplus a_1(x_1 \oplus 1) \oplus \dots \oplus a_n(x_n \oplus 1) =$$

$$= 1 \oplus a_0 \oplus a_1 \oplus a_n \oplus a_1x_1 \oplus \dots \oplus a_nx_n = 1 \oplus a_1x_1 \oplus \dots \oplus a_nx_n = f(x_1 \dots x_n),$$

което противоречи на $f \notin S$.

Така $f \notin L$ и от теоремата на Пост-Яблонски следва, че f е Шеферова.

□

5.5 Задачи за упражнение

Задача 1. Колко са n-местните булеви функции?

Задача 2. Представете всяка от следните функции с помощта на таблица:

1. $(x \to y) \to y$
2. $(x \to y)(y \to x)$
3. $x \oplus 1$
4. $xy \oplus x \oplus 1$
5. $xy \oplus x \oplus y$
6. $xy \vee \overline{xy}$
7. $x\overline{y} \vee \overline{x}y$
8. $\overline{x \to y}$

Задача 3. Напишете вектора от стойности за всяка от следните функции:

1. $(x \to y) \oplus ((y \to \overline{z}) \to xy)$
2. $\overline{(x \leftrightarrow y) \to (\overline{xz} \to y)} \to \overline{x}z$
3. $((x \to y) \oplus (x \to yz))|(x \downarrow y)$
4. $((x \downarrow y)|z) \downarrow y$

Задача 4. Докажете следните равенства.

1. Константи: $x \vee 1 = x \to 1 = 0 \to x = x \vee \overline{x} = 1$,$x \wedge 0 == x\overline{x} = 0$, $x \vee 0 = x.1 = 1 \leftrightarrow x = x \oplus 0 = x$, $x \to 0 = x \leftrightarrow 0 = x \oplus 1 = \overline{x}$.
2. Комутативност: $xy = yx$, $x \vee y = y \vee x$, $x \oplus y = y \oplus x$, $x \leftrightarrow y = y \leftrightarrow x$
3. Асоциативност: $(xy)z = x(yz)$, $(x \vee y) \vee z = x \vee (y \vee z)$, $(x \oplus y) \oplus z = x \oplus (y \oplus z)$.

4. Отрицание: $\overline{\overline{x}} = x$, $\overline{xy} = \overline{x} \vee \overline{y}$, $\overline{x \vee y} = \overline{x}\overline{y}$.
5. Дистрибутивност: $x(y \vee z) = xy \vee xz$, $x(y \oplus z) = xy \oplus xz$, $x \vee yz = (x \vee y)(x \vee z)$.
6. Поглъщане: $x(x \vee y) = x \vee xy = x$.
7. Представяне чрез $\{., \vee, \bar{}\}$: $x \to y = \overline{x} \vee y$, $\overline{x \to y} = x\overline{y}$, $x \leftrightarrow y = xy \vee \overline{x}\overline{y}$, $x \oplus y = x\overline{y} \vee \overline{x}y$, $x|y = \overline{xy} = \overline{x} \vee \overline{y}$, $x \downarrow y = \overline{x \vee y} = \overline{x}\overline{y}$.
8. Представяне чрез $\{., \oplus, 1\}$: $x \vee y = xy \oplus x \oplus y$,$\overline{x} = x \oplus 1$, $x \to y = xy \oplus x \oplus 1$, $x \leftrightarrow y = x \oplus y \oplus 1$, $x|y = xy \oplus 1$, $x \downarrow y = xy \oplus x \oplus y \oplus 1$.

Задача 5. Проверете дали $f = g$, където:

1. $f = (x \vee \overline{y}) \downarrow (\overline{x} \to (y \to z))$, $g = \overline{y \to (x \vee z)}$;
2. $f = (x \to y) \oplus ((y \to \overline{z}) \to xy)$, $g = \overline{yz \to x}$;
3. $f = (x \vee \overline{y}) \downarrow (\overline{x} \to (y \to z))$, $g = \overline{y \to (x \vee z)}$;
4. $f = \overline{(x \downarrow y) \vee (x \leftrightarrow z)}|(x \oplus yz)$, $g = \overline{x}(yz) \vee \overline{x \to z}$
5. $f = ((x \vee y)\overline{z} \to ((x \leftrightarrow \overline{z}) \oplus \overline{y}))((x \oplus y)\overline{z})$, $g = (x \to yz)\overline{x \to y}$;
6. $f = (\overline{x} \vee y) \to ((y|\overline{z}) \to (x \leftrightarrow xz))$, $g = xy \vee (\overline{x \to x\overline{y}} \to z)$;
7. $f = (\overline{x} \to y) \to (\overline{x}y \leftrightarrow (x \oplus y))$, $g = (\overline{xy} \to x) \to y$;
8. $f = (xy \vee (\overline{x} \to yz)) \leftrightarrow ((\overline{x} \to \overline{y}) \to z)$, $g = (x \to y) \oplus (y \oplus z)$.

Задача 6. Намерете съвършена дизюнктивна нормална форма на:

1. $f(x_1, x_2, x_3) = (x_1 \vee x_2) \to x_3$;
2. $f(x_1, x_2, x_3) = (x_1 \to x_2) \oplus (x_1|x_2x_3)$;
3. $f(x_1, x_2) = (0010)$
4. $f(x_1, x_2, x_3) = (10100010)$;
5. $f(x_1, x_2, x_3) = (10101111)$;
6. $f(x_1, x_2, x_3) = (00001111)$;
7. $f(x_1, x_2, x_3, x_4) = (x_1 \to x_2x_3x_4)(x_3 \to x_1x_2)$;
8. $f(x_1, x_2, x_3, x_4) = (1001000110000101)$;

Задача 7. Намерете полинома на Жегалкин на:

1. $f(x_1, x_2, x_3) = (x_1 \vee x_2) \to x_3$;
2. $f(x_1, x_2, x_3) = (x_1 \to x_2) \oplus (x_1|x_2x_3)$;
3. $f(x_1, x_2) = (0010)$

4. $f(x_1, x_2, x_3) = (10100010)$;
5. $f(x_1, x_2, x_3) = (10101111)$;
6. $f(x_1, x_2, x_3) = (00001111)$;
7. $f(x_1, x_2, x_3, x_4) = (x_1 \to x_2x_3x_4)(x_3 \to x_1x_2)$;
8. $f(x_1, x_2, x_3, x_4) = (1001000110000101)$;

Задача 8. Проверете дали f е двойнствена на g:

1. $f(x, y) = x \to y$, $g(x, y) = \overline{x}y$;
2. $f(x, y) = (\overline{x} \to \overline{y}) \to (y \to x)$, $g(x, y) = (x \to y)(\overline{y} \to \overline{x})$;
3. $f(x, y, z) = x \oplus y \oplus z$, $g(x, y, z) = x \oplus y \oplus z$;
4. $f(x, y, z) = xy \vee z$, $g(x, y, z) = x(y \vee z)$
5. $f(x, y, z) = xy \oplus xz \oplus yz$,$g(x, y, z) = xy \vee xz \vee yz$;
6. $f(x, y, z) = xy \to z$, $g = \overline{xy}z$;
7. $f(x, y, z, t) = (x \vee y \vee z)t \vee xyz$,$g(x, y, z, t) = (x \vee y \vee z)t \vee xyz$;
8. $f(x, y, z, t) = (x \to y)(z \to t)$, $g(x, y, z, t) = (x \to \overline{z})(x \to t)(\overline{y} \to \overline{z})(\overline{y} \to t)$.

Задача 9. Намерете полинома на Жегалкин на f^* ако:

1. $f = (10101010)$
2. $f = (111001111)$
3. $f = (1011011101111111)$

Задача 10. Намерете броя на n-местните булеви функции, които са от

1. T_0, T_1;
2. $_0 \setminus T_1$
3. $T_0 \cup T_1$

Задача 11. Проверете дали $f \in T_0, T_1$:

1. $f = x_1 \oplus x_2 \oplus \ldots x_n$;
2. $1 \oplus (x_1 \to x_2)(x_2 \to x_3) \ldots (x_n \to x_1)$;
3. $f = \bigoplus_{1 \leq i < j \leq n} x_i \vee x_j$;

Задача 10. Намерете броя на n-местните булеви функции, които са от

1. S;
2. $_0 \cap S$
3. $T_0 \cap T_1 \cap S$
4. $(T_0 \setminus T_1) \cap S$

Задача 11. Самодвойнствени ли са следните функции:

1. $xy \vee yz \vee zx$;
2. $x_1x_2 \oplus x_2x_3 \oplus x_3x_1 \oplus x_2 \oplus x_3$
3. $(x_1 \to x_2) \oplus (x_2 \to x_3) \oplus (x_3 \to x_1) \oplus x_3$;
4. $x_1x_2 \oplus x_3(x_1 \vee x_2)$
5. (1110011100011000);

Задача 12. Линейни ли са следните функции:

1. $x\overline{y}(x \leftrightarrow y)$;
2. $xy\overline{z} \vee x\overline{z}$;
3. $xyz \oplus x(\overline{yz}) \oplus x(y \vee z)$;
4. (11100011)
5. $xy \oplus yz \oplus xz \oplus \overline{xyz} \oplus xyz$.

Задача 13. Намерете броя на n-местните булеви функции, които са от

1. L
2. $L \cap T_0$
3. $L \cap T_1$
4. $L \cap S$

Задача 14. Монотонни ли са следните функции:

1. $(x_1 \oplus x_2) \wedge (x_1 \leftrightarrow x_2)$;
2. $x_1(x_2 \vee x_2)$;
3. (00011101)
4. (0001110111111111)
5. $x_1x_2 \oplus x_3(x_1 \vee x_2)$
6. $(x_1 \to x_2) \oplus (x_2 \to x_3) \oplus (x_3 \to x_1) \oplus x_3$;

Задача 15. Намерете броя на n-местните булеви функции, които са от

1. $M \setminus T_0$
2. $M \setminus T_1$
3. $M \setminus (T_0 \cup T_1)$

Задача 16. Определете дали следните множества функции са пълни и определете всички техни базиси.

1. $F = \{xy, x \vee y, x \oplus y, xy \vee yz \vee zx\}$
2. $F = \{xy, x \vee y, x \oplus y \oplus z \oplus 1\}$
3. $F = \{xy(x \oplus y), xy \oplus x \oplus y, 1, xy \oplus yz \oplus xz\}$
4. $F = \{\overline{x}, 1, x(y \leftrightarrow z) \oplus \overline{x}(y \oplus z), x \oplus y \oplus z\}$
5. $F = \{f_1 = (11), f_2 = (0110), f_3 = (00110111)\}$
6. $F = \{x \to y, x \oplus y\}$
7. $F = \{x|y\}$
8. $F = \{f_1 = (10000001), f_2 = (0110), f_3 = (01101001)\}$
9. $F = \{xy \oplus z, x \oplus y \oplus 1, x\overline{y}, \overline{x}\}$
10. $F = \{xy, xy \vee z, x \oplus y \oplus z, x \to y, x \leftrightarrow y\}$.

Глава 6

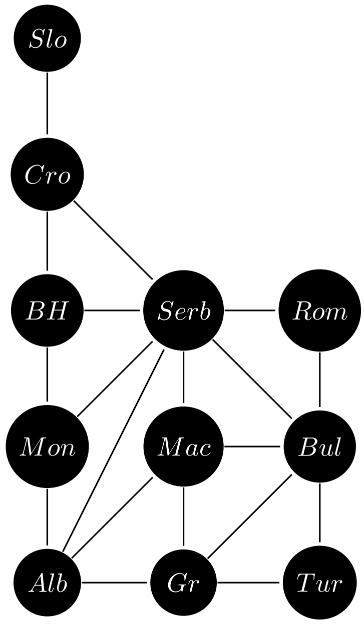
Графи и алгоритми за графи

6.1 Основни дефиниции

Дадена е карта на балканския полуостров.

Какъв минимален брой цветове трябва да се използват, за да няма две съседни страни, оцветени с един и същи цвят? Може ли да се намери маршрут така, че да минем през всяка страна точно по веднъж? Може ли да се намери маршрут, който стартира в България и прекосява всички граници точно по веднъж, като завършва отново в България? Всеки от тези въпроси е свързан с понятието граф и с алгоритми свързани с него.

Преди всичко, за да отговорим на някой от въпросите, не ни е необходима пълната информация, която се задава с помощта на картата. Например не ни интересува, каква е формата на държавата Сърбия. Единственото, което е необходимо като информация е - кои са държавите на балканския полуостров и коя е свързана с коя.



Определение 6.1. Краен (неориентиран) граф наричаме наредена двойка множества $G = (V, E)$, където V е крайно непразно множество от върхове, а E е множество е дву-елементни подмножества на V, които наричаме ребра.

Така горният пример задава графа $G = (V, E)$, където

$$V = \{Slo, Cro, BH, Mon, Alb, Serb, Mac, Gr, Rom, Bul, Tur\}$$

$$E = \{\{Slo, Cro\}, \{Cro, BH\}, \{Cro, Serb\}, \{BH, Mon\}, \{BH, Serb\}, \{Mon, Alb\},$$
$$\{Mon, Serb\}, \{Alb, Serb\}, \{Alb, Mac\}, \{Alb, Gr\}, \{Serb, Mac\}, \{Serb, Rom\},$$
$$\{Serb, Bul\}, \{Mac, Gr\}, \{Mac, Bul\}, \{Gr, Bul\}, \{Gr, Tur\}, \{Rom, Bul\}, \{Bul, Tur\}\}$$

6.1.1 Представяне на графи

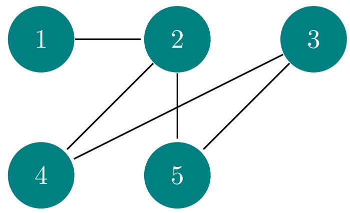
Ще илюстриране различните представяния на графи върху следният примерен граф:

$$G = (\{1, 2, 3, 4, 5\}, \{\{1, 2\}, \{2, 4\}, \{2, 5\}, \{3, 4\}, \{3, 5\}\})$$

Графично представяне

Графичното представяне на граф прилича на графичното представяне на релация. Разликата е че вместо да използваме стрелки свързващи два възела които са в релация, използваме неориентирани дъги.

Два върха $u, v \in V$ в граф наричаме съседни, ако са свързани с ребро, т.е. $\{u, v\} \in E$. За всеки връх от графа поставяме по един възел, а възлите, съответстващи на съседни върхове, свързваме с дъга.



Таблично представяне

Графичното представяне е удобно за работа, защото ни дава визуална представа за структурата на графа. Ако обаче трябва да съхраним информацията за даден граф в компютърна програма, това представяне не е подходящо. Отново, както при релациите, имаме и алтернативно таблично представяне на граф, чрез така наречената матрица на съседство. В общия случай, ако $G = (V, E)$ е граф и $V = \{v_1 \dots v_n\}$, матрицата на съседство е квадратна матрица $M = (m_{i,j})_{1 \leq i,j \leq n}$, с размерност- броя на върховете, $|V| = n$, където

$$m_{i,j} = \begin{cases} 0, & \text{ако } \{v_i, v_j\} \in E; \\ 1, & \text{ако } \{v_i, v_j\} \notin E. \end{cases}$$

Матрицата на съседство на примерния граф е:

*	1	2	3	4	5
1	0	1	0	0	0
2	1	0	0	1	1
3	0	0	0	1	1
4	0	1	1	0	0
5	0	1	1	0	0

Представяне чрез списък на съседство

В някои случаи по-удобно е да разполагаме с информацията, която описва един граф, в друга форма. Изреждаме всички върхове на графа в списък. С всеки връх v, свързваме списък от върховете u такива, че $\{u, v\} \in E$, т.е списъкът от неговите съседи.

Списъкът на съседство на примерния граф е:

1	$\rightarrow$	2		
2	$\rightarrow$	1	4	5
3	$\rightarrow$	4	5	
4	$\rightarrow$	2	3	
5	$\rightarrow$	2	3	

6.1.2 Някои основни характеристики на граф

Определение 6.2. Нека $G = (V, E)$ и $G' = (V', E')$ са графи. Казваме, че G е изоморфен на G', и пишем $G \cong G'$, ако съществува биекция $f : V \rightarrow V'$ такава, че за всяка двойка върхове $u, v \in V$,

$$\{u, v\} \in E \Leftrightarrow \{f(u), f(v)\} \in E'.$$

Два изоморфни графа не се различават по нищо друго, освен наименованието на техните върхове. Затова ние ще отъждествяваме изоморфните графи.

Определение 6.3. Нека $G = (V, E)$ е граф и $v \in V$. Степен на върха v, $d(v)$, наричаме броят на ребрата, на които v е край:

$$d(v) = |\{e \in E \mid v \in e\}.|$$

Степен на графа G, $d(G)$, е сумата от степените на неговите върхове:

$$d(G) = \sum_{v \in V} d(v).$$

Следващото твърдение, което е просто наблюдение, дава връзката между степента на граф и броя на неговите ребра.

Твърдение 6.4. Нека $G = (V, E)$.

$$d(G) = 2|E|$$

Доказателство. $d(G) = \sum_{v \in V} d(v) = \sum_{v \in V} |\{e \in E \mid v \in e\}$. Така ако e е реброто $e = \{u, v\}$, то e се брои точно два пъти: веднъж в степента на u и веднъж в степента на v. Така $d(G) = 2||$. $\square$

Определение 6.5. Нека $G = (V, E)$ е граф и $u, v \in V$. Път в G с дължина k от u до v, наричаме последователност от върхове $u = v_0, v_1, \dots v_k = v$ такива, че:

1. $\{v_i, v_{i+1}\} = e_i \in E$ за всяко $i = 0 \dots k - 1$;
2. $e_i \neq e_j$ за всяко $i \neq j$.

Забележете, че съгласно горната дефиниция, за всеки връх $v \in V$ има тривиален път от v до v с дължина 0.

Прост път, ще наричаме път в който няма повтарящ се връх. В сила е следното твърдение.

Твърдение 6.6. Нека $G = (V, E)$ е граф и $u = v_0, v_1, \dots v_k = v$ са върхове в G такива, че за всяко $i = 0 \dots k - 1$, $\{v_i, v_{i+1}\} \in E$. Тогава в G има прост път от u do v.

Доказателство. Ще опишем алгоритъм за намиране на прост път. Ако $u = v$, то има път от u до v, тривиалният път с дължина 0. Той е прост, защото съдържа само един връх.

Докато в P има повтарящ се връх, нека i е позицията на първия връх, който се повтаря в P. Нека j е последната позиция на която се среща върха v_j. Така

$$P = (v_0 \dots v_{i-1}, v_i, v_{i+1}, \dots v_{j-1}, v_i, v_{j+1} \dots v_k).$$

Тогава заменяме P с

$$P = (v_0 \dots v_{i-1}, v_i, v_{j+1} \dots v_k).$$

Алгоритъмът представлява цикъл, при всяко започване на който, P е редица от върхове такива, че първият е u, последният е v и всеки два върха на съседни позиции са свързани с ребро. Наистина, тъй като $u \neq v$, то или $i \neq 0$, или $j \neq k$. При всяко преминаване в цикъла, дължината на тази редица намалява с $j - i > 0$, следователно след краен брой стъпки алгоритъмът ще завърши и в P ще има последователност от върхове $u = v_0 \dots v_{k'} = v$ такива, че:

1. $\{v_i, v_{i+1}\} = e_i \in E$ за всяко $i = 0 \dots k' - 1$;

2. $v_i \neq v_j$ за всяко $i \neq j$, а следователно и $e_i \neq e_j$ за $i = 0 \dots k' - 1$.

□

Ще казваме че два върха в граф са свързани, ако има път между тях. Релацията, която се поражда от това понятие, е релация на еквивалентност.

Твърдение 6.7. Нека $G = (V, E)$. Тогава $C = \{(u, v) \mid u \text{ е свързан с } v\}$ е релация на еквивалентност над V.

Доказателство. Всеки връх $v \in V$ е свързан със себе си посредством тривиалният път с дължина 0, така $(v, v) \in C$ и релацията C е рефлексивна.

Нека $(u, v) \in C$. Нека $u = v_0, v_1 \dots v_k = v$ е път от u до v. Тогава $v = v_k, v_{k-1}, \dots v_1, v_0 = u$ е път от v до u, така $(v, u) \in C$ и C е симетрична.

Нека $(u, v) \in C$ и $(v, w) \in C$. Нека $u = v_0, v_1 \dots v_k = v$ е път от u до v и $v = w_0, w_1 \dots w_m = w$ е път от v до w. Тогава $u = v_0, v_1 \dots v_k = w_0, w_1 \dots w_m = w$ е редица от върхове, такива че всеки два върха на съседни позиции са свързани с ребро. Съгласно Твърдение 6.6 има път (дори прост път) от u до w, така $(u, w) \in C$ и C е транзитивна. □

Релацията C разделя V на класове на еквивалентност, които наричаме свързани компоненти на графа G.

Един граф G наричаме свързан, ако има само една свързана компонента, т.е. всеки два върха в G са свързани.

6.1.3 Цикли. Ойлеров и Хамилтонов цикъл.

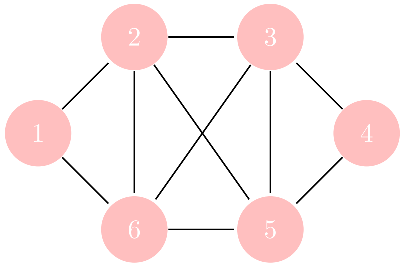
Освен тривиалният път с дължина 0, от връх v до v в граф, възможно е да има и по-дълги пътища. Разбира се, път от v до v с дължина 1 не не може да има, защото ребрата са винаги с по два различни върха. Не може да има и път от v do v с дължина 2, защото всеки две ребра в път трябва да са различни. Така най-късият нетривиален път от v до v е с дължина 3.

Определение 6.8. Нека $G = (V, E)$ е граф и $v \in V$. Път в G с дължина $k \geq 3$ от v до v, наричаме цикъл в G през v.

Ще разгледаме две специални вида цикъл в граф. Първият минава през всяко ребро точно по веднъж, вторият през всеки връх точно по веднъж.

Определение 6.9. Нека $G = (V, E)$ е граф и $v \in V$. Цикъл през v, който съдържа всяко ребро $e \in E$ точно по веднъж наричаме Ойлеров цикъл. Граф, който съдържа Ойлеров цикъл, наричаме Ойлеров граф.

Следният граф е Ойлеров.



Ойлер е намерил пълна характеризация на Ойлеровите графи:

Теорема 6.10. Нека $G = (V, E)$ е свързан граф. G е Ойлеров тогава и само тогава, когато всеки връх в G има четна степен.

Доказателство. Нека G е Ойлеров и нека $v = v_0, v_1 \dots v_k = v$ е Ойлеров цикъл в G. Всяко срещане на връх u в редицата $v_0 \dots v_{k-1}$ съответства на две ребра през u: ако $u = v_0$, ребрата са $\{v_0, v_1\}$ и $\{v_{k-1}, v_0\}$; ако $u = v_i$ и $i > 0$, ребрата са $\{v_i, v_{i+1}\}$ и $\{v_{i-1}, v_i\}$. Тъй като всички ребра в графа се срещат точно по веднъж в цикъла, степента на произволен връх $u \in V$ е равна на два пъти броя на срещанията на u в цикъла. Така $d(u)$ е четно число.

Нека сега G е свързан граф, в който всеки връх има четна степен и $u \in V$. Ще построим Ойлеров цикъл C през u.

Обявяваме u за текущ връх t, $C = (u)$.

1. *Докато има необходено ребро $e = \{t, v\}$ през t, добавяме t към C, обявяваме e за обходено и v за текущ връх t.*

Тъй като при всяко преминаване през цикъла, броят на необходените ребра намалява, цикълът ще завърши след краен брой стъпки k, и $C = (u = v_0, v_1, \dots v_k)$. При това твърдим, че $v_k = u$. Наистина, да допуснем, че $v_k \neq u$. Тъй като алгоритъмът завършва, всички ребра през v_k са обходени и на $k+1$-ва стъпка няма необходени ребра през v_k. На стъпка, на която v_k става текущ, обхождаме едно ребро през v_k и броят на обходените ребра през v_k е нечетен. На следващата стъпка, ако v_k престане да е текущ, обхождаме второ ребро през v_k броят на обходените ребра през v_k става четен. Така на последната стъпка, на която v_k става текущ, броят на обходените ребра през v_k е нечетен, но тогава алгоритъмът завършва, защото няма как да се избере следващ текущ връх, всички ребра през v_k са обходени. Това означава, че през v_k има нечетен брой ребра, което противоречи на четността на степента на v_k.

2. Следователно $v_k = u$ и C е цикъл. Ако C съдържа всички ребра, C е Ойлеров цикъл. Иначе, C съдържа поне един връх v_i, който е край на необходено ребро. Това следва от свързаността на графа. Повтаряме цикъла 1. с начален връх v_i като строим нов цикъл $C' = (v_i = u_0, u_1, \dots u_m = v_i)$. Заменяме C с цикъла

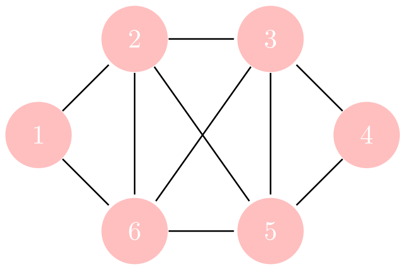
$$C = (v_0 \dots v_{i-1}, v_i = u_0, u_1, \dots u_m = v_i, v_{i+1}, \dots v_k)$$

и отново се връщаме на точка 2.

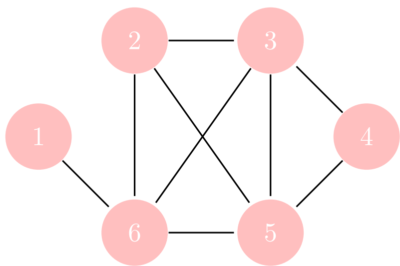
Вторият външен цикъл също ще завърши, защото при всяко преминаване през него, броят на необходените ребра намалява. Така в крайна сметка C съдържа Ойлеров цикъл. $\square$

Ако приложим алгоритъма към примерния граф с начален връх 1 получаваме следната последователност от стъпки:

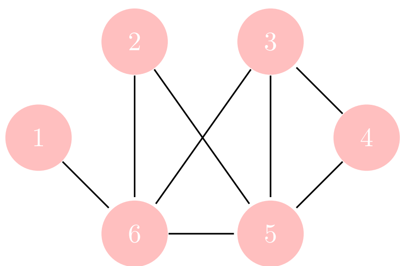
1. $C = (1), t = 1.$



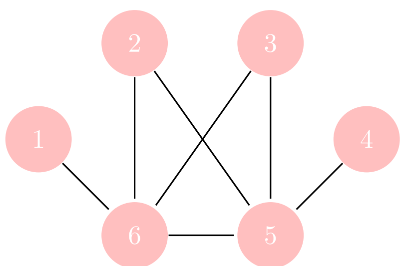
2. $C = (1, 2), t = 2.$



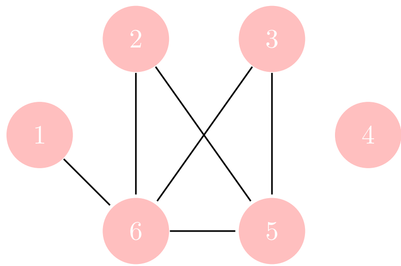
3. $C = (1, 2, 3), t = 3.$



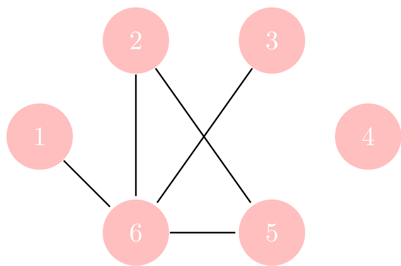
4. $C = (1, 2, 3, 4), t = 4.$



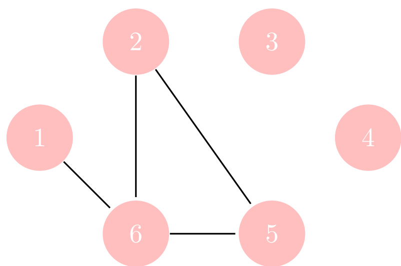
5. $C = (1, 2, 3, 4, 5), t = 5.$



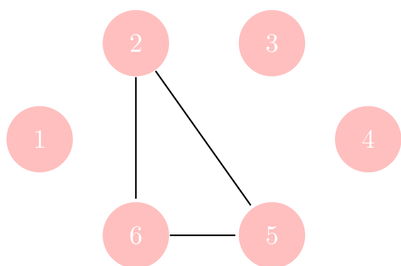
6. $C = (1, 2, 3, 4, 5, 3), t = 3.$



7. $C = (1, 2, 3, 4, 5, 3, 6), t = 6.$

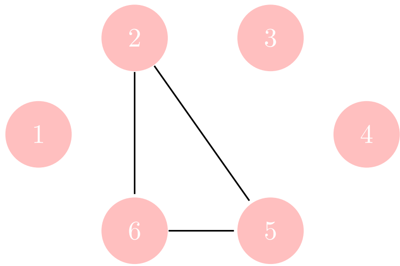


8. $C = (1, 2, 3, 4, 5, 3, 6, 1), t = 1.$

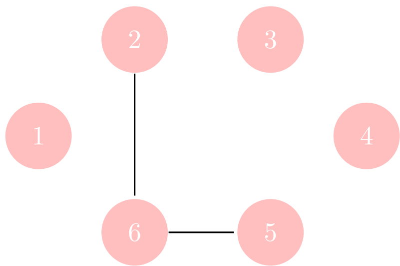


Сега C е цикъл, но не съдържа всички ребра. Стартираме алгоритъма отново с начален връх 2, защото има необходено ребро с край 2:

1.$C' = (2), t = 2.$



2. $C' = (2, 5), t = 5.$



3. $C' = (2, 5, 6), t = 6.$

4. $C' = (2, 5, 6, 2), t = 2.$

От $C = (1, 2, 3, 4, 5, 3, 6, 1)$ и $C' = (2, 5, 6, 2)$ строим цикъла $C = (1, 2, 5, 6, 2, 3, 4, 5, 6, 1)$. Това е вече Ойлеров цикъл.

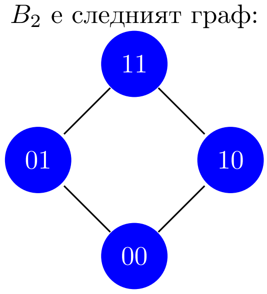
Определение 6.11. Нека $G = (V, E)$ е граф и $v \in V$. Цикъл през v, който съдържа всеки връх $v \in V$ точно по веднъж наричаме Хамилтонов цикъл. Граф, който съдържа Хамилтонов цикъл, наричаме Хамилтонов граф.

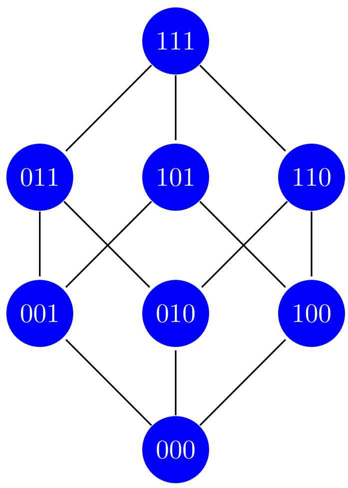
За разлика от Ойлеровите графи, нямаме добра характеризация на Хамилтоновите. Все пак ще разгледаме една група Хамилтонови графи.

Определение 6.12. Булев граф с размерност n наричаме граф $B_n = (V_n, E_n)$, където $V_n = \{0, 1\}^n$, n-мерните булеви вектори, а

$$E_n = \{\{\alpha, \beta\} \mid \alpha \text{ и } \beta \text{ се различават само в една позиция } \}.$$

B_2 е следният граф:





B_3 е следният граф:

Твърдение 6.13. За всяко $n \geq 2$, B_n е Хамилтонов граф.

Доказателство. Доказателството е с индукция по n.

Хамилтонов цикъл в B_2 е $(00), (01), (11), (10), (00)$.

Нека твърдението е в сила за B_n и нека $\alpha_1, \alpha_2, \ldots \alpha_{2^n}, \alpha_1$ е Хамилтонов цикъл в B_n. Тогава

$$0\alpha_1, 0\alpha_2, \ldots 0\alpha_{2^{n-1}}, 0\alpha_{2^n}, 1\alpha_{2^n}, 1\alpha_{2^{n-1}}, \ldots 1\alpha_2, 1\alpha_1, 0\alpha_1$$

е Хамилтонов цикъл в B_{n+1} □

6.2 Дървета

Ще дадем две дефиниции на структурата дърво. Първата показва, че дървото е специален случай на граф, а втората дава интуиция за структурата на едно дърво.

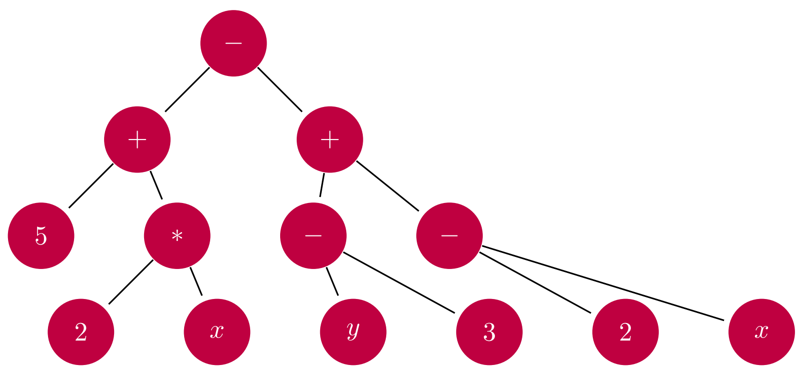
Определение 6.14. Граф $D = (V, E)$, който е свързан и няма цикли, наричаме дърво.

Втората дефиниция е за дърво, един от възлите на който се нарича корен. Дефиницията е индуктивна.

Определение 6.15. Графът $D = (\{r\}, \emptyset)$ е дърво с корен r и единствен лист r.

Нека $D = (V, E)$ е дърво с корен r и листа $l_1, \ldots l_n$. Нека $v \in V$ и $u \notin V$. Тогава $D' = (V \cup \{u\}, E \cup \{\{v, u\}\})$ е дърво с корен r. Ако $v = l_i$ за някое $i = 1 \ldots n$, листата на D' са $l_1 \ldots l_{i-1}, u, l_{i+1}, \ldots l_n$. Ако $v \neq l_i$ за всяко $i = 1 \ldots n$, то листата на D' са $l_1 \ldots l_n, u$.

Кореново дърво може да се използва за описание на израз без скоби - главната операция е корен на дървото, листата са атомарните стойности в израза. Например $(5 + 2x) - ((y - 3) + (2 - x))$ се представя така:



Твърдение 6.16. Всяко кореново дърво е дърво.

Доказателство. Доказателството е с индукция по дефиницията на кореново дърво. Графът $D = (\{r\}, \emptyset)$ е свързан граф без цикли, защото има само един възел.

Нека кореновото дърво $D = (V, E)$ е свързан граф без цикли. Нека $D' = (V \cup \{u\}, E \cup \{\{v, u\}\})$. Трябва да покажем, че D' също е свързан граф без цикли. Да изберем произволни два върха в D' - v_1, v_2. Ако $v_1 = v_2$, то има път - тривиален път с дължина нула от v_1 до v_2. Ако $v_1, v_2 \in V$, то v_1 и v_2 са върхове в графа D. Съгласно индукционното предположение, той е свързан граф. Следователно има път в D, от v_1 до v_2. Но всеки път в D е път и в D', защото ребрата в D са ребра и в D'. Така има път в D' от v_1 до v_2. Последният случай е един от върховете v_1 или v_2 да е новият връх u. Без ограничение на общността ще предполагаме, че $v_2 = u$. Тогава v_1, v са върхове в D и между тях има път $v_1 = u_1, u_2, \dots u_k = v$. Така $v_1 = u_1, u_2, \dots u_k = v, u$ е път в D' от v_1 до u. Следователно графът D' е свързан. Ако допуснем, че в него има цикъл $v_1, v_2, \dots v_k, v_1$, то всеки връх в цикъла v_i участва като край на две различни ребра: $\{v_{i-1}, v_i\}$ и $\{v_i, v_{i+1}\}$. Новият връх u е край на едно единствено ребро, следователно не участва в цикъла. Така $v_1, v_2, \dots v_k, v_1$ е цикъл в D, което противоречи на индукционното предположение. Така и D' е свързан граф без цикли. □

Едно от основните предимства на структурата дърво е следното свойство.

Твърдение 6.17. Нека $D = (V, E)$ е дърво и $u, v \in V$. Тогава между u и v има единствен път в D.

Доказателство. Да допуснем, че между u и v има два различни пътя: $u = u_1 \dots u_k = v$ и $u = v_1 \dots v_m = v$. Ще покажем, че в D има цикъл. Нека i е първата разлика между двата пътя: $u_1 = v_1, u_2 = v_2 \dots u_{i-1} = v_{i-1}$ и $u_i \neq v_i$. Нека j е най- малката позиция, такава, че u_j се среща измежду $v_{i-1}, \dots v_m$, например $v_{j'} = u_j$. Такова j съществува, защото $v_m = u_k$ $(j \leq k)$. Така

$$v_{i-1}, \dots v_{j'} = u_j, u_{j-1}, \dots u_i, u_{i-1}$$

е цикъл в D. Наистина всички върхове в този цикъл са различни с изключение на краищата. □

6.3 Покриващо дърво

Всеки свързан граф $G = (V, E)$ има покриващо дърво - дърво със същите върхове като G, но само с част от ребрата в G.

Определение 6.18. Нека $G = (V, E)$ е граф. Покриващо дърво на G наричаме дърво $D = (V, E')$, където $E' \subseteq E$.

За да покажем, че всеки свързан граф има покриващо дърво, ще докажем едно помощно твърдение.

Твърдение 6.19. Нека $G = (V, E)$ е свързан граф и $e \in E$ е ребро, което участва в цикъл в G. Тогава $G' = (V, E \setminus \{e\})$ също е свързан граф.

Доказателство. Нека $e = \{x, y\}$. Нека $y, x, x_1, x_2 \dots x_m = y$ е цикълът, в който участва e. Така съгласно дефиницията на път и цикъл в граф, e не се среща в пътя $x, x_1, x_2 \dots x_m = y$.

Да разгледаме два произволни върха $v_0, v_k \in V$. G е свързан граф следователно има път от v_0 до v_k в G, $v_0, v_1 \dots v_k$. Ако в този път не участва реброто e, то това е път в G'. Ако участва в този път - например $\{v_i, v_{i+1}\} = e$ и $v_i = x$, $v_{i+1} = y$, разглеждаме следната редица:

$$v_0 \dots v_{i-1}, v_i = x, x_1, x_2 \dots x_m = y = v_{i+1}, v_{i+2} \dots v_k.$$

Това е редица, в която всеки два съседни върха са свързани с ребро в G' и следователно съгласно Твърдение 6.6 има път от v_0 до v_k в G'. Така G' е свързан граф. □

Горното твърдение ни позволява да докажем, че всеки свързан граф има покриващо дърво с прост алгоритъм.

Твърдение 6.20. Граф $G = (V, E)$ има покриващо дърво, тогава и само тогава, когато е свързан.

Доказателство. Ако $G = (V, E)$ има покриващо дърво $D = (V, E')$, то $E' \subseteq E$ и всеки път в D е път в G. Щом D е свързан граф, то и G е свързан граф.

Нека сега $G = (V, E)$ е свързан граф. Прилагаме следния алгоритъм:

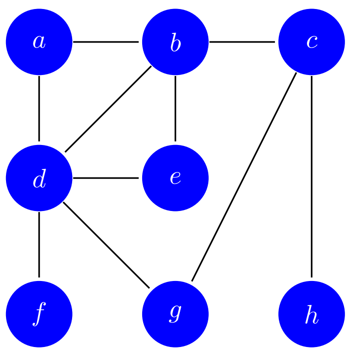
Нека $E' = E$. Докато в $G' = (V, E')$ има цикъл, намираме ребро $e \in E'$, което участва в цикъл с G' и заменяме E' с $E' \setminus \{e\}$.

Съгласно предишното твърдение при всяко изпълнение на цикъла G' е свързан граф. Алгоритъмът завършва, защото на всяка стъпка броят на ребрата в E' намалява с единица. Така след приключване на алгоритъма $G' = (V, E')$ е свързан граф без цикли. □

6.3.1 Обхождане на графи

Има много задачи свързани с обхождане на графи: да се провери дали има път между два върха, да се намери най-къс път от връх до всички останали, да се построи покриващо дърво. Имаме два основни метода за обхождане на граф: в дълбочина и в широчина.

Да разгледаме следният граф G:



Ще си мислим, че той е представен чрез списък от съседство:

a	$\to$	b	d			
b	$\to$	a	c	d	e	
c	$\to$	b	g	h		
d	$\to$	a	b	e	f	g
e	$\to$	b	d			
f	$\to$	d				
g	$\to$	c	d			
h	$\to$	c				

Обхождане в дълбочина

Основната идея на обхождане в дълбочина е: "Докато можем, вървим напред. Когато няма как да продължим - връщаме се една стъпка назад". За реализация на този алгоритъм ще използваме стек. Стекът е структура от данни, организирани на принципа - последен влязъл, пръв излязъл. Представете си, че прибираме книги в кутия, първата книга поставяме на дъното на кутията, всяка следваща върху предишната. Най-отгоре стои последната книга, която сме добавили. За да достигнем първата книга в кутията, трябва да извадим всички останали. Дефиницията на стек, заедно с трите операции *top* (връх на стека), *pop* (изтриване на елемент от стека) и *push* (добавяне на елемент към стека) е индуктивна.

Определение 6.21. Празният стек означаваме с $\{\ \}$. За него дефинираме $pop(\{\ \}) = \{\ \}$, $top(\{\ \}) = \{\ \}$.

Нека S е стек и x е елемент. Тогава $S' = push(S, x)$ е стек, като $top(S') = x$, $pop(S') = S$.

Нека $G = (V, E)$ е произволен граф с n върха и $v_0 \in V$ е начален връх. Ще построим списък $DFS = ((v_0, \emptyset), (v_1, s(v_1)), \dots (v_n, s(v_n))$, който включва всички върхове $v_1 \dots v_n$ и техните непосредствени предшественици в покриващото дърво с корен v_0: $D = (V, E')$, където $E' = \{\{v_i, s(v_i)\} \mid i = 1 \dots n\}$.

Ще използваме помощен стек S и текущ връх t. В началото $DFS = ((v_0, \emptyset))$ и $S = \{\ \}$, $t = v_0$ и v_0 е обходен.

Докато има необходен връх в V:

1. *Ако има необходен съсед* v *на* t*, обявяваме* v *за обходен, добавяме* (v, t) *към списък* $DFS = DFS \cup \{(v, t)\}$*, добавяме* t *към стека:* $S := push(S, t)$*, текущ връх става* $t := v$.

2. *Ако няма необходен съсед на* t*, връщаме се една стъпка назад:* $t = top(S)$, $S := pop(S)$.

За илюстрация ще приложим алгоритъма към примерния граф с начален връх a. Ето какви последователни стъпки ще имаме:

1. $DFS = ((a, \emptyset)), t = a, S = \{\ \}$.

2. $DFS = ((a, \emptyset), (b, a)), t = b, S = \{a\}$.

3. $DFS = ((a, \emptyset), (b, a), (c, b)), t = c, S = \{b, a\}$.

4. $DFS = ((a, \emptyset), (b, a), (c, b), (c, g)), t = g, S = \{c, b, a\}$.

5. $DFS = ((a, \emptyset), (b, a), (c, b), (c, g), (d, g)), t = d, S = \{g, c, b, a\}$.

6. $DFS = ((a, \emptyset), (b, a), (c, b), (c, g), (d, g), (e, d)), t = e, S = \{d, g, c, b, a\}$.

7. $DFS = ((a, \emptyset), (b, a), (c, b), (c, g), (d, g), (e, d)), t = d, S = \{g, c, b, a\}$.

8. $DFS = ((a, \emptyset), (b, a), (c, b), (c, g), (d, g), (e, d), (f, d)), t = f, S = \{d, g, c, b, a\}$.

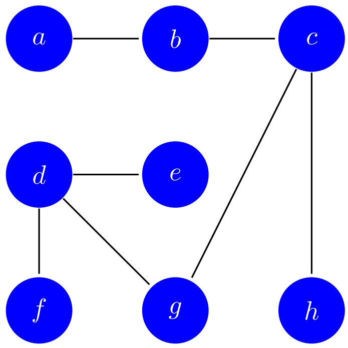
9. $DFS = ((a, \emptyset), (b, a), (c, b), (c, g), (d, g), (e, d), (f, d)), t = d, S = \{g, c, b, a\}$.

10. $DFS = ((a, \emptyset), (b, a), (c, b), (c, g), (d, g), (e, d), (f, d)), t = g, S = \{c, b, a\}$.

11. $DFS = ((a, \emptyset), (b, a), (c, b), (c, g), (d, g), (e, d), (f, d)), t = c, S = \{b, a\}$.

12. $DFS = ((a, \emptyset), (b, a), (c, b), (c, g), (d, g), (e, d), (f, d), (h, c)), t = h, S = \{c, b, a\}$.

В крайна сметка получаваме следното покриващо дърво:



Обхождане в дълбочина е ефективно при задачи от вида - да се намери път в свързан граф от връх u_0 до връх u_1. За целта ще модифицираме алгоритъма по следния начин:

В началото $S = \{\ \}$, $t = u_1$ и u_1 е обходен.

Докато $t \neq u_0$:

1. *Ако има необходен съсед v на t, обявяваме v за обходен, добавяме t към стека: $S := push(S, t)$, текущ връх става $t := v$.*

2. *Ако няма необходен съсед на t, връщаме се една стъпка назад: $t = top(S)$, $S := pop(S)$.*

При завършване на алгоритъма в S ще е записан търсеният път.

Обхождане в широчина

Основната идея на обхождане в широчина е: "Докато можем вървим в страни. След това минаваме едно ниво надолу". За реализация на този алгоритъм ще използваме опашка. Опашката е структура от данни, организирани на принципа - пръв влязъл, пръв излязъл. Представете си, в един идеален свят - опашка за лифт, в която нито един скиор или сноубордист не се предрежда: този който се е наредил пръв, пръв ще се качи на лифта. Дефиницията на опашка, заедно с трите операции *top*, *pop* и *push* отново е индуктивна.

Определение 6.22. Празната опашка означаваме с $\{\ \}$. За нея $pop(\{\ \}) = top(\{\ \}) = \{\ \}$.

Нека Q е опашка и x е елемент. Тогава $Q' = push(Q, x)$ е опашка.

$$top(Q') = \begin{cases} x, & \text{ако } Q = \{\ \}; \\ top(Q), & \text{ако } Q \neq \{\ \}. \end{cases}$$

$$pop(Q') = \begin{cases} \{\ \}, & \text{ако } Q = \{\ \}; \\ push(pop(Q), x), & \text{ако } Q \neq \{\ \}. \end{cases}.$$

Нека $G = (V, E)$ е произволен граф с n върха и $v_0 \in V$ е начален връх. Ще построим списък $BFS = ((v_0, \emptyset), (v_1, s(v_1)), \dots (v_n, s(v_n)))$, който включва всички върхове $v_1 \dots v_n$ и техните непосредствени предшественици в покриващото дърво с корен v_0: $D = (V, E')$, където $E' = \{\{v_i, s(v_i)\} \mid i = 1 \dots n\}$.

Ще използваме помощна опашка Q и текущ връх t. В началото $BFS = ((v_0, \emptyset))$ и $Q = \{\ \}$, $t = v_0$ и v_0 е обходен.

Докато има необходен връх в V:

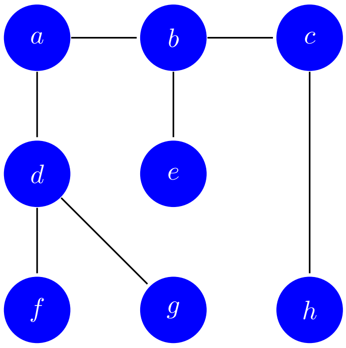
1. *Ако има необходен съсед* v *на* t*, обявяваме* v *за обходен, добавяме* (v, t) *към списък* $BFS = BFS \cup \{(v, t)\}$*, добавяме* v *към опашката:* $Q := push(Q, v)$.

2. *Ако няма необходен съсед на* t*, текущ връх става първият връх на опашката:* $t = top(Q)$, $Q := pop(Q)$.

За илюстрация ще приложим алгоритъма към примерния граф с начален връх a. Ето какви последователни стъпки ще имаме:

1. $BFS = ((a, \emptyset)), t = a, Q = \{\ \}$.
2. $BFS = ((a, \emptyset), (b, a)), t = a, Q = \{b\}$.
3. $BFS = ((a, \emptyset), (b, a), (d, a)), t = a, Q = \{b, d\}$.
4. $BFS = ((a, \emptyset), (b, a), (d, a)), t = b, Q = \{d\}$.
5. $BFS = ((a, \emptyset), (b, a), (d, a), (c, b)), t = b, Q = \{d, c\}$.
6. $BFS = ((a, \emptyset), (b, a), (d, a), (c, b), (e, b)), t = b, Q = \{d, c, e\}$.
7. $BFS = ((a, \emptyset), (b, a), (d, a), (c, b), (e, b)), t = d, Q = \{c, e\}$.
8. $BFS = ((a, \emptyset), (b, a), (d, a), (c, b), (e, b), (f, d)), t = d, Q = \{c, e, f\}$.
9. $BFS = ((a, \emptyset), (b, a), (d, a), (c, b), (e, b), (f, d), (g, d)), t = d, Q = \{c, e, f, g\}$.
10. $BFS = ((a, \emptyset), (b, a), (d, a), (c, b), (e, b), (f, d), (g, d)), t = c, Q = \{e, f, g\}$.
11. $BFS = ((a, \emptyset), (b, a), (d, a), (c, b), (e, b), (f, d), (g, d), (c, h)), t = c, Q = \{e, f, g, h\}$.

В крайна сметка получаваме следното покриващо дърво:



Теорема 6.23. Обхождане в широчина намира най-късите пътища от началния връх до всички останали върхове в графа.

Доказателство. Нека с $d(v)$ означим дължината на минимален път от началният връх до v. Първо ще покажем, следното:

Когато връх v става текущ, всички върхове u с $d(u) < d(v)$ вече са били текущи. Наистина, да допуснем че v е първият връх, който става текущ преди друг връх $u \in V$ с $d(u) < d(v)$ да е бил избран за текущ. Забележете, че $v \neq v_0$, защото $d(v_0) = 0$ и няма връх u с по-къс път до v_0. След като v не е начален, той става текущ, защото е връх на опашката. Той е добавен към опашката, когато текущ връх е бил някой негов съсед t. Така $d(t) \geq d(v) - 1$.

Върхът u също не е начален, защото все още, когато v става текущ, той не е бил текущ. Така всеки минимален път от v_0 до u има дължина $k \geq 1$. Да вземем един такъв път $v_0, u_1 \dots u_{k-1}, u_k = u$. Да разгледаме върха u_{k-1}. За него имаме $d(u_{k-1}) = d(u) - 1 < d(v) - 1 \leq d(t)$. Съгласно избора на v като пръв, който нарушава условието, u_{k-1} трябва да е бил текущ преди t. Но съгласно алгоритъма u ще влезне в опашката, най-късно по време на стъпките, когато u_{k-1} е текущ и следователно, преди v. Щом u е пред v в опашката, съгласно алгоритъма, той ще е текущ преди v- което противоречи на допускането.

Да разгледаме път $v_0, v_1 \dots v_k = v$ от началният връх до връх v в покриващото дърво D. Да допуснем, че $d(v_i) = i$ за $i < k$, но има по-къс път от v_0 до v. Отново $d(v) \geq 1$, защото ако $d(v) = 0$, то $v = v_0$, а най-къс път от v_0 до v_0 в D е тривиалният път с дължина 0. Нека най-къс път v_0 до v е $v_0, u_1, \dots u_m = v$, $m < k$. Така $d(v_{k-1}) = k - 1 < m - 1 = d(u_{m-1})$. Следователно u_{m-1} става текущ преди v_{k-1}. Но тогава алгоритъмът ще обяви v за обходен, когато u_{m-1} е текущ, и няма да добави реброто $\{v, v_{k-1}\}$ към покриващото дърво, когато на по-късен етап v_{k-1} е текущ, което е противоречие с допускането. $\square$

6.3.2 Минимално покриващо дърво

Нека е даден свързан граф $G = (V, E)$. Нека $c : E \to \mathbb{N}$ е функция, която задава цена на всяко ребро.

Определение 6.24. Минимално покриващо дърво на G наричаме дърво $D = (V, E_0)$ такова, че за всяко друго покриващо дърво на G, $D' = (V, E')$ е в сила следното неравенство:

$$\sum_{e \in E_0} c(e) \leq \sum_{e \in E'} c(e)$$

Ще докажем едно твърдение, което ще ни позволи да намерим алгоритми за намиране на минимално покриващо дърво на свързан граф.

Твърдение 6.25. Нека $U \subseteq V$ и нека $e = \{u, v\} \in E$ е ребро такова, че $u \in U$, $v \in V \setminus U$ и измежду всички ребра $e' = \{u', v'\}$ с $u' \in U$ и $v' \in V \setminus U$, реброто e е с най-ниска цена, т.е. $c(e) \leq c(e')$. Тогава G има минимално покриващо дърво, в което участва e.

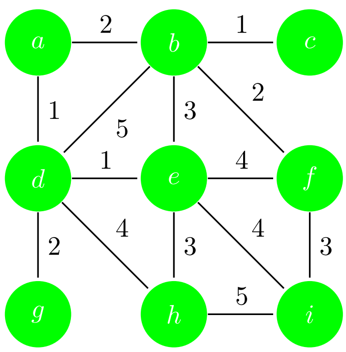
Доказателство. Нека $D(V, E_0)$ е минимално покриващо дърво. Да допуснем, че e не участва в E_0. Тогава в D има път от u до v, $u = u_0, u_1 \ldots, u_k = v$. В този път участва поне едно ребро $e' = \{u_i, u_{i+1}\}$ такова, че $u_i \in U$ и $u_{i+1} \in V \setminus U$. Така в графа $D' = (V, E_0 \cup \{e\})$ има цикъл $v, u = u_0, u_1 \ldots, u_k = v$. Съгласно Твърдение 6.19 графът $D'' = (V, (E_0 \cup \{e\}) \setminus \{e'\})$ е свързан и има покриващо дърво (V, E_1), където $e \in E_1 \subseteq (E_0 \cup \{e\}) \setminus \{e'\}$. По условие $c(e) \leq c(e')$, следователно:

$$\sum_{e \in E_1} c(e) \leq \sum_{e \in (E_0 \cup \{e\}) \setminus \{e'\}} c(e) \leq \sum_{e \in E_0} c(e).$$

□

Това свойство ни дава възможност да прилагаме така наречените алчни алгоритми за намиране на минимално покриващо дърво.

Отново ще разгледаме примерен граф, върху който да илюстрираме алгоритмите.



Алгоритъм на Прим

Нека $G = (V, E)$ е свързан граф и нека $c : E \to \mathbb{N}$ е функция, която задава цена на всяко ребро. Алгоритъмът на Прим построява минимално покриващо кореново дърво $MST = (V, E_0)$ на G с корен, отнапред зададен начален връх $v_0 \in V$. По време на изпълнение на алгоритъма V' ще съдържа всички обходени досега върхове. $E_0 \subseteq E$ ще съдържа ребрата, които до момента сме включили в дървото.

В началото $MST = (V' = \{v_0\}, E' = \emptyset)$.

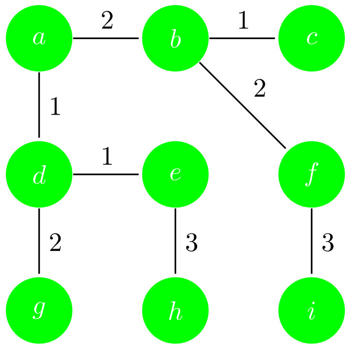
Докато $V' \neq V$: намираме ребро $e = \{u, v\} \in E$, такова че $u \in V'$, $v \in V \setminus V'$ и измежду всчики такива ребра, e е с минимална цена, т.е. за всяко ребро $e' = \{u', v'\} \in E$ такова, че $u' \in V'$ и $v' \in V \setminus V'$ имаме, че $c(e) \leq c(e')$. Добавяме към $'$, $E' := E' \cup \{e\}$ и добавяме v към V', $V' := V' \cup \{v\}$.

Алгоритъмът завършва, защото на всяка стъпка $|V \setminus V'|$ намалява с единици. Съгласно Твърдение 6.25, MPD е минимално покриващо дърво.

Стъпките, от този алгоритъм, приложен към примерния граф с начален връх a са следните:

1. $V' = \{a\}$, $E' = \emptyset$.
2. $V' = \{a, d\}$, $E' = \{\{a, d\}\}$.
3. $V' = \{a, d, e\}$, $E' = \{\{a, d\}, \{d, e\}\}$.
4. $V' = \{a, d, e, b\}$, $E' = \{\{a, d\}, \{d, e\}, \{a, b\}\}$.
5. $V' = \{a, d, e, b, c\}$, $E' = \{\{a, d\}, \{d, e\}, \{a, b\}, \{b, c\}\}$.
6. $V' = \{a, d, e, b, c, f\}$, $E' = \{\{a, d\}, \{d, e\}, \{a, b\}, \{b, c\}, \{b, f\}\}$.
7. $V' = \{a, d, e, b, c, f, g\}$, $E' = \{\{a, d\}, \{d, e\}, \{a, b\}, \{b, c\}, \{b, f\}, \{d, g\}\}$.
8. $V' = \{a, d, e, b, c, f, g, h\}$, $E' = \{\{a, d\}, \{d, e\}, \{a, b\}, \{b, c\}, \{b, f\}, \{d, g\}, \{e, h\}\}$.
9. $V' = \{a, d, e, b, c, f, g, h, i\}$, $E' = \{\{a, d\}, \{d, e\}, \{a, b\}, \{b, c\}, \{b, f\}, \{d, g\}, \{e, h\}, \{f, i\}\}$.

Дървото, което се получава, е:



Алгоритъм на Крускал

Вторият алгоритъм за построяване на минимално покриващо дърво е на Крускал. Тук не е зададен отнапред корен на дървото.

Нека отново $G = (V, E)$ е свързан граф и нека $c : E \to \mathbb{N}$ е функция, която задава цена на всяко ребро. Нека броят на ребрата е $|E| = n$. Алгоритъмът на Крускал построява минимално покриващо дърво $MST = (V, E_0)$ на G.

1. *Сортираме ребрата във възходящ ред на тяхната цена:* $E = \{e_1, \ldots e_n\}$, *така, че* $c(e_1) \leq c(e_2) \leq \ldots c(e_n)$. *Ще използваме брояч* i, *който в началото е* $i := 1$.

2. *За всеки от върховете* $v \in V$ *строим тривиално дърво с корен* v: $D_v = (\{v\}, \emptyset)$. *Нека* $D = \{D_v \mid v \in V\}$.

3. *Докато има D съдържа повече от едно дърво: Разглеждаме реброто $e_i = \{u_i, v_i\}$. Ако u_i и v_i са в две различни дървета $D_{u_i} = (V_{u_i}, E_{u_i})$ и $D_{v_i} = (V_{v_i}, E_{v_i})$, изтриваме тези две дървета от D и добавяме ново дърво $D_{u_i,v_i} = (V_{u_i} \cup V_{v_i}, E_{u_i} \cup E_{v_i} \cup \{e_i\})$. Така $D := (D \setminus \{D_{u_i}, D_{v_i}\}) \cup \{D_{u_i,v_i}\}$. При висчки случаи увеличаваме i с единица: $i := i + 1$.*

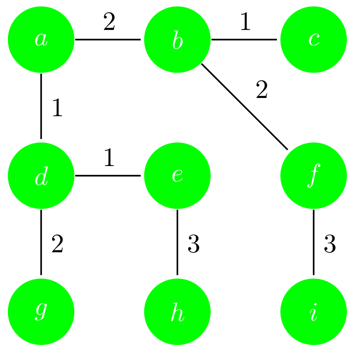
Сортирани ребрата от примерния граф изглеждат така:

$$\{\{a,d\},\{b,c\},\{d,e\},\{a,b\},\{b,f\},\{d,g\},\{b,e\}$$
$$\{e,h\},\{f,i\},\{d,h\},\{e,f\},\{e,i\},\{d,b\},\{h,i\}\}$$

Стъпките, от този алгоритъм, приложен към примерния граф са следните.

1. $i = 1, D = \{(\{a\},\emptyset),(\{b\},\emptyset),(\{c\},\emptyset),(\{d\},\emptyset),(\{e\},\emptyset),(\{f\},\emptyset),(\{g\},\emptyset),(\{h\},\emptyset),(\{i\},\emptyset)\}$
2. $i = 2, D = \{(\{a,d\},\{\{a,d\}\}),(\{b\},\emptyset),(\{c\},\emptyset),(\{e\},\emptyset),(\{f\},\emptyset),(\{g\},\emptyset),(\{h\},\emptyset),(\{i\},\emptyset)\}$
3. $i = 3, D = \{(\{a,d\},\{\{a,d\}\}),(\{b,c\},\{\{b,c\}\}),(\{e\},\emptyset),(\{f\},\emptyset),(\{g\},\emptyset),(\{h\},\emptyset),(\{i\},\emptyset)\}$
4. $i = 4, D = \{(\{a,d,e\},\{\{a,d\},\{d,e\}\}),(\{b,c\},\{\{b,c\}\}),(\{f\},\emptyset),(\{g\},\emptyset),(\{h\},\emptyset),(\{i\},\emptyset)\}$
5. $i = 5, D = \{(\{a,d,e,b,c\},\{\{a,d\},\{d,e\},\{b,c\},\{a,b\}\}),(\{f\},\emptyset),(\{g\},\emptyset),(\{h\},\emptyset),(\{i\},\emptyset)\}$
6. $i = 6, D = \{(\{a,d,e,b,c,f\},\{\{a,d\},\{d,e\},\{b,c\},\{a,b\},\{b,f\}\}),(\{g\},\emptyset),(\{h\},\emptyset),(\{i\},\emptyset)\}$
7. $i = 7, D = \{(\{a,d,e,b,c,f,g\},\{\{a,d\},\{d,e\},\{b,c\},\{a,b\},\{b,f\},\{d,g\}\}),(\{h\},\emptyset),(\{i\},\emptyset)\}$
8. $i = 8, D = \{(\{a,d,e,b,c,f,g\},\{\{a,d\},\{d,e\},\{b,c\},\{a,b\},\{b,f\},\{d,g\}\}),(\{h\},\emptyset),(\{i\},\emptyset)\}$
9. $i = 9, D = \{(\{a,d,e,b,c,f,g,h\},\{\{a,d\},\{d,e\},\{b,c\},\{a,b\},\{b,f\},\{d,g\},\{e,h\}\}),(\{i\},\emptyset)\}$
10. $i = 10, D = \{(\{a,d,e,b,c,f,g,h,i\},\{\{a,d\},\{d,e\},\{b,c\},\{a,b\},\{b,f\},\{d,g\},\{e,h\},\{f,i\}\})\}$

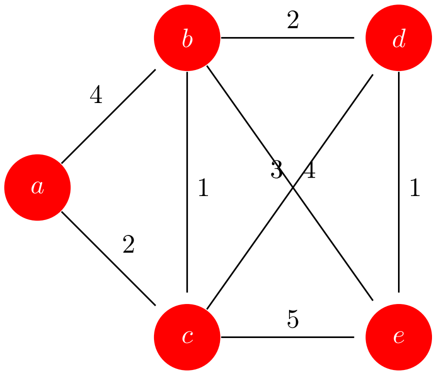
Дървото, което се получава, е същото:



6.4 Минимален път. Алгоритъм на Дийкстра

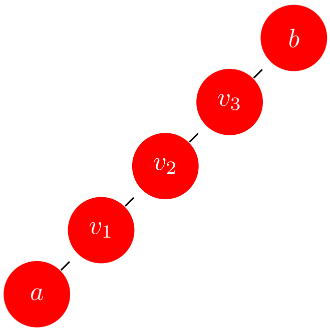
Нека $G = (V, E)$ е граф и нека $c : E \to \mathbb{N}$ е функция, която задава цена на всяко ребро. Задачата, която ще разгледаме в този раздел е да се намери път с минимална цена от даден начален връх $v_0 \in V$, до всички останали върхове.

Да разгледаме следният примерен граф:



Ако ценовата функция е константата едно, то задачата за минимален път в граф от даден връх до останалите върхове се свежда до задчата за най-къс път в граф от даден връх до останалите върхове. Тази задача, ние вече видяхме как можем да решим - строим покриващо дърво обхождане в широчина, с начален връх - даденият. Ако ценовата функция не е константа, отново бихме могли да сведем задачата до намиране на най-къс път, към граф който получаваме от дадения по следния начин: за всяко ребро $e \in E$ с $c(e) = k$ добавяме нови върхове $v_1, v_2 \dots v_{k-1}$ и заменямае реброто $e = \{u, v\}$ с ребрата $\{u, v_1\}, \{v_1, v_2\}, \dots \{v_{k-1}, v_k\}$.

Така в примерния граф, ще заменим реброто $\{a, b\}$ с цена 4 с:



Този подход е изключително неикономичен. Дийкстра е предложил следния по-добър алгоритъм за намиране на минимален път. В него вместо опашка, каквато използвахме при обхождане в широичина, ще използваме така наречената приоритетна опашка. Приоритетна опашка е структура от данни, в която допълнително с всеки елемент сме свързали ключ. Ключът е някаква числова стойност, която задава приоритет на всеки елемент. Например ние ще използваме приоритетна опашка от върховете на графа, а за ключ на връх ще използваме текущата ни апроксимация на най-къс път от върха до началния връх. Връх на приоритетната опашка ($top(PQ)$), ще е елемент с минимална стойност на ключа. Когато изтриваме елемент от приоритетна опашка, винаги изтриваме върха на опашката.

Нека v_0 е началният връх. Добавяме всички върхове $v \in V$ в графа G към приоритетна опашка PQ, като за ключ ще използваме $d(v)$, апроксимацията ни за цената на минималният път от v_0 до v. Начални стойности за този ключ са $d(v_0) = 0$ и $d(v) = \infty$, за $v \neq v_0$. Текущ връх ще е t, в началото t не е дефиниран. Обходените върхове ще събираме в списък S. Ще имаме и апроксимация за предшественика на връх v по минималния път, която ще пазим в $s(v)$. В началото $s(v_0) = v_0$, а за всеки друг връх v, $s(v)$ не е дефиниран. Така накрая ще можем да възстановим минималния път от v_0 до v, това ще е $v_0, v_1, \dots v_k = v$, където $v_i = s(v_{i+1})$ за $i = 0 \dots k-1$.

Докато има необходен връх:

Нека $t = top(PQ)$, $PQ = pop(PQ)$. Обявяваме t за обходен и го добавяме към S. За всеки съсед u на текущия връх t, проверяваме дали $d(u) > d(t) + c(\{u,t\})$ и ако е така, променяме стойността на ключа $d(u) := d(t) + c(\{u,t\})$ и на предшественика $s(u) = t$.

Стъпките от този алгоритъм, приложен към примерния граф с начален връх a, са следните:

1. $S = \emptyset$, $t = \emptyset$, $PQ = (a,b,c,d,e)$
   $d(a) = 0$, $d(b) = \infty$, $d(c) = \infty$, $d(d) = \infty$, $d(e) = \infty$
   $s(a) = a$, $s(b) = \emptyset$, $s(c) = \emptyset$, $s(d) = \emptyset$, $s(e) = \emptyset$.

2. $S = (a)$, $t = a$, $PQ = (b,c,d,e)$
   $d(a) = 0$, $d(b) = 4$, $d(c) = 2$, $d(d) = \infty$, $d(e) = \infty$
   $s(a) = a$, $s(b) = a$, $s(c) = a$, $s(d) = \emptyset$, $s(e) = \emptyset$.

3. $S = (a,c)$, $t = c$, $PQ = (b,d,e)$
   $d(a) = 0$, $d(b) = 3$, $d(c) = 2$, $d(d) = 6$, $d(e) = 7$
   $s(a) = a$, $s(b) = a$, $s(c) = a$, $s(d) = c$, $s(e) = c$.

4. $S = (a,c,b)$, $t = b$, $PQ = (d,e)$
   $d(a) = 0$, $d(b) = 3$, $d(c) = 2$, $d(d) = 5$, $d(e) = 6$
   $s(a) = a$, $s(b) = a$, $s(c) = a$, $s(d) = b$, $s(e) = b$.

5. $S = (a,c,b,d)$, $t = d$, $PQ = (d)$
   $d(a) = 0$, $d(b) = 3$, $d(c) = 2$, $d(d) = 5$, $d(e) = 6$
   $s(a) = a$, $s(b) = a$, $s(c) = a$, $s(d) = b$, $s(e) = b$.

6. $S = (a,c,b,d,e)$, $t = e$, $PQ = ()$
   $d(a) = 0$, $d(b) = 3$, $d(c) = 2$, $d(d) = 5$, $d(e) = 6$
   $s(a) = a$, $s(b) = a$, $s(c) = a$, $s(d) = b$, $s(e) = b$.

Теорема 6.26. Алгоритъмът на Дийкстра намира минималният път от началния връх до произволен друг връх в графа.

Доказателство. Нека с $\delta(v)$ означим цената на минималния път от v_0 до v. Ще покажем, че когато алгоритъмът завърши $d(v) = \delta(v)$, за всеки връх $v \in V$.

Първо, нека отбележем, че в началото на всеки цикъл, $d(v) \geq \delta(v)$ за всеки връх $v \in V$. Наистина, в началото на първия цикъл, твърдението е вярно, защото $d(v_0) = 0 = \delta(v_0)$ и $d(v) = \infty \geq \delta(v)$ за всеки друг връх v. Ако твърдението е вярно за всички върхове в началото на даден цикъл и по време на цикъла заменим стойността на $d(v)$ с $d(t) + c(\{t, v\})$, то понеже $\delta(t) \leq d(t)$ от индукционното предположение и понеже $\delta(v) \leq \delta(t) + c(\{t, v\})$, имаме че новата стойност на $d(v)$ изпълнява условието $d(v) \geq \delta(v)$.

Нека $S = (v_0, v_1, \ldots v_n)$ резултатът от изпълнението на алгоритъма. С индукция по i ще докажем, че когато v_i става текущ на стъпка i, стойността $d(v_i)$ е равна на $\delta(v_i)$. Твърдението е в сила за $i = 0$, защото v_0 е началният връх и $d(v_0) = \delta(v_0) = 0$ на стъпка 0.

Нека твърдението е в сила за всички върхове $v_0, \ldots, v_{i-1}$ и на стъпка i върхът v_i става текущ. Да допуснем, че $\delta(v_i) < d(v_i)$. Нека разгледаме минималния път от v_0 до v_i. Ако предпоследния връх по този път е v_j, за $j < i$, то на стъпка j, когато v_j става текущ, имаме следното:

1. съгласно индукционното предположение: $d(v_j) = \delta(v_j)$;
2. $d(v_i) \geq \delta(v_i)$;
3. $\delta(v_i) = \delta(v_j) + c(\{v_j, v_i\})$.

Тогава на стъпка j, алгоритъмът би променил $d(v_i)$ на $\delta(v_i)$ и тъй като $d(v_i)$ може само да намалява, няма как на стъпка i да имаме $\delta(v_i) < d(v_i)$.

Така в минималния път от v_0 до v_i има връх u, който на стъпка i все още не е посетен и следователно е в опашката. Нека разгледаме първият такъв връх u по пътя и нека предходния е v_j, където $j < i$. Тогава както преди можем да покажем, че на стъпка j алгоритъмът ще промени стойността на $d(u)$ и ще имаме

$$d(u) \leq \delta(v_j) + c(\{v_j, u\}) < \delta(v_i) \leq d(v_i).$$

На стъпка i алгоритъмът би избрал u вместо v_i за текущ. Така достигнахме до противоречие, следователно допускането ни е грешно и $\delta(v_i) = d(v_i)$ на стъпка i. $\square$

6.5 Задачи за упражнение

Задача 1. Даден е следният граф: $G = (V, E)$, където $V = \{1, 2, 3, 4, 5, 6, 7, 8\}$, $E = \{\{1, 2\}, \{1, 5\}, \{1, 6\}, \{2, 5\}, \{3, 6\}, \{3, 7\}, \{3, 8\}, \{4, 7\}, \{4, 8\}\}$. Намерете:

1. Графично представяне на G.
2. Таблично представяне на G.
3. Списък на съседство за G.
4. Каква е степента на върховете $1, 3, 6$.
5. Каква е степента на G
6. Свързан ли е G.
7. Намерете три различни пътя от 1 до 8.

8. Намерете цикъл през 1 с дължина 3.

9. Ойлеров ли е този граф?

Задача 2. Нека $G = (V, E)$ е граф с n върха.

1. Докажете, че броят на върховете в G с нечетна степен е четен. (Използвайте, че $d(G) = 2|E|$)

2. Каква е максималната степен на връх в G? Каква е минималната степен на връх в G?

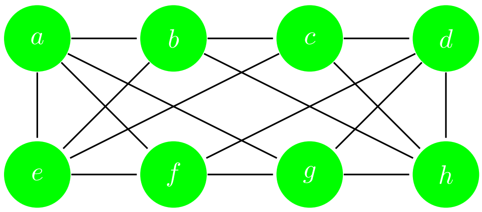
3. Възможно ли е в G едновременно да има връх с минимална и връх с максимална степен.

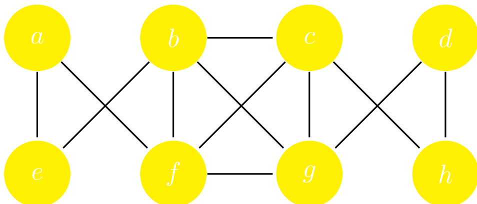
4. Каква е максималната степен на графа G.

5. Докажете, че ако $n \geq 2$, то в G има поне два върха с равна степен.

6. Докажете, че ако $|E| \geq \frac{(n-1)(n-2)}{2}$, то G е свързан.

Задача 3. Намерете Ойлеров цикъл в G, зададен гарфично:

1. 

2. 

Задача 4. Намерете Хамилтонов цикъл в четиримерния булев граф B_4.

Задача 5. Нека $D = (V, E)$ е кореново дърво. Докажете, че:

1. $|V| = |E| + 1$.

2. Ако $|V| \geq 2$, то в D има поне два върха със степен 1.

3. Ако в D има връх със степен k, то в D има поне k върха със степен 1.

Задача 6. Графът G е зададен с помощта на списък на съседство. Намерете покриващи дърво с обхождане на графа в дълбочина и в широчина.

1.

1	$\rightarrow$	2	4	5
2	$\rightarrow$	1	3	4
3	$\rightarrow$	2	4	5
4	$\rightarrow$	1	2	3
5	$\rightarrow$	1	3	6
6	$\rightarrow$	6		

2.

1	$\rightarrow$	2	4	6	8
2	$\rightarrow$	1	8		
3	$\rightarrow$	5	8		
4	$\rightarrow$	1			
5	$\rightarrow$	3	6	7	
6	$\rightarrow$	1	5		
7	$\rightarrow$	5	8		
8	$\rightarrow$	1	2	3	7

Библиография

[1] *Г. Гаврилов и А. Сапоженко 2005: Задачи и упражнения по дискретной математике, ФИЗМАТЛИТ, Москва.*

[2] *К. Манев 2005: Увод в дискретната математика, Четвърто издание, КЛМН, София.*

[3] *J. Matousek and J.Nesetril* 2009 : *Invitation to Dicrete Mathematics, Oxford University Press.*