

Записки по Дискретни структури

15 декември 2022 г.

Съдържание

1	Тема 1	6
1.1	Съждителна логика - съждения, логически съюзи	6
1.2	Еквивалентност на съставни съждения	9
1.3	Методи за доказателство на еквивалентност	9
1.4	Основни свойства на логическите съюзи	10
1.5	Основи на предикатната логика	11
1.6	Свойства на отрицанието в предикатната логика	13
2	Тема 2	14
2.1	Аксиома за обема	14
2.2	Аксиома за отделянето	14
2.3	Аксиома за степенното множество	15
2.4	Минималност и максималност по включване	15
2.5	Операции върху множества	16
2.6	Основни свойства на операциите върху множества	16
2.7	Покриване и разбиване на множество	18
2.8	Диаграми на Venn	18
3	Тема 3	20
3.1	Индуктивно дефинирани множества	20
3.2	Доказателства по индукция - обикновена, силна, структур- на. Примери	20
3.3	Наредена двойка. Декартово произведение	21
4	Тема 4	22
4.1	Релации	22
4.2	Двуместни релации над декартови квадрати и представяне чрез матрици и графи (диаграми)	22
4.3	Свойства на двуместни релации	23
4.4	Затваряния на релации	23
4.5	Релации на еквивалентност	24
4.6	Теорема за класовете на еквивалентност	24
5	Тема 5	26
5.1	Частични наредби	26
5.2	Линейни наредби	26
5.3	Вериги и контури в релации	26
5.4	Теорема за контурите	26
5.5	Влагане на частична наредба в линейна наредба	27

6	Тема 6	28
6.1	Функции – частични и тотални	28
6.2	Еднозначна функция, сюрекция, биекция, обратна функция	28
6.3	Крайни множества и брой на елементите. Безкрайни из- броими множества	29
6.4	Теорема за съществуване на неизброимо (безкрайно) мно- жество	30
7	Тема 7	31
7.1	Теорема за мощността на декартовото произведение на две изброимо безкрайни множества	31
7.2	Теорема за за мощността на степенното множество на из- броимо безкрайно множество	31
7.3	Теорема за за съществуване на минимален и максимален елемент във всяка крайна частична наредба	32
7.4	Теорема за за разширяване (влагане) на крайна частична наредба до пълна	32
8	Тема 8	34
8.1	Принципи на изброителната комбинаторика	34
8.2	Принцип на включването и изключването	34
9	Тема 9	38
9.1	Основни комбинаторни конфигурации и формули за броя на елементите им	38
9.2	Биномен коефициент. Основни свойства	40
9.3	Теорема на Нютон	41
9.4	Д-ва на комбинаторни твърдения с комбинаторни разсъж- дения	42
10	Тема 10	43
10.1	Рекурентни уравнения (РУ) - линейни с константни кое- фициенти и крайна история – хомогенни и нехомогенни. Примери.	43
10.2	Примери за броене в комбинаториката чрез рекурентни уравнения	46
11	Тема 11	47
11.1	Крайни мултиграфи и графи – ориентирани и неориенти- рани. Дефиниции	47

11.2	Полустепени на входа и изхода, маршрути и контури в ориентирани графи	47
11.3	Степени, пътища и цикли в неориентирани графи. Лема за ръкостисканията	48
11.4	Теорема за броя на маршрутите със зададена дължина в крайни ориентирани мултиграфи	49
12	Тема 12	51
12.1	Подграфи. Индуцирани подграфи	51
12.2	Свързаност и свързани компоненти в неориентирани графи	52
12.3	Силна и слаба свързаност, силно свързани компоненти в ориентирани графи	53
12.4	Оцветяване на графи	53
12.5	Планарност на графи	54
13	Тема 13	56
13.1	Дървета. Индуктивна и неиндуктивна дефиниция на „дърво“. Еквивалентност на тези две дефиниции	56
13.2	Теорема за: връзката между броя на ребрата и на върховете и за единственост на път между два върха в дърво . .	58
13.3	Коренови дървета. Височина и разклоненост на кореновите дървета. Представяния на дървета	59
13.4	Покриващо дърво. Теорема за съществуване на покриващо дърво	60
14	Тема 14	61
14.1	Обхождания на графи – в дълбочина и ширина. Дърво на обхождането	61
14.2	Ойлерови/Хамилтонови обхождания/графи	62
14.3	Теорема за съществуване на Ойлеров цикъл и Ойлеров път в неориентиран и ориентиран мултиграф	62
15	Тема 15	66
15.1	Тегловни графи. Минимално покриващо дърво на тегловен граф. МПД свойство.	66
15.2	Алгоритми на Прим и Крускал. Коректност на тези алгоритми.	66
16	Тема 16	69
16.1	Най-къси пътища в графи.	69
16.2	Най-къси пътища в тегловни граф.	69

16.3	Алгоритъм на Дейкстра.	70
17	Тема 17	71
17.1	Булеви функции (на една и две променливи). Съществени и несъществени променливи.	71
17.2	Формула над множество булеви функции. Булева функция, съответна на дадена формула.	71
17.3	Свойства на функциите на една и две променливи.	71
18	Тема 18	73
18.1	Пълни множества БФ. Теорема на Бул.	73
18.2	Пълнота на множество БФ чрез свеждане до известно пълно множество.	73
18.3	Литерали, конюнктивни и дизюнктивни клаузи, свършени на ДНФ.	74
18.4	Полиноми на Жегалкин – съществуване, единственост и алгоритми за получаване.	77
19	Тема 19	81
19.1	Функционални елементи. Дефиниция на схема от ФЕ. Построяване на схема от ФЕ от СъвДНФ.	81
19.2	Пример с двоичен суматор	81
20	All you need to know...	83

1 Тема 1

1.1 Съжителна логика - съждения, логически съюзи

В съжителната логика не се допускат "междинни възможности" на частична истинност, т.е. дадено съждение е или истина, или лъжа, друга възможност няма.

Определение. *Просто съждение е просто разказвателно изречение (още се нарича логическа променлива), което е или истина, или лъжа. Въпросителните изречения и възклицанията не са съждения, както и разказвателните изречения, за които не можем да твърдим, че са или истина, или лъжа.*

Пример. "Това изречение е лъжа."

Бележки. Бележим истината с T (или 1), а лъжата с F (или 0), където T и F са **логически константи**.

Определение. *Съставни съждения се образуват от прости съждения, други съставни съждения и логически константи чрез логически съюзи.*

Видове логически съюзи

Нека p и q са съждения.

1. Дизюнкция (съответства на "или" от естествения език)
Бележи се с ' \vee '. Дизюнкцията на p и q е $p \vee q$. Тя е съставно съждение, което е:

- лъжа, ако и p , и q са лъжа,
- истина, във всеки останал случай.

Тоест дизюнкцията е истина тогава и само тогава, когато поне едно от участващите съждения е истина.

Друг начин да се определи е чрез таблица на истинност, в която на всеки ред на таблицата отговаря точно една възможна комбинация от F и T за p и q . Всяко такова "раздаване" на конкретни стойности (F или T) на променливите, се нарича **валюация**. Броят на валюациите при n променливи е 2^n .

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

2. Изключващо или

Бележи се с ' \oplus '. Изключващото или на p и q е $p \oplus q$, което за да бъде истина, се изисква точно едно от участващите съждения да е истина, а другото лъжа.

p	q	$p \oplus q$
0	0	0
0	1	1
1	0	1
1	1	0

3. Конюнкция (съответства на 'и' от естествения език)

Бележи се с ' \wedge '. Конюнкцията на p и q е $p \wedge q$. Тя е съставно съждение, което е:

- истина, ако и p , и q са истина,
- лъжа, във всеки останал случай.

Тоест конюнкцията е истина тогава и само тогава, когато всички участващи съждения са истина.

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

4. Импликация (съответства на "ако ..., то ...")

Бележи се с ' \rightarrow '. Импликацията на p и q е $p \rightarrow q$ (чете се " p импликация q "). Тя е съставно съждение, което е:

- лъжа, ако p е истина и q е лъжа,
- истина, във всеки останал случай.

Съждението p се нарича антецедент и е свързан с достатъчността, q се нарича консеквент и е свързан с необходимостта.

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

5. Би-импликация

Бележи се с ' \leftrightarrow '. Би-импликацията на p и q е $p \leftrightarrow q$ (чете се " p тогава и само тогава, когато q "). Тя е съставно съждение, което е:

- истина, когато p и q имат една и съща логическа стойност,
- лъжа, във всеки останал случай.

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

6. Отрицание (негация)

Бележи се с ' \neg '. Прилага се към едно съждение. Отрицанието на p е $\neg p$, което е:

- лъжа, ако p е истина,
- истина, ако p е лъжа.

p	$\neg p$
0	1
1	0

Приоритети на логическите съюзи (в намаляващ порядък):

1. отрицание
2. конюнкция, дизюнкция
3. импликация, би-импликация

1.2 Еквивалентност на съставни съждения

Определение. Съставно съждение, чиято стойност е T за всяка валоация на простите му съждения, се нарича **тавтология**.

Пример. $p \vee \neg p$

p	$\neg p$	$p \vee \neg p$
0	1	1
1	0	1

Определение. Съставно съждение, чиято стойност е F за всяка валоация на простите му съждения, се нарича **противоречие**.

Пример. $p \wedge \neg p$

p	$\neg p$	$p \wedge \neg p$
0	1	0
1	0	0

Определение. Съставно съждение, чиято стойност е T за поне една валоация и F за поне една валоация на простите му съждения, се нарича **условност**.

Пример. $p \rightarrow q$

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

Определение. За всеки две съставни съждения s и t казваме, че s и t са **еквивалентни** тогава и само тогава, когато $s \leftrightarrow t$ е тавтология. Бележим с ' $s \equiv t$ ' (' \equiv ' не е логически съюз, така че $s \equiv t$ не е съставно съждение).

1.3 Методи за доказателство на еквивалентност

Пример. $(p \rightarrow q) \wedge p \equiv p \wedge q$

- Табличен метод

p	q	$p \rightarrow q$	$(p \rightarrow q) \wedge q$	$p \wedge q$
0	0	1	0	0
0	1	1	0	0
1	0	0	0	0
1	1	1	1	1

- *Метод чрез еквивалентни преобразувания*
 $(p \rightarrow q) \wedge p \equiv //$ св-во на импликацията
 $(\neg p \vee q) \wedge p \equiv //$ дистрибутивност
 $(\neg p \wedge p) \vee (q \wedge p) \equiv //$ св-во на отрицанието
 $F \vee (q \wedge p) \equiv //$ св-во на константите
 $(q \wedge p) \equiv //$ комутативност
 $p \wedge q$

1.4 Основни свойства на логическите съюзи

Нека p , q и r са произволни съждения. Тогава следните свойства са в сила:

1. Свойство на константите

- $p \wedge T \equiv p$
- $p \wedge F \equiv F$
- $p \vee T \equiv T$
- $p \vee F \equiv p$

2. Свойство на отрицанието

- $p \vee \neg p \equiv T$
- $p \wedge \neg p \equiv F$

3. Идемпотентност

- $p \vee p \equiv p$
- $p \wedge p \equiv p$

4. Закон за двойното отрицание

- $\neg(\neg p) \equiv p$

5. Комутативност

- $p \vee q \equiv q \vee p$

- $p \wedge q \equiv q \wedge p$;
- $p \oplus q \equiv q \oplus p$
- $p \rightarrow q \not\equiv q \rightarrow p$
- $p \iff q \equiv q \iff p$

6. Асоциативност

- $(p \vee q) \vee r \equiv p \vee (q \vee r) \equiv p \vee q \vee r$
- $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r) \equiv p \wedge q \wedge r$

7. Дистрибутивност

- $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
- $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

8. Закони на де Морган

- $\neg(p \wedge q) \equiv \neg p \vee \neg q$
- $\neg(p \vee q) \equiv \neg p \wedge \neg q$

9. Закон за поглъщането

- $p \vee (p \wedge q) \equiv p$
- $p \wedge (p \vee q) \equiv p$

10. Свойство на импликацията

- $p \rightarrow q \equiv \neg p \vee q$

11. Свойствона би-импликацията

- $p \iff q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

1.5 Основи на предикатната логика

Определение. *Едноместен предикат* е съждение, в което има “празно място”, в което празно място се слага обект от някаква предварително зададена област, наречена **домейн**. За всеки обект от домейна предикатът е или истина, или лъжа. Бележим с $P(x)$ (или други главни латински букви), където x е обект от домейна. Сам по себе си $P(x)$ не е нито истина, нито лъжа. Истина или лъжа се получава само след заместване на x с някой обект от областта, като има два случая на такова заместване:

- когато има поне един обект, за който предикатът е истина. Това бележим с $\exists x : P(x)$, където “ \exists ” е **екзистенциален квантор**. Ако обектите от областта са краен брой, да речем a_1, a_2, \dots, a_n , то $\exists x : P(x)$ има смисъл на $P(a_1) \vee P(a_2) \vee \dots \vee P(a_n)$
- когато за всеки обект предикатът е истина. Това бележим с $\forall x : P(x)$, където “ \forall ” е **универсален квантор**. Ако обектите от областта са краен брой, да речем a_1, a_2, \dots, a_n , то $\forall x : P(x)$ има смисъл на $P(a_1) \wedge P(a_2) \wedge \dots \wedge P(a_n)$

Бележки. Когато е използван квантор върху някаква променлива, казваме, че тя е **свързана**. В противен случай, казваме, че тя е **свободна**. Предикат, в който всички променливи са свързани, е **свързание**.

Пример. В израза $\forall x \underbrace{(P(x) \rightarrow Q(x))}_{\text{обхват на квантора}}$, x е свързана променлива.

В израза $\forall x \underbrace{P(x)}_{\text{обхват на квантора}} \rightarrow Q(x)$, x е свободна променлива в $Q(x) \implies Q(x)$ не е нито истина, нито лъжа.

Пример. Отрицания на изрази с едноместни предикати:

- $\neg \forall x P(x) \equiv \exists x \neg P(x)$
- $\neg \exists x P(x) \equiv \forall x \neg P(x)$

Определение. Предикатите могат да имат повече от едно "празно място" за попълване, т.е. да са двуместни, триместни и т.н.

Бележки. В израза $\forall x \forall y P(x, y)$ казваме, че кванторите (които може да са от различен вид) са **вложени**.

Еднотипни квантори могат да бъдат размествани без това да се отразява на истинността, тоест винаги:

- $\forall x \forall y P(x, y) \equiv \forall y \forall x P(x, y)$
- $\exists x \exists y P(x, y) \equiv \exists y \exists x P(x, y)$

От друга страна, разнотипни квантори не може да бъдат размествани, тоест, в общия случай:

- $\forall x \exists y P(x, y) \not\equiv \exists y \forall x P(x, y)$
- $\exists x \forall y P(x, y) \not\equiv \forall x \exists y P(x, y)$

Пример. В израза $\forall x P(x, y)$, y е свободна променлива $\implies P(x, y)$ не е нито истина, нито лъжа.

1.6 Свойства на отрицанието в предикатната логика

Пример. *Негация на израз с много квантори:*

$$\begin{aligned} & \neg(\forall \epsilon > 0 \exists \delta > 0 \forall x (0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon)) \\ & \equiv \\ & \exists \epsilon > 0 \forall \delta > 0 \exists x (0 < |x - a| < \delta \wedge |f(x) - L| \geq \epsilon) \end{aligned}$$

2 Тема 2

Определение. *Множество* е първично понятие, което не се дефинира. Интуитивно го определяме като колекция от различни обекти. Обикновено, но не винаги, имената на множествата са главни латински букви: A, B, \dots . При изреждане на елементите се ползват фигурните скоби $\{ \}$, а имената на елементите са разделени със запетай, например $A = \{a, b, c\}$.

Бележки. Принадлежността към множество се бележи с $'\in'$, а непринадлежността с $'\notin'$, например $a \in \{a, b, c\}; d \notin \{a, b, c\}$.

Множества може да са елементи на други множества.

2.1 Аксиома за обема

Аксиома. Две множества са равни тогава и само тогава, когато съдържат едни и същи елементи, т.е.

$$\forall X \forall Y (\forall z (z \in X \iff z \in Y) \rightarrow X = Y).$$

Бележки. От аксиомата за обема следва, че редът в който са записани елементите на дадено множество, както и наличието на повторения на елементи, е без значение.

Пример. $\{a, b, c\} = \{a, a, b, b, b, c\} = \{a, b, c, b, a\} = \{c, b, a\}$.

2.2 Аксиома за отделянето

Аксиома. С предикат може да отделим подмножество от множество.

Ако X е множество и π е предикат с домейн X , то съвкупността Y от елементите на X , които имат свойството π , е множество:

$$\forall X \exists Y \forall z (z \in Y \iff \pi(z))$$

Нека X е множество, π е предикат над него и $Y = \{x \in X : \pi(x)\}$. Казваме, че Y е **подмножество** (**надмножество**) на X и пишем $Y \subseteq X$ ($X \supseteq Y$).

Имаме следните 2 случая:

- $\forall x \in X : \pi(x)$

Товага $Y = X$. Виждаме, че всяко множество е подмножество на себе си.

- $\neg \exists x \in X : \pi(x) \equiv \forall x \in X : \neg \pi(x)$

Тогава Y е празното множество. Пишем $Y = \emptyset$. Празното множество е подмножество на всяко множество, включително и на себе си.

Бележки. Когато $Y \subseteq X$ ($X \supseteq Y$), но $Y \neq X$ казваме, че Y е **същинско подмножество (надмножество)** на X и пишем $Y \subset X$ ($X \supset Y$), което за да бъде изпълнено, трябва да съществува елемент $x \in X$, такъв че $x \notin Y$.

2.3 Аксиома за степенното множество

Аксиома. За всяко множество X съществува множеството от всички негови подмножества, което наричаме степенното множество на X , т.е.

$$\forall X \exists Y \forall z (z \in Y \iff z \subseteq X).$$

Бележем го с 2^X .

Пример. Ако:

- $X = \emptyset \implies 2^X = \{\emptyset, \emptyset\} = \{\emptyset\}$
- $X = \{a, b, c\} \implies 2^X = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$

2.4 Минималност и максималност по включване

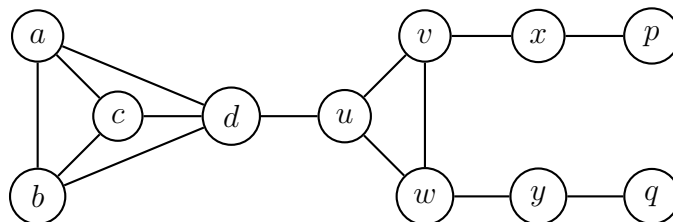
Определение. Нека е дадено множество A и предикат σ върху 2^A . За всяко множество $B \subset A$, казваме, че B е максимално [минимално] по включване по отношение на σ , ако:

1. $\sigma(B)$
2. $\forall C : (B \subset C \subseteq A \rightarrow \neg \sigma(C)) \not\models C : (C \subset B \rightarrow \neg \sigma(C))$

Максимално [минимално] по включване подмножество е такова, за което предикатът е в сила, но той не е в сила за никое негово същинско надмножество [подмножество].

Бележки. За да говорим за максималност и минималност по включване, трябва да имаме предвид предикат. Без предикат, тези понятия нямат смисъл.

Пример. Разграничение между "максимално по включване" (*maximal*) и "глобално максимално" (*maximit*) чрез клика в граф:



Клика в граф е множество от върхове, всеки два от които са свързани с ребро.

Всеки връх е тривиална клика.

Примерни клики са $\{x, p\}$, $\{v, x\}$, $\{u, v, w\}$, $\{a, b, c, d\}$.

Тук $\{a, b, c, d\}$ е най-голямата клика (т.е. максимална клика - отговаря на "глобално максимално") - друга клика с 4 върха няма. Към $\{u, v, w\}$ не може да се добави връх, запазвайки свойството множеството да е клика, т.е. $\{u, v, w\}$ отговаря на "максимално по включване".

2.5 Операции върху множества

Нека X и Y са множества.

- Обединението на X и Y е $X \cup Y = \{x | x \in X \vee x \in Y\}$.
- Сечението на X и Y е $X \cap Y = \{x | x \in X \wedge x \in Y\}$.
- Разликата X и Y е $X \setminus Y = \{x | x \in X \wedge x \notin Y\}$.
- Симетричната разлика то на X и Y е $X \Delta Y = \{x | x \in X \oplus x \in Y\}$.
- Допълнението на X до даден универсум U е $\overline{X^U} = \{x | x \in U \wedge x \notin X\}$.

2.6 Основни свойства на операциите върху множества

Нека X , Y и Z са множества и U е универсум.

1. Свойство на константите

- $X \cup \emptyset = X$
- $X \cup U = U$

- $X \cap \emptyset = \emptyset$
- $X \cap U = X$

2. Свойство на отрицанието

- $X \cup \overline{X} = U$
- $X \cap \overline{X} = \emptyset$

3. Идемпотентност

- $X \cup X = X$
- $X \cap X = X$

4. Закон за двойното отрицание

- $\overline{\overline{X}} = X$

5. Комутативност

- $X \cup Y = Y \cup X$
- $X \cap Y = Y \cap X$
- $X \Delta Y = Y \Delta X$
- $X \setminus Y \neq Y \setminus X$

6. Асоциативност

- $X \cup (Y \cup Z) = (X \cup Y) \cup Z = X \cup Y \cup Z$
- $X \cap (Y \cap Z) = (X \cap Y) \cap Z = X \cap Y \cap Z$

7. Дистрибутивност

- $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$
- $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$

8. Закони на де Морган

- $\overline{X \cup Y} = \overline{X} \cap \overline{Y}$
- $\overline{X \cap Y} = \overline{X} \cup \overline{Y}$

9. Закон за поглъщането

- $X \cup (X \cap Y) = X$
- $X \cap (X \cup Y) = X$

10. Свойство на импликацията

$$\bullet p \rightarrow q \equiv \neg p \vee q$$

11. Свойство на би-импликацията

$$\bullet X \subseteq Y \wedge Y \subseteq X \iff X = Y$$

2.7 Покриване и разбиване на множество

Определение. *Протоелементите са първични елементи, не са множества. Множествата изграждаме от протоеlementи и/или други множества.*

*Множеството от протоеlementите, които може да се появяват, се нарича **опорно множество**.*

*Множество от множества се нарича **фамилия**.*

Пример. $A = \{a, b, c\}$ е опорно множество, а фамилии над него са $X = \{\{a, b\}, \{c\}\}$, $Y = \{\{a, c\}\}$

Определение. *Нека X е непразно множество. **Покриване** на X е всяка фамилия $X = \{X_1, X_2, \dots, X_k\}$ такава, че $k \geq 1$ и:*

$$1. \forall i \in \{1, 2, \dots, k\} : X_i \subseteq X$$

$$2. \forall i \in \{1, 2, \dots, k\} : X_i \neq \emptyset$$

$$3. \cup_{i=1}^k X_i = X$$

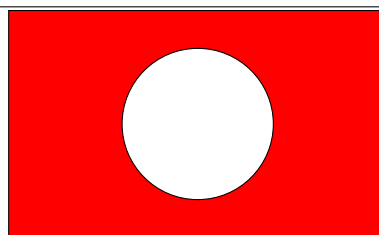
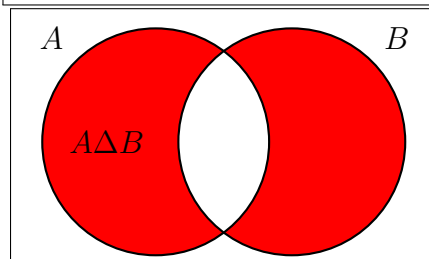
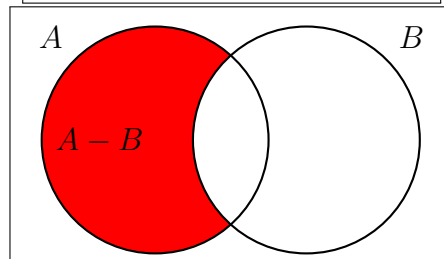
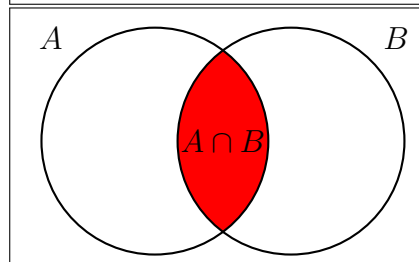
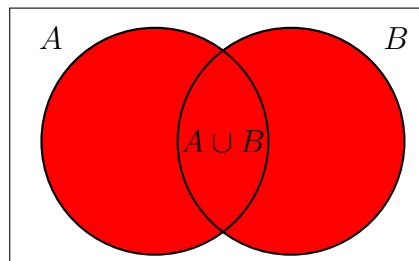
*Ако освен това е вярно и $\forall i \forall j (1 \leq i < j \leq k \rightarrow X_i \cap X_j = \emptyset)$ казваме, че X е **разбиване** на X .*

Пример. *Нека $X = \{x, y, z, t\}$, покриване на X е $\{\{x, y\}, \{y, z, t\}, \{x, z, t\}\}$, разбиване на X е $\{\{x, z\}, \{y\}, \{t\}\}$.*

2.8 Диаграми на Venn

В пълните диаграми на Venn, универсумът винаги присъства. Районите са точно 2^n при n множества.

Общо положение при две множества:



3 Тема 3

3.1 Индуктивно дефинирани множества

Аксиома. Можем да си я представим като безкрайна процедура, която генерира множество, стартирайки от някаква база и прилагайки итеративно дадени операции.

Нека е дадена непразно множество M_0 , което наричаме **базово множество**, и непразно множество от операции F , приложими в тази конструкция.

- Включваме елементите на M_0 в M , т.е. $M \leftarrow M_0$.
- Прилагаме неограничено следното:
 - нека M' е множеството от елементите, които се получават при всевъзможните приложения на операциите от F върху текущото M
 - добавяме M' към M , т.е. $M \leftarrow M \cup M'$

Така полученото M е множество. Пишем $M = (M_0, F)$.

Множества, генерирани чрез безкрайната процедура от аксиомата за индукцията, наричаме **индуктивно генерирани множества**.

Пример. Множеството на естествените числа \mathbb{N}

При него $M_0 = \{0\}$, а F съдържа една единствена операция - добавяне на единица.

3.2 Доказателства по индукция - обикновена, силна, структурна. Примери

Нека е даден предикат $P(n)$ и трябва да докажем $\forall x \in \mathbb{N} : P(n)$.

Схема. Схемата на доказателствата по индукция върху естествените числа е следната:

(База) доказваме $P(0)$, като просто проверяваме истиността на предиката за $n = 0$

(И.П.) допускаме $P(n)$ за произволно $n \in \mathbb{N}$ и въз основа на това допускаме доказваме $P(n + 1)$ (И.С.)

Пример.

Схема. Схемата на доказателствата със силна индукция върху естествените числа е следната:

(База) доказваме $P(0)$, като просто проверяваме истиността на предиката за $n = 0$

(И.П.) допускаме, че за произволно $n \in \mathbb{N}$ са изпълнени $P(0), P(1), \dots, P(n)$

(И.С.) въз основа на тези допускания доказваме $P(n + 1)$

Пример.

Схема. В по-общия случай доказваме предикат $P(x)$, където домейнът е някакво индуктивно дефинирано множество $M = (M_0, F)$. Схемата на доказателство е следната:

(База) за всеки елемент x от M_0 проверяваме истиността на $P(x)$.

(И.П.) допускаме $P(x)$ за произволно $x \in M$

(И.С.) въз основа на това допускане доказваме, че за всеки елемент y , който се получава при прилагането на операциите от F върху текущото M , то $P(y)$ е вярно

Пример.

3.3 Наредена двойка. Декартово произведение

Определение (Дефиниция на Kuratowski). Всяко множество $\{\{a\}, \{a, b\}\}$ наричаме **наредена двойка** с първи елемент a и втори елемент b . Бележим " (a, b) ".

Определение. Нека A и B са множества. **Декартовото произведение** на A и B е множеството $A \times B = \{(a, b) | a \in A \wedge b \in B\}$.

4 Тема 4

4.1 Релации

Определение. Нека $n \geq 1$ и A_1, A_2, \dots, A_n са множества, наречена съответно първи домейн, втори домейн, ..., n -ти домейн. **Релация** над декартовото произведение $A_1 \times A_2 \times \dots \times A_n$ е всяко множество $R \subseteq A_1 \times A_2 \times \dots \times A_n$. Казваме, че R е n -местна или n -арна.

Пример. $<, \leq, >, \geq, =$ са релации над декартовия квадрат \mathbb{R}^2 .

Нека S е множество, \subseteq_S е релация над $2^S \times 2^S$, дефинирана така:

$$\forall a, b \in 2^S : (a, b) \in \subseteq_S \iff a \subseteq b$$

Нека $S = \{a, b\}$. Тогава $(\{a\}, \{a, b\}) \in \subseteq_S, (\{a, b\}, \{a\}) \notin \subseteq_S$ и т.н.

4.2 Двуместни релации над декартови квадрати и представяне чрез матрици и графи (диаграми)

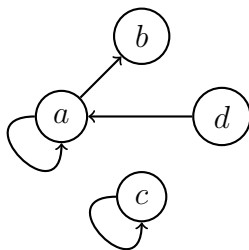
Нека $A = \{a_1, a_2, \dots, a_n\}$ и $R \subseteq A^2$. Например, $A = \{a, b, c, d\}, R = \{(a, a), (a, b), (c, c), (d, a)\}$.

Схема (Представяне чрез матрици). Можем да представим R чрез булева матрица $n \times n$, в която на ред i и колона j е:

- 1, ако $a_i R a_j$
- 0, в противен случай

	a	b	c	d
a	1	1	0	0
b	0	0	0	0
c	0	0	1	0
d	1	0	0	0

Схема (Представяне чрез графи). Можем да представим R чрез диаграма от точки и стрелки, в която на всяко a_i съответства отделна точка, наречена връх, а ребро от връх a_i до връх a_j има тогава и само тогава, когато $a_i R a_j$.



4.3 Свойства на двуместни релации

Нека $R \subseteq A^2$.

1. Рефлексивност
 R е рефлексивна тогава и само тогава, когато $\forall a \in A : aRa$.
2. Антирефлексивност
 R е антирефлексивна тогава и само тогава, когато $\forall a \in A : \neg aRa$.
3. Симетричност
 R е симетрична тогава и само тогава, когато $\forall a, b \in A, a \neq b : aRb \rightarrow bRa$.
4. Антисиметричност
 R е антисиметрична тогава и само тогава, когато $\forall a, b \in A, a \neq b : aRb \rightarrow \neg bRa$.
5. Силна антисиметричност
 R е силно антисиметрична тогава и само тогава, когато $\forall a, b \in A, a \neq b : aRb \oplus bRa$.
6. Транзитивност
 R е транзитивна тогава и само тогава, когато $\forall a, b \in A : aRb \wedge bRc \rightarrow aRc$.

4.4 Затваряния на релации

Определение. *Рефлексивното/симетричното/транзитивното затваряне* на R е минималното множество $R' \subseteq A^2$, такова че $R \subseteq R'$ и R' е рефлексивна/симетрична/транзитивна релация.

" R' е минималното множество" означава, че за всяко $R'' \subseteq A^2$, такова че $R \subseteq R''$ и R'' е рефлексивна/симетрична/транзитивна, е вярно, че $R' \subseteq R''$.

Релация е рефлексивна/симетрична/транзитивна тогава и само тогава, когато съвпада с рефлексивното/симетричното/транзитивното си затваряне.

Допълнение. Нека A е крайно и релациите над A са представени с матрици.

Рефлексивното затваряне се получава с едно сканиране на главния диагонал и обръщане на всяка 0 в 1.

Симетричното затваряне се получава чрез сканиране за двойки $(0; 1)$ и $(1; 0)$, които са симетрично спрямо главния диагонал, и обръщане на 0-та от двойката в 1-ца.

Транзитивното затваряне се получава по-сложно - нещо като умножение на матрицата със себе си $n - 1$ пъти.

4.5 Релации на еквивалентност

Определение. Релация е релация на еквивалентност тогава и само тогава, когато рефлексивна, симетрична и транзитивна.

Пример. $=$ е релация на еквивалентност над реалните числа.

Бележки. Нека $R \subseteq A^2$ е релация на еквивалентност. За всеки елемент $a \in A$ дефинираме множеството $[a] = \{b \in A | aRb\}$.

4.6 Теорема за класовете на еквивалентност

Определение. Семейството $\{[a] | a \in A\}$ е разбиване на A . Елементите на тази фамилия се наричат **класове на еквивалентност**.

Доказателство.

- Всеки елемент на A е в поне един елемент на фамилията, понеже в $\{[a] | a \in A\}$ a взема последователно стойностите на всички елементи от A .
- Всеки елемент на фамилията е непразен, понеже R е рефлексивна.
- Всеки два различни елемента на фамилията имат празно сечение (което ще докажем).

Лема. $[a] \neq [b] \rightarrow [a] \cap [b] = \emptyset$

Доказателство.

Контрапозитивното е $[a] \cap [b] \neq \emptyset \rightarrow [a] = [b]$.

Да допуснем, че $[a] \cap [b] \neq \emptyset$ за някои $a, b \in A$.

Щом $[a] \cap [b] \neq \emptyset$, то $\exists c \in A : c \in [a] \cap [b]$.

Да разгледаме елемент $d \in [a]$. Визуално:

Знаем, че $a \in [a]$ и $b \in [b]$.

От допускането имаме, че (1) $(c \in [a] \implies aRc)$ и (2) $(c \in [b] \implies bRc)$.

По дефиниция $[a] = \{x \in A | aRx\}$.

Тогава:

$aRd \rightarrow dRa$ (симетричност)

$dRa \wedge aRc \rightarrow dRc$ (транзитивност)

cRb (симетричност и (2))

$dRc \wedge cRb \rightarrow dRb$ (транзитивност)

$dRb \implies bRd$ (симетричност)

$bRd \implies d \in [b]$

Доказахме, че $d \in [a] \rightarrow d \in [b]$ за произволен елемент d .

Следователно $[a] \subseteq [b]$.

Аналогично доказваме, че $[b] \subseteq [a]$ и от аксиомата за обема получаваме, че $[a] = [b]$. □

□

5 Тема 5

5.1 Частични наредби

Определение. Релация е релация на частична наредба тогава и само тогава, когато е рефлексивна, антисиметрична и транзитивна.

Пример. $=, \leq, \geq$ над \mathbb{R}^2

Бележки. При частичните наредби може (но не непременно) да има несравними елементи (примерно наредените двойки $(4, 5)$ и $(5, 4)$). Елементи a и b са несравними, ако $\neg aRb$ и $\neg bRa$.

5.2 Линејни наредби

Определение. Релация е релация на линејна наредба тогава и само тогава, когато е рефлексивна, силно антисиметрична и транзитивна.

Бележки. Не може да има несравними елементи заради силната антисиметричност.

Ако $R \subseteq A^2$ е линејна наредба и $A = \{a_1, \dots, a_n\}$, то R има точно $\frac{n(n+1)}{2}$ елемента.

ЛН-и са частен случай на ЧН-и.

5.3 Вериги и контури в релации

Определение. Ако $R \subseteq A^2$ е произволна релация и $A = \{a_1, \dots, a_n\}$, то **верига** в R е всяка редица a_{i_0}, \dots, a_{i_k} , където $i_0, \dots, i_k \in \{1, \dots, n\}$, ако $a_{i_j}Ra_{i_{j+1}}$ за $0 \leq j \leq k-1$. Ограничение за k няма, тоест $k \geq 0$. Тогава един единствен елемент е верига.

Ако $a_{i_0} = a_{i_k}$ и $k > 0$, то веригата е **контур**. Тогава $k > 0$ налага $k > 1$. Един единствен елемент не е контур.

Пример.

5.4 Теорема за контурите

Теорема. Нека $R \subseteq A^2$ е рефлексивна и транзитивна релация. Тогава R е частична наредба тогава и само тогава, когато няма контури.

Доказателство.

\Rightarrow) : Нека R е частична наредба.

Ще докажем, че R няма контури.

Да допуснем, че R има контур $a_{i_0}, a_{i_1}, \dots, a_{i_{k-1}}, a_{i_k} = a_{i_0}$.

От определението за контур и транзитивността на R имаме, че:

$$\begin{aligned} a_{i_0}Ra_{i_1} \wedge a_{i_1}Ra_{i_2} &\implies a_{i_0}Ra_{i_2} \\ a_{i_0}Ra_{i_2} \wedge a_{i_2}Ra_{i_3} &\implies a_{i_0}Ra_{i_3} \\ &\dots \\ a_{i_0}Ra_{i_{k-2}} \wedge a_{i_{k-2}}Ra_{i_{k-1}} &\implies a_{i_0}Ra_{i_{k-1}} \end{aligned}$$

Но тогава имаме, че $a_{i_0}Ra_{i_{k-1}}$ и $a_{i_{k-1}}Ra_{i_0}$ (понеже $a_{i_k} = a_{i_0}$ от определението за контур).

Следователно R не е антисиметрична \implies не е частична наредба $\implies \nexists$

\Leftarrow) : Нека R е няма контури.

Ще докажем, че R е частична наредба.

Допускаме противното - R не е частична наредба.

В началото сме допуснали, че R е рефлексивна и транзитивна и това допускане е в сила.

Тогава за да не е частична наредба, тя не трябва да е антисиметрична.

Щом не е антисиметрична, то задължително съществуват $a, b \in A$, такива че $a \neq b : aRb \wedge bRa$ (не е антисиметрична: $\neg(aRb \rightarrow \neg bRa) \equiv \neg(\neg aRb \vee \neg bRa) \equiv aRb \wedge bRa$).

Но тогава a, b, a е контур \implies противоречие с това, че R няма контури. \square

5.5 Влагане на частична наредба в линейна наредба

Определение. Ако $R \subseteq A^2$ е частична наредба, $R' \subseteq A^2$ е линейна наредба и $R \subseteq R'$, казваме, че R се влага в R' (или че R' е линейно разширение на R).

Бележки. При $A = \{a_1, \dots, a_n\}$, броят на линейните разширения варира от 1 (самата R е линейна наредба) до $n!$ (няма несравними елементи в R).

Допълнение. Нека $R \subseteq A^2$ е частична наредба. За всеки елемент $a \in A$ казваме, че a е **минимален** в R , ако

$$\neg \exists b \in A, b \neq a : bRa \equiv \forall b \in A, b \neq a : \neg bRa.$$

Аналогично, a е **максимален** в R , ако

$$\neg \exists b \in A, b \neq a : aRb \equiv \forall b \in A, b \neq a : \neg aRb.$$

Може да има повече от един минимален и повече от един максимален елемент или да няма нито минимален, нито максимален.

6 Тема 6

6.1 Функции – частични и тотални

Нека X и Y са множества.

Определение. Частична функция с домейн X и кодомейн Y е всяка релация $f \subseteq X \times Y$, такава че за всяко $x \in X$ съществува не повече от едно $y \in Y$, такава че $(x, y) \in f$, т.е.

$$\forall x \in X : ([\neg \exists y \in Y : (x, y) \in f] \vee [(\exists y \in Y : (x, y) \in f) \wedge (\forall w, z \in Y : (x, w) \in f \wedge (x, z) \in f \rightarrow w = z)])$$

Определение. Тотална функция с домейн X и кодомейн Y е всяка релация $f \subseteq X \times Y$, такава че за всяко $x \in X$ съществува точно едно $y \in Y$, такава че $(x, y) \in f$, т.е.

$$\forall x \in X : ([\exists y \in Y : (x, y) \in f] \wedge [\forall w, z \in Y : (x, w) \in f \wedge (x, z) \in f \rightarrow w = z])$$

Бележки. При дадени X и Y , тоталните функции са строго подмножество на частичните. Всяка функция (тотална) е частична функция, но обратното не е вярно.

Формално, функция е вид релация.

6.2 Еднозначна функция, сюрекция, биекция, обратна функция

Нека $f : X \rightarrow Y$. Тогава:

- f е инекция, ако $\forall x_1, x_2 \in X : f(x_1) = f(x_2) \rightarrow x_1 = x_2$
- f е сюрекция, ако $\forall y \in Y \exists x \in X : f(x) = y$. Неформално - кодомейнът да бъде "покрит" от изображението.
- f е биекция, ако е инекция и сюрекция. Още се казва взаимноеднозначно изображение.

Пример. Сядането на хора в зала е частична функция с домейн хората и кодомейн столовете, ако никой не седи на повече от един стол, възможно е да има правостоящи.

Ако няма правостоящи, сядането е функция.

Ако на никой стол не седи повече от един човек, сядането е инекция.

Ако няма празни столове, сядането е сюрекция.

Ако всеки човек седи на отделен стол и няма празни столове, сядането е биекция. Тогава броят на столовете е равен на броя на хората.

Нека $X = \{x_1, x_2, \dots, x_m\}$, $Y = \{y_1, y_2, \dots, y_n\}$ и $f : X \rightarrow Y$.
Необходимо условие f да е:

- инекция е $m \leq n$
- сюрекция е $m \geq n$
- биекция е $m = n$

Иначе казано, при:

- $m > n$ няма инекция
- $m < n$ няма сюрекция
- $m \neq n$ няма биекция

Определение. Нека $f : X \rightarrow Y$ е биекция. **Обратната функция** на f се бележи с f^{-1} . Тя е с домейн Y и кодомейн X и се дефинира така: $\forall y \in Y : f^{-1}(y) = x$, където x е уникалният елемент на X , такъв че $f(x) = y$.

6.3 Крайни множества и брой на елементите. Безкрайни изброими множества

Бележки. Кардиналност (мощност) на множество A е броят на елементите му и се бележи с $|A|$.

Определение. Множество A е **крайно**, ако:

- $A = \emptyset$, тогава $|A| = 0$
- или съществува $n \in \mathbb{N}^+$, такова че съществува биекция $f : A \rightarrow \{1, 2, \dots, n\}$. Тогава $|A| = n$.

Определение. Множество е **безкрайно**, ако не е крайно.

Определение. Множество е **изброимо безкрайно**, ако е равномощно на \mathbb{N} .

Определение. Множество е **изброимо**, ако е крайно или изброимо безкрайно.

Определение. Множество е **неизброимо**, ако не е изброимо.

6.4 Теорема за съществуване на неизброимо (безкрайно) множество

Теорема. *Не съществува биекция $f : 2^{\mathbb{N}} \rightarrow \mathbb{N}$, т.е. $2^{\mathbb{N}}$ е неизброимо.*

Доказателство. Да допуснем, че $2^{\mathbb{N}}$ е изброимо, т.е. съществува биекция $h : 2^{\mathbb{N}} \rightarrow \mathbb{N}$. Ще опровергаем, че характеристичните редици на \mathbb{N} могат да бъдат изброени.

Допускаме изброяване на характеристичните редици: A_0, A_1, \dots , като всяка характеристична редица се появява точно веднъж.

Нека $A_0 = (a_{0,0}, a_{0,1}, \dots)$, $A_1 = (a_{1,0}, a_{1,1}, \dots)$ и т.н.

Представяме си ги написани в безкрайна колона:

$$A_0 = (a_{0,0}, a_{0,1}, a_{0,2}, a_{0,3}, \dots)$$

$$A_1 = (a_{1,0}, a_{1,1}, a_{1,2}, a_{1,3}, \dots)$$

$$A_2 = (a_{2,0}, a_{2,1}, a_{2,2}, a_{2,3}, \dots)$$

$$A_3 = (a_{3,0}, a_{3,1}, a_{3,2}, a_{3,3}, \dots)$$

...

Разглеждаме главния диагонал: редицата $X = (a_{0,0}, a_{1,1}, a_{2,2}, \dots)$.

Образуваме нейната "побитова инверсия", т.е. редицата

$$\bar{X} = (\bar{a}_{0,0}, \bar{a}_{1,1}, \bar{a}_{2,2}, \dots).$$

За всеки $i, j : \bar{a}_{i,j} = 0$, ако $a_{i,j} = 1$ и обратно. Щом всяка булева числова редица се среща в изброяването (колоната), трябва и \bar{X} да се среща. Но \bar{X} не може да е A_0 , защото се различават в поне една позиция - нулевата.

Ако $a_{0,0} = 0$, то $\bar{a}_{0,0} = 1$ и ако $a_{0,0} = 1$, то $\bar{a}_{0,0} = 0$.

Аналогично, \bar{X} не може да е A_1 , защото се различават в първата позиция, \bar{X} не може да е A_2 , защото се различават във втората позиция и т.н.

Тогава \bar{X} не се среща в колоната, иначе казано, подмножеството B на \mathbb{N} , съответстващо на \bar{X} , няма образ в хипотетичната биекция $h : 2^{\mathbb{N}} \rightarrow \mathbb{N}$. \square

Алтернативно доказателство:

Теорема. *За всяко множество A , не съществува сюрекция $g : A \rightarrow 2^A$.*

Доказателство. Да допуснем обратното - съществува множество A , такова че съществува сюрекция $g : A \rightarrow 2^A$.

Разглеждаме множеството $S = \{a \in A \mid a \notin g(a)\}$ (1)

Но $S \in 2^A$ и g е сюрекция, следователно $\exists x \in A : g(x) = S$. Тогава:

- ако $x \in S$, то $x \notin S$ съгласно (1) \implies противоречие
- ако $x \notin S$, то $x \in S$ съгласно (1) \implies противоречие

\square

Бележки.

7 Тема 7

7.1 Теорема за мощността на декартовото произведение на две изброимо безкрайни множества

Теорема. Нека A и B са множества, $|A| = n$, $|B| = m$. Тогава $|A \times B| = n * m$.

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

База: $n = 0$

Тогава $A = \emptyset$ и $\emptyset \times B = \emptyset$. Следователно $|\emptyset \times B| = 0 = 0 * m$.

Индукционно предположение (ИП): нека твърдението е в сила за множество с n елемента, т.е. $A = \{a_1, \dots, a_n\}$ и $B = \{b_1, \dots, b_m\}$, където m е произволно. Тогава $|A \times B| = n * m$.

Индукционна стъпка: ще докажем твърдението за множество с $n + 1$ елемента, т.е. нека $A = \{a_1, \dots, a_n, a_{n+1}\}$ и $B = \{b_1, \dots, b_m\}$, където m е произволно. Тогава

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

Съгласно ИП, $|\{a_1, a_2, \dots, a_n\} \times \{b_1, b_2, \dots, b_m\}| = n * m$

Броят на елементите в множеството $\{a_{n+1}\} \times \{b_1, b_2, \dots, b_m\} = \{(a_{n+1}, b_1), (a_{n+1}, b_2), \dots, (a_{n+1}, b_m)\}$ е m .

Множествата $\{a_1, a_2, \dots, a_n\} \times \{b_1, b_2, \dots, b_m\}$ и $\{a_{n+1}\} \times \{b_1, b_2, \dots, b_m\}$ са непресичащи се, защото елементите на първото множество са наредени двойки с първи елемент различен от a_{n+1} , а елементите на второто множество са наредени двойки с първи елемент a_{n+1} .

Тогава $|A \times B| = n * m + m = (n + 1) * m$. □

7.2 Теорема за мощността на степенното множество на изброимо безкрайно множество

Теорема. Нека A е множество с n на брой елемента. Тогава 2^A има 2^n на брой елемента, т.е. $|2^A| = 2^{|A|} = 2^n$.

Доказателство. Ще докажем твърдението с индукция по n .

База: $n = 0$

Тогава $A = \emptyset$ и $2^\emptyset = \{\emptyset\}$. Следователно $|2^A| = |2^\emptyset| = 2^{|\emptyset|} = 2^0 = 1$.

Индукционно предположение (ИП): нека твърдението е изпълнено за множество с n елемента, т.е. $|A| = n$.

Индукционна стъпка: ще докажем твърдението за множество с $n + 1$ елемента, т.е. $|A| = n + 1$.

Нека $x \in A$. Ще разделим 2^A на две непресичащи се множества:

$$U_0 = \{B | B \subseteq A \wedge x \notin B\} \text{ и } U_1 = \{B | B \subseteq A \wedge x \in B\}.$$

Така $2^A = U_0 \cup U_1$ и съгласно принципа за събирането $|2^A| = |U_0| + |U_1|$.

Имаме, че $B \in U_0 \iff B \subseteq A \setminus \{x\}$. Следователно $U_0 = 2^{A \setminus \{x\}}$, като $A \setminus \{x\}$ е множество с n елемента и съгласно ИП $|U_0| = 2^n$.

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 .

$$\text{Така } |2^A| = |U_0| + |U_1| = 2^n + 2^n = 2^{n+1}. \quad \square$$

7.3 Теорема за съществуване на минимален и максимален елемент във всяка крайна частична наредба

Теорема. Нека A е крайно множество и нека $R \subseteq A^2$ е частична наредба. Тогава R има поне един минимален и поне един максимален елемент.

Доказателство. Да допуснем, че съществува крайно A и поне една частична наредба R над A , такава че R няма минимален елемент.

Избираме произволно $a \in A$. По допускане a не е минимален, така че $\exists b \in A : b \neq a \wedge bRa$.

По допускане b не е минимален, така че $\exists c \in A : c \neq b \wedge cRb$ и т.н.

В общия случай, веригата p , завършваща на a , изглежда така:

$$p = z, \dots, \underbrace{x, \dots, x}_{\text{контур}}, \dots, c, b, a$$

Може x да е a , или b , или c , или z . Тогава в R има контур, което противоречи на това, че в частичните наредби няма контури. Следователно противоречие с допускането. \square

7.4 Теорема за разширяване (влагане) на крайна частична наредба до пълна

Теорема. Нека A е крайно множество, $|A| = n$ и $R \subseteq A^2$ е частична наредба. Тогава съществува поне едно линейно разширение R' на R .

Доказателство (чрез алгоритъма "Топологично сортиране"). Ще построим масив $B[1, \dots, n]$, в който ще разположим елементите на A . Разполагането на елементите на множество в масив задава еднозначно линейна наредба.

Формално, B и R' се свършено различни обекти - най-малкото $|R'| = \frac{n*(n+1)}{2}$. Но R' може да бъде конструирана лесно от B .

Алгоритъм. *Имаме:*

Вход: крайно множество A , $|A| = n$, частична наредба $R \subseteq A^2$

Изход: масив B , реализиращ линейно разширение R' на R

1. $i \leftarrow 1$
2. избираме произволно $a \in A$, който е минимален елемент на R
3. $B[i] \leftarrow a$, изтриваме a от A и от R , правим $i++$
4. ако $i = n + 1$, върни B , в противен случай иди на 2)

□

Бележки. Алгоритъмът е коректен, тъй като в началото има поне един минимален елемент, а при всяко следващо достигане на ред 2) пак има поне един минимален елемент, тъй като изтриване на елемент от релацията не може да образува цикъл, тя остава частична наредба след всяко изтриване на ред 3).

8 Тема 8

8.1 Принципи на изброителната комбинаторика

Принцип (на Дирихле). Ако X и Y са крайни множества и $|X| > |Y|$, то не съществува инекция $f : X \rightarrow Y$.

Алтернативна формулировка: ако има m ябълки в n чекмеджета и $m > n$, то в поне едно чекмедже има повече от една ябълка.

Обобщение: ако има $k \cdot n + 1$ ябълки в n чекмеджета, то в поне едно чекмедже има повече от k ябълки.

Принцип (на биекцията). Нека X и Y са крайни множества. Тогава $|X| = |Y|$ тогава и само тогава, когато съществува биекция $f : X \rightarrow Y$.

Принцип (на събирането (разбиването)). Нека е дадено множество X и разбиване $Y = \{Y_1, \dots, Y_k\}$ на X . Тогава $|X| = |Y_1| + \dots + |Y_k|$.

Това остава в сила дори някои от множествата Y_1, \dots, Y_k да са празни, защото мощностите на празните Y_i са нули и те не се отразяват на сумата.

Принцип (на изваждането). Нека е дадено множество X в универсум U . Тогава $|X| = |U| - |\bar{X}|$.

Очевидно $\{X, \bar{X}\}$ е разбиване на универсума, така че от принципа на събирането имаме, че $|U| = |X| + |\bar{X}|$. Не е възможно \bar{X} да е празно, но дори тогава твърдението остава в сила.

Принцип (на умножението). Нека X и Y са множества. Тогава $|X \times Y| = |X| \cdot |Y|$.

Принцип (на делението). Нека X е множество и $R \subseteq X^2$ е релация на еквивалентност. Нека X има k класа на еквивалентност и всеки клас на еквивалентност има мощност m . Тогава $m = \frac{|X|}{k}$.

8.2 Принцип на включването и изключването

Принцип (на включването и изключването). Нека е дадено покриване на множество и търсим мощността на множеството, като събираме и изваждаме мощностите на дяловете на покриването, техните сечения по двойки, по тройки и т.н.

Обща формулировка: За всяко $n \geq 1$, за всеки n множества A_1, A_2, \dots, A_n :

$$|A_1 \cup \dots \cup A_n| = \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \dots + (-1)^{n-1} |A_1 \cap \dots \cap A_n| \quad (1)$$

Доказателство. С индукция по n :

База: $n = 1$

Тогава (1) става $|A_1| = |A_1|$.

Индукционно предположение: нека твърдението е изпълнено за всеки $n - 1$ множества, т.е.

$$\begin{aligned} |A_1 \cup \dots \cup A_{n-1}| &= \sum_{1 \leq i \leq n-1} |A_i| - \sum_{1 \leq i < j \leq n-1} |A_i \cap A_j| \\ &\quad + \dots + (-1)^{n-2} |A_1 \cap \dots \cap A_{n-1}| \end{aligned} \quad (2)$$

Индукционна стъпка: ще докажем твърдението за всеки n множества.

В сила е

$$\begin{aligned} |A_1 \cup \dots \cup A_{n-1} \cup A_n| &= |\underbrace{(A_1 \cup \dots \cup A_{n-1})}_X \cup \underbrace{A_n}_Y| = \\ &= |\underbrace{(A_1 \cup \dots \cup A_{n-1})}_X| + |\underbrace{A_n}_Y| - |\underbrace{(A_1 \cup \dots \cup A_{n-1})}_X \cap \underbrace{A_n}_Y| \end{aligned} \quad (3)$$

, тъй като $|X \cup Y| = |X| + |Y| - |X \cap Y|$ (от (1) при $n = 2$).

Знаем колко е $|A_1 \cup \dots \cup A_{n-1}|$ от (2).

Да разгледаме $|(A_1 \cup \dots \cup A_{n-1}) \cap A_n|$. В сила е

$$(A_1 \cup \dots \cup A_{n-1}) \cap A_n = (A_1 \cap A_n) \cup \dots \cup (A_{n-1} \cap A_n) \quad (4)$$

заради дистрибутивността на сечението спрямо обединението. Дясната страна на (4) е обобщение на $n - 1$ множества и (2) е приложимо, т.е.:

$$\begin{aligned} |(A_1 \cap A_n) \cup \dots \cup (A_{n-1} \cap A_n)| &= \\ &= \sum_{1 \leq i \leq n-1} |A_i \cap A_n| - \sum_{1 \leq i < j \leq n-1} |(A_i \cap A_n) \cap (A_j \cap A_n)| \\ &\quad + \sum_{1 \leq i < j < k \leq n-1} |(A_i \cap A_n) \cap (A_j \cap A_n) \cap (A_k \cap A_n)| \\ &\quad + \dots + (-1)^{n-2} |(A_1 \cap A_n) \cap \dots \cap (A_{n-1} \cap A_n)| \end{aligned} \quad (5)$$

Получаваме

$$\begin{aligned}
|(A_1 \cup \dots \cup A_{n-1}) \cap A_n| &= \sum_{1 \leq i \leq n-1} |A_i \cap A_n| \\
&- \sum_{1 \leq i < j \leq n-1} |A_i \cap A_j \cap A_n| \\
&+ \sum_{1 \leq i < j < k \leq n-1} |A_i \cap A_j \cap A_k \cap A_n| \\
&\dots \\
&+ (-1)^{n-2} |A_1 \cap A_2 \cap \dots \cap A_{n-1} \cap A_n|
\end{aligned} \tag{6}$$

От (2) и (6) получаваме

$$\begin{aligned}
|A_1 \cup \dots \cup A_{n-1} \cup A_n| &= \\
&(\sum_{1 \leq i \leq n-1} |A_i| - \sum_{1 \leq i < j \leq n-1} |A_i \cap A_j| \\
&+ \dots + (-1)^{n-2} |A_1 \cap \dots \cap A_{n-1}|) \\
&+ |A_n| \\
&- (\sum_{1 \leq i \leq n-1} |A_i \cap A_n| \\
&- \dots + (-1)^{n-2} |A_1 \cap A_2 \cap \dots \cap A_{n-1} \cap A_n|) = \\
&\sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n-1} |A_i \cap A_j| \\
&+ \dots + (-1)^{n-2} |A_1 \cap \dots \cap A_{n-1}| \\
&- \sum_{1 \leq i \leq n-1} |A_i \cap A_n| \\
&+ \dots + (-1)^{n-1} |A_1 \cap A_2 \cap \dots \cap A_{n-1} \cap A_n|
\end{aligned}$$

Групираме събираемите по подходящ начин:

$$\begin{aligned}
|A_1 \cup \dots \cup A_{n-1} \cup A_n| = & \sum_{1 \leq i \leq n} |A_i| - \underbrace{\sum_{1 \leq i < j \leq n-1} |A_i \cap A_j|}_* + \underbrace{\sum_{1 \leq i < j < k \leq n-1} |A_i \cap A_j \cap A_k|}_{**} \\
& + \dots + \underbrace{(-1)^{n-2} |A_1 \cap \dots \cap A_{n-1}|}_{***} \\
& - \underbrace{\sum_{1 \leq i \leq n-1} |A_i \cap A_n|}_* + \underbrace{\sum_{1 \leq i < j \leq n-1} |A_i \cap A_j \cap A_n|}_{**} \\
& - \dots + \\
& + \underbrace{(-1)^{n-2} \sum_{1 \leq i_1 < \dots < i_{n-2} \leq n-1} |A_{i_1} \cap \dots \cap A_{i_{n-2}} \cap A_n|}_{***} \\
& + (-1)^{n-1} |A_1 \cap \dots \cap A_n| = \\
& \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j \leq n} |A_i \cap A_j \cap A_k| \\
& + \dots + (-1)^{n-2} \sum_{1 \leq i_1 < \dots < i_{n-1} \leq n} |A_{i_1} \cap \dots \cap A_{i_{n-1}}| \\
& + (-1)^{n-1} |A_1 \cap \dots \cap A_n| = (1)
\end{aligned}$$

□

Следствие. За всяко $n \geq 1$, за всеки n множества A_1, A_2, \dots, A_n , намиращи се в произволен универсум U :

$$\begin{aligned}
|\overline{A_1} \cap \dots \cap \overline{A_n}| = |U| - \sum_{1 \leq i \leq n} |A_i| + \sum_{1 \leq i < j \leq n} |A_i \cap A_j| \\
- \dots + (-1)^n |A_1 \cap \dots \cap A_n|
\end{aligned} \tag{7}$$

Доказателство. Имаме $|\overline{A_1 \cup \dots \cup A_n}| = |U| - |A_1 \cup \dots \cup A_n|$ от принципа на изваждането. Тогава $|\overline{A_1 \cup \dots \cup A_n}| = |\overline{A_1} \cap \dots \cap \overline{A_n}| = |U| - (1)$ и получаваме точно (7). □

9 Тема 9

9.1 Основни комбинаторни конфигурации и формули за броя на елементите им

Определение (Конфигурации с наредба и повтаряне). Множеството от конфигурациите с наредба и повтаряне с големина m (т.е. броят на елементите в нея) над опорно множество X с мощност n означаваме с " $K_{n,n}(n, m)$ ". Елементите му са наредените m -торки (вектори с дължина m), чиито елементи са от опорното множество X . Тогава $K_{n,n}(n, m) = X^m$.

От обобщения принцип на умножението: $|K_{n,n}(n, m)| = |X^m| = n^m$

Пример. Нека $X = \{a, b, c\}, m = 2$.

Тогава $K_{n,n}(3, 2) = \{(a, a); (a, b); (a, c); (b, a); (b, b); (b, c); (c, a); (c, b); (c, c)\}$ и $|K_{n,n}(3, 2)| = 3^2 = 9$.

Определение (Конфигурации с наредба без повтаряне). Множеството от конфигурациите с наредба без повтаряне с големина m над опорно множество X с мощност n означаваме с " $K_n(n, m)$ ". Елементите му са наредените m -торки без повтаряне, чиито елементи са от опорното множество X .

Процеса на изграждането на някой от тези вектори е следния:

- за първата позиция можем да изберем всеки елемент от X , т.е. имаме n възможности
- за втората позиция имаме $n - 1$ възможности, защото елементът от X , избран за първа позиция, вече не може да се ползва
- аналогично за третата позиция има само $n - 2$ възможности
- и т.н., за m -тата позиция има само $n - (m - 1)$ възможности

Тогава

$$\begin{aligned} |K_n(n, m)| &= n * (n - 1) * (n - 2) * \dots * (n - (m - 1)) \\ &= n * (n - 1) * \dots * (n - m + 1) \\ &= \prod_{k=0}^{m-1} (n - k) = n^{\overline{m}} \end{aligned}$$

¹ $n^{\overline{m}}$ - " n на падаща степен m "

Бележки. Този резултат не се получава от принципа на умножението. Резултатът остава в сила и при $m > n$, тогава дясната страна ще е 0.

Пример. Нека $X = \{a, b, c\}, m = 2$

Тогава $K_n(3, 2) = \{(a, b); (a, c); (b, a); (b, c); (c, a); (c, b)\}$ и $|K_n(3, 2)| = 3 * \dots * (3 - 2 + 1) = 3 * 2 = 6$.

Тук $K_n(3, 2)$ не е Декартово произведение нито на 3-елементно и 2-елементно множество, нито на 6-елементно и 1-елементно множество. Както на първа, така и на втора позиция се срещат и трите елемента на X .

Пример. Нека $X = \{a, b, c\}, m = 4$

Тогава $K_n(3, 2) = \emptyset$, тъй като е невъзможно да не повторим елемент от X съгласно принципа на Дирихле.

Следователно $|K_n(3, 4)| = 3^4 = 3 * 2 * 1 * 0 = 0$.

Частен случай е $n = m$, тогава векторите се наричат пермутации. Пермутациите на n на брой, два по два различни обекта, са разполаганията в линейна наредба на тези обекти. Така $|K_n(n, m)| = |K_n(n, n)| = n!$

Определение (Конфигурации без наредба и без повтаряне). Множеството от конфигурациите без наредба и без повтаряне с големина m над опорно множество X с мощност n означаваме с " $K(n, m)$ ". Елементите му са наредените m -елементните подмножества на опорното множество. Наричат се още комбинации.

Въвеждаме релация $R \subseteq K_n(n, m) \times K_n(n, m)$ така: $\forall X, Y \in K_n(n, m) : XRY \iff X$ и Y имат едни и същи елементи.

R е релация на еквивалентност и всеки нейн клас на еквивалентност има мощност $m!$, а $|K(n, m)|$ е броят на класовете на еквивалентност, като $|K(n, m)| = \frac{K_n(n, m)}{m!} = \frac{n * (n-1) * (n-2) * \dots * (n-m+1)}{m!} = \frac{n!}{m! * (n-m)!}$, което се нарича **биномен коефициент**.

Пример. Колко са възможните фишове при тото 6/49?

Отговор: $\frac{49 * 48 * 47 * 46 * 45 * 44}{6!} = \frac{10068347520}{720} = 13983816$

Причината да делим на $6! = 720$ е, че няма значение в какъв ред се изтеглят числата.

Определение (Конфигурации без наредба с повтаряне). Множеството от конфигурациите без наредба с повтаряне с големина m над опорно множество X с мощност n означаваме с " $K_n(n, m)$ ". Елементите му са мултимножества с големина m на опорното множество. $|K_n(n, m)| = \binom{n-1+m}{n-1} = \binom{n-1+m}{m}$

Пример. Нека $X = \{a, b, c\}, m = 5$. Тогава

$$K_n(3, 5) = \{\{a, a, a, a, a|\},$$

$$\dots,$$

$$\{|b, b, b, b, b|\},$$

$$\{a, a, a, a, |c\},$$

$$\dots,$$

$$\{a, |b, b|, c, c\},$$

$$\{||c, c, c, c, c\}\}$$

$$|K_n(3, 5)| = \binom{3-1+5}{3-1} = \binom{7}{2} = 7 * 3 = 21$$

Пример. 12 еднакви билета се раздават на 10 човека. По колко начина може да стане това?

Р-е: множеството от хората е опорното множество. Броят на билетите е големината на конфигурацията, т.е. $n = 10, m = 12$.

Отговорът е: $\binom{12-1+10}{12} = \binom{12-1+10}{10-1} = 239930$

Едно от раздаванията може да бъде: **|||***||*|*****|*|, където първият човек е с 2 билета, 2-ят, 3-ят и 4-ят са с по 0 билета, 5-ят е с 3, 6-ят е с 0, 7-ят е с 1, 8-ят е с 5, 9-ят е с 1 и 10-ят е без билети.

Пример. Колко са фишовете в 6/49, ако след изтегляне на топка, тя бива връщана отново в сферата?

Отговор: $\binom{49-1+6}{6} = 25827165$

9.2 Биномен коефициент. Основни свойства

Дефинираме е $\binom{n}{m} = \frac{n!}{m!(n-m)!} = \frac{n*(n-1)*...*(n-m+1)}{m!}$ за $n, m \in \mathbb{N}$, което се нарича **биномен коефициент**.

Основни свойства:

- ако $m > n$, то $\binom{n}{m} = 0$, което има комбинаторен смисъл на "има 0 начина да изберем m -елементно подмножество на X , ако $|X| = n$ и $m > n$ "
- $\binom{n}{0} = \binom{n}{n} = 1$, което има комбинаторен смисъл на "има точно 1 начин да изберем 0 нещо от n - не избираме нищо, т.е. избираме \emptyset " и "има точно 1 начин да изберем n неща от n - избираме всичко, т.е. X "
- $\binom{n}{1} = \binom{n}{n-1} = n$, което има комбинаторен смисъл на "има n начина да изберем 1 нещо от n " и "има n начина да изберем $n - 1$ неща от n "

- изобщо, при $m \leq n$, е в сила $\binom{n}{m} = \binom{n}{n-m}$
- при фиксиран горен индекс n , сумата от всички биномни коефициенти е 2^n :

$$\sum_{k=0}^n \binom{n}{k} = \underbrace{\binom{n}{0}}_1 + \underbrace{\binom{n}{1}}_n + \underbrace{\binom{n}{2}}_{\frac{n*(n-1)}{2}} + \dots + \underbrace{\binom{n}{n-2}}_{\frac{n*(n-1)}{2}} + \underbrace{\binom{n}{n-1}}_n + \underbrace{\binom{n}{n}}_1 = 2^n$$

2^n , което има комбинаторен смисъл на "дясната страна брой всички подмножества на n -елементно множество - те са 2^n , а лявата страна брой разбиването на всички подмножества по мощности". Това се извежда с броене на характеристичните вектори с дължина n , които са $|\{0, 1\}^n| = |\{0, 1\}|^n = 2^n$.
- ако $n, m \geq 1$ е в сила $\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$ - триъгърник на Паскал

9.3 Теорема на Нютон

Теорема. $\forall x, y \in \mathbb{R} \forall n \in \mathbb{N} : (x + y)^n = \sum_{k=0}^n \binom{n}{k} * x^k * y^{n-k}$

Доказателство. Лявата страна е $\underbrace{(x + y) * (x + y) * \dots * (x + y)}_{n \text{ множителя}} * (x + y)$

След отварянето на скобите, ще се получи сума от 2^n събираеми от вида $x^k * y^{n-k}$ по всички $k \in \{0, \dots, n\}$. Разбиваме множеството от събираемите в $n + 1$ множества по степента на x (която диктува степента на y): $x^0 * y^n, x^1 * y^{n-1}, \dots, x^n * y^0$. Коефициентът пред $x^k * y^{n-k}$ е броят на появите това събираемо, като съобразяваме, че x^k "идва" от k на брой множителя (останалите множители дават y^{n-k}). Тези k множителя можем да изберем от всички n множителя по $\binom{n}{k}$ начина. Примерно, $x^n * y^0$ се появява само веднъж, понеже за него трябва да "дойде" x от всеки множител, $x^{n-1} * y^1$ се появява точно n пъти, защото от един множител "идва" y , а от останалите - x , като този един множител може да изберем по n начина и т.н. \square

Бележки. Обобщение:

$$(x_1 + \dots + x_k)^n = \sum_{n_1 + \dots + n_k = n} \binom{n!}{n_1! * n_2! * \dots * n_k!} * x_1^{n_1} * \dots * x_k^{n_k}$$

Изразът $\binom{n!}{n_1! * \dots * n_k!}$, където $n_1 + \dots + n_k = n$, има същата стойност като $\binom{n}{n_1} * \binom{n-n_1}{n_2} * \dots * \binom{n-n_1-\dots-n_{k-1}}{n_k}$ се нарича **мултиномен коефициент**. Той брой пермутации с повторения (на мултимножество).

9.4 Д-ва на комбинаторни тъждества с комбинаторни разсъждения

Пример. Ще докажем, че $\binom{2n}{n} = \sum_{k=0}^n \binom{n}{k}^2$.

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

Задачата се свежда до "по колко начина можем да сложим p единици и q нули в редица?".

Общо $p+q$ булеви цифри. Това са характеристичните вектори с дължина $p+q$ и точно p единици. Те съответстват биективно на p -елементните подмножества на $p+q$ -елементно множество. Тези подмножества са $\binom{p+q}{p}$. Тогава и въпросните характеристичните вектори са толкова.

10 Тема 10

10.1 Рекурентни уравнения (РУ) - линейни с константни коефициенти и крайна история – хомогенни и нехомогенни. Примери.

Определение. Уравнението $a_n = c_1 \cdot a_{n-1} + c_2 \cdot a_{n-2} + \dots + c_k \cdot a_{n-k}$, където c_1, \dots, c_k са (целочислени) константи, $c_k \neq 0, k = \text{const}$, се нарича линейно (хомогенно) рекурентно уравнение (ЛХРУ) от k -ти ред с константни коефициенти и крайна история.

Началните условия са k на брой - $a_1 = q_1, \dots, a_k = q_k$, където q_i са цели числа.

Бележки. Уравнението

$$T_n = \begin{cases} n * T_{n-1} & \text{ако } n \geq 1 \\ 1 & \text{ако } n = 0 \end{cases}$$

не е с константни коефициенти.

Уравнението

$$S_n = \begin{cases} S_{n-1} + S_{n-2} + \dots + S_1 + S_0 & \text{ако } n \geq 1 \\ 1 & \text{ако } n = 0 \end{cases}$$

не е с крайна история.

Такива уравнения не могат да се решат със следния алгоритъм:

1. Конструираме характеристичното у-е на даденото ни ЛХРУ

- заместваме a_i с x^i за $i \in n - k, \dots, n$ и получаваме $x^n = c_1 x^{n-1} + c_2 x^{n-2} + \dots + c_{k-1} x^{n-k+1} + c_k x^{n-k}$
- делим на x^{n-k} и получаваме $x^k = c_1 x^{k-1} + c_2 x^{k-2} + \dots + c_{k-1} x + c_k$

Съгласно основната теорема на алгебрата, характеристичното у-е има k на брой, не непременно различни, комплексни корени.

Нека $\{\alpha_1, \dots, \alpha_k\}_M$ е мултимножеството от корените.

- ако корените са два по два различни, то общото решение е $a_n = A_1 \alpha_1^n + \dots + A_k \alpha_k^n$, където A_1, \dots, A_k са неизвестни константи.
 - ако началните условия не са дадени, то не можем да намерим тези константи и решението именно горното у-е

– ако началните условия са дадени (k на брой), то можем да намерим A_1, \dots, A_k , замествайки n със стойностите на аргумента в началните условия. Получаваме система от k линейни уравнения с k неизвестни. Решаваме системата, намираме константите и заместваем в горното у-е.

- нека различните корени са β_1, \dots, β_t за $t \leq k$. Нека β_i има кратност r_i за $1 \leq i \leq t$, като $r_1 + \dots + r_t = k$.

Тогава общото решение е

$$\begin{aligned} a_n = & A_{1,1}\beta_1^n + A_{1,2}n\beta_1^n + \dots + A_{1,r_1}n^{r_1-1}\beta_1^n + \\ & A_{2,1}\beta_2^n + A_{2,2}n\beta_2^n + \dots + A_{2,r_2}n^{r_2-1}\beta_2^n + \\ & \dots + \\ & A_{t,1}\beta_t^n + A_{t,2}n\beta_t^n + \dots + A_{t,r_t}n^{r_t-1}\beta_t^n \end{aligned}$$

Двойно индексиранияте константи $A_{i,j}$ са точно k на брой и може да бъдат намерени от началните условия.

Пример. Нека $a_n = 12a_{n-1} - 51a_{n-2} + 92a_{n-3} - 60a_{n-4}$ с начални условия $a_1 = 1, a_2 = 2, a_3 = 4, a_4 = 6$.

Характеристичното у-е е

$$x^4 - 12x^3 + 51x^2 - 92x + 60 = 0 \iff (x-2)^2(x-3)(x-5) = 0$$

Мултимножеството от корените му е $\{2, 2, 3, 5\}_M$.

Тогава общото му решение е $a_n = A2^n + Bn2^n + C3^n + D5^n$ за константите A, B, C, D .

Константите получаваме от началните условия:

$$\begin{aligned} a_1 &= A.2^1 + B.1.2^1 + C.3^1 + D.5^1 \\ a_2 &= A.2^2 + B.2.2^2 + C.3^2 + D.5^2 \\ a_3 &= A.2^3 + B.3.2^3 + C.3^3 + D.5^3 \\ a_4 &= A.2^4 + B.4.2^4 + C.3^4 + D.5^4 \end{aligned}$$

Знаем началните условия и ги заместваем:

$$\begin{aligned} 1 &= 2.A + 2.B + 3.C + 5.D \\ 2 &= 4.A + 8.B + 9.C + 25.D \\ 4 &= 8.A + 24.B + 27.C + 125.D \\ 6 &= 16.A + 64.B + 81.C + 625.D \end{aligned}$$

Получаваме, че константите са $A = \frac{2}{9}, B = \frac{-1}{6}, C = \frac{1}{3}, D = \frac{-1}{45}$.

Тогава решението е $a_n = \frac{2^{n+1}}{9} - \frac{n.2^n}{6} + 3^{n-1} - \frac{5^n}{45}$.

Определение. Уравнението

$$a_n = \underbrace{c_1 \cdot a_{n-1} + c_2 \cdot a_{n-2} + \dots + c_k \cdot a_{n-k}}_{\text{хомогенна част}} + \underbrace{p_1(n) \cdot b_1^n + \dots + p_l(n) \cdot b_l^n}_{\text{нехомогенна част}}$$

, където k, l, c_1, \dots, c_k са константи, b_1, \dots, b_l са две по две различни константи, а $p_1(n), \dots, p_l(n)$ са полиноми на n , се нарича линейно (нехомогенно) рекурентно уравнение (ЛНХРУ) от k -ти ред с константни коефициенти и крайна история.

Алгоритъм. Прилагаме следните стъпки:

1. Съставя се характеристичното y -е само от хомогенната част и се намира мултимножеството X от корените му.
2. Нека Y е мултимножеството от числата b_1, \dots, b_l , всяко от които има кратност колкото е степента на съответния полином $+ 1$
3. Обединяваме мултимножествата X и Y и съставяме общото решение спрямо това обединение

Бележки. Неизвестните константи се намират чрез началните условия, които са k на брой. Обединението на X и Y има мощност $k + l$, така че неизвестните константи са $k + l$ на брой. За да ги намерим си правим още l начални условия от даденото ни първоначално уравнение.

Пример. Нека

$$L(n) = \begin{cases} L(n-1) + n & \text{ако } n \geq 1 \\ 1 & \text{ако } n = 0 \end{cases}$$

$$\text{Тогава } L(n) = \underbrace{L(n-1)}_{\text{хомогенна част}} + \underbrace{n^1 \cdot 1^n}_{\text{нехомогенна част}}$$

1. Характеристичното y -е е $x - 1 = 0$ и мултимножеството от корените е $X = \{1\}_M$
2. От нехомогенната част образуваме мултимножеството $Y = \{1, 1\}_M$, което съдържа 1-ци, защото основата на експонентата е 1-ца, а броят им е две, защото степента на полинома е едно $+ 1 = 2$.
3. Обединението на X и Y е $\{1, 1, 1\}_M$

Общото решение е $L(n) = A.1^n + B.n.1^n + C.n^2.1^n = A + B.n + C.n^2$.
 За да намерим A, B и C трябва да направим още 2 начални условия,
 освен даденото, т.е. $L(1) = 2, L(2) = 4$ и съставяме системата:

$$\begin{aligned} 1 &= A + B.0 + C.0^2 = A \\ 2 &= A + B.1 + C.1^2 = A + B + C \\ 4 &= A + B.2 + C.4 \end{aligned}$$

Намираме, че $A = 1, B = C = \frac{1}{2}$.
 Тогава $L(n) = 1 + \frac{n+n^2}{2} = 1 + \frac{n.(n+1)}{2}$.

10.2 Примери за броене в комбинаториката чрез рекурентни уравнения

11 Тема 11

11.1 Крайни мултиграфи и графи – ориентирани и неориентирани. Дефиниции

Определение. *Краен неориентиран граф* е наредена двойка $G = (V, E)$, където $V = \{v_1, \dots, v_n\}$ е крайно непразно множество от върхове, $E = \{e_1, \dots, e_m\}$ е крайно множество от ребра, като $E \subseteq \{X \subseteq V : |X| = 2\}$.

Определение. *Краен неориентиран мултиграф* е наредена тройка $G = (V, E, f_G)$, където $V = \{v_1, \dots, v_n\}$ е крайно непразно множество от върхове, $E = \{e_1, \dots, e_m\}$ е крайно множество от ребра, $V \cap E = \emptyset$ и $f_G : E \rightarrow \{X \subseteq V : |X| = 2\}$ е свързваща функция.

Определение. *Краен ориентиран граф* е наредена двойка $G = (V, E)$, където $V = \{v_1, \dots, v_n\}$ е крайно непразно множество от върхове, $E = \{e_1, \dots, e_m\}$ е крайно множество от ребра, като $E \subseteq (V \times V) \setminus \{(v, v) : v \in V\}$.

Определение. *Краен ориентиран мултиграф* е наредена тройка $G = (V, E, f_G)$, където $V = \{v_1, \dots, v_n\}$ е крайно непразно множество от върхове, $E = \{e_1, \dots, e_m\}$ е крайно множество от ребра, $V \cap E = \emptyset$ и $f_G : E \rightarrow V \times V$ е свързваща функция.

Пример. Примери за графи.

11.2 Полустепени на входа и изхода, маршрути и контури в ориентирани графи

Определение. Нека $G = (V, E)$ е ориентиран граф. За всеки връх $v \in V$, **входната степен** (или полустепен на входа) на v е $|\{e \in E : v \text{ е край на } e\}|$, а **изходната степен** (или полустепен на изхода) на v е $|\{e \in E : v \text{ е начало на } e\}|$. Бележим с $d^-(v)$ входната степен, а с $d^+(v)$ изходната степен за $v \in V$.

Определение. *Ориентиран път (маршрут)* в граф G наричаме всяка алтернираща редица от върхове и ребра за някое $t \geq 0$:

$$p = (v_{i_0}, e_{k_0}, v_{i_1}, e_{k_1}, v_{i_2}, \dots, v_{i_{t-1}}, e_{k_{t-1}}, v_{i_t})$$

, където $v_{i_p} \in V$ за $0 \leq p \leq t$, $e_{k_p} \in E$ за $0 \leq p \leq t-1$ и е изпълнено, че $f_G(e_{k_p}) = (v_{i_p}, v_{i_{p+1}})$ за $0 \leq p \leq t-1$. Казваме, че p е път от v_{i_0} до v_{i_t} .

Контур е маршрут, в който първият и последният връх съвпадат.

11.3 Степени, пътища и цикли в неориентирани графи. Лема за ръкостисканията

Определение. Нека $G = (V, E)$ е граф. **Неориентиран път** (или само път) в G наричаме всяка алтернираща редица от върхове и ребра за някое $t \geq 0$:

$$p = (v_{i_0}, e_{k_0}, v_{i_1}, e_{k_1}, v_{i_2}, \dots, v_{i_{t-1}}, e_{k_{t-1}}, v_{i_t})$$

, където $v_{i_p} \in V$ за $0 \leq p \leq t$, $e_{k_p} \in E$ за $0 \leq p \leq t-1$ и е изпълнено, че $e_{k_p} = (v_{i_p}, v_{i_{p+1}})$ за $0 \leq p \leq t-1$.

Бележки. Връх v_{i_0} се нарича начало на пътя, а връх v_{i_t} се нарича край на пътя. Останалите върхове са вътрешните върхове на пътя.

Дължината на пътя е броят на ребрата в него. Бележим я с $|p|$. Ако всички елементи на пътя - върхове и ребра са уникални, казваме, че p е прост (не)ориентиран път.

Определение. Нека $G = (V, E)$ е граф и p е път в него, като:

$$p = (v_{i_0}, e_{k_0}, v_{i_1}, e_{k_1}, v_{i_2}, \dots, v_{i_{t-1}}, e_{k_{t-1}}, v_{i_t}).$$

Казваме, че p е **цикъл**, ако $v_{i_0} = v_{i_t}$.

Казваме, че p е **прост цикъл**, ако p е цикъл с поне едно ребро и освен това - всички елементи са уникални освен $v_{i_0} = v_{i_t}$.

Лема. Нека $G = (V, E)$ е граф с поне 2 върха. Тогава съществуват поне 2 различни върха $u, v \in V$, такива че $d(u) = d(v)$.

Доказателство. За всеки връх $v \in V : d(v) \in \{0, \dots, n-1\}$. Това са n различни стойности.

Да допуснем, че в графа има поне един изолиран връх.

Тогава редицата от степените на върховете в графа започва с 0. Също така няма връх от степен $n-1$ - ако има такъв, то той е съсед на всички останали върхове (включително на изолираните), което противоречи с допускането ни (че имаме изолирани върхове). Покажахме, че няма връх от степен $n-1$.

Тогава $\forall v \in V : d(v) \in \{0, \dots, n-2\}$, което са $n-1$ на брой стойности, а ние имаме n върха.

Тогава от принципа на Дирихле следва, че има поне 2 върха u и v , такива че $d(u) = d(v)$. \square

11.4 Теорема за броя на маршрутите със зададена дължина в крайни ориентирани мултиграфи

Теорема. За всеки ориентиран мултиграф G и за всяко $k \geq 0$ е вярно, че $M^k[i, j]$ е броят на (ориентираните) пътища с дължина k от i до j в G , където M е матрицата на съседство на G .

Доказателство. С индукция по k :

База: $k = 0$

Тогава M^0 е единичната матрица с единици по главния диагонал и нули извън него. Следователно за всички $i, j \in \{1, \dots, n\}$, $M^0[i, j]$ е броят на пътищата с дължина 0 от i до j :

- ако $i \neq j$, такива пътища няма, което точно отговаря на факта, че $M^0[i, j] = 0$
- ако $i = j$, има точно 1 такъв път, а именно самият връх i , което точно отговаря на факта, че $M^0[i, j] = M^0[i, i] = 1$

Индукционно предположение: да допуснем, че твърдението е вярно за стойност на аргумента k , т.е. $M^k[i, j]$ е броят на пътищата с дължина k от i до j .

Индукционна стъпка: ще докажем твърдението за стойност на аргумента $k + 1$.

Нека с $T_{i,j}^l$ означим множеството от пътищата от i до j с дължина $l \geq 0$. Ще докажем, че $M^k[i, j] = |T_{i,j}^k|$ влече $M^{k+1}[i, j] = |T_{i,j}^{k+1}|$ за всички $i, j \in \{1, \dots, n\}$.

(От къде? Защо?) За лявата страна имаме, че

$$M^{k+1}[i, j] = \sum_{1 \leq s \leq n} M^k[i, s] \cdot M[s, j] \quad (8)$$

Да разгледаме дясната страна $|T_{i,j}^{k+1}|$.

Тъй като $k + 1 \geq 1$, всеки път от множеството $T_{i,j}^{k+1}$ има предпоследен връх, при това точно един. Тогава $T_{i,j}^{k+1}$ се разбива на n множества (може да са празни) по предпоследен връх.

Нека с $W_{i,j,s}^l$ означим множеството от пътищата от i до j с предпоследен връх s и дължина $l \geq 1$ за $i, j, s \in \{1, \dots, n\}$. Така $T_{i,j}^{k+1}$ има разбиване $\{W_{i,j,1}^{k+1}, W_{i,j,2}^{k+1}, \dots, W_{i,j,n}^{k+1}\}$, като някои (или всички) дялове на това разбиване може да са празни.

Съгласно принципа на разбиването следва, че

$$|T_{i,j}^{k+1}| = \sum_{1 \leq s \leq n} |W_{i,j,s}^{k+1}| \quad (9)$$

Илюстрация на разбиването на множеството $W_{i,j,s}^{k+1}$: <picture>

Тогава $W_{i,j,s}^{k+1}$ се явява като Декартово произведение на $T_{i,j}^k$ и множеството от ребрата от s до j . Така всеки път от $W_{i,j,s}^{k+1}$ се явява комбинация на един път от $T_{i,s}^k$ и едно ребро от s до j . Тоест броят на начините да стигнем от i до j с точно $k+1$ ребра и s за предпоследен връх е произведението от:

- броя на начините да стигнем от i до s с точно k ребра
- броя на начините да стигнем от s до j с точно 1 ребро

Тогава броят на ребрата от s до j е $M[s, j]$. Следователно

$$|W_{i,j,s}^{k+1}| = |T_{i,s}^k| \cdot M[s, j] \quad (10)$$

От (9) и (10) следва, че $|T_{i,j}^{k+1}| = \sum_{1 \leq s \leq n} |T_{i,s}^k| \cdot M[s, j]$.

От И.П. имаме, че $|T_{i,s}^k| = M^k[i, s]$.

Следователно $|T_{i,j}^{k+1}| = \sum_{1 \leq s \leq n} M^k[i, s] \cdot M[s, j] = M^{k+1}[i, j]$. \square

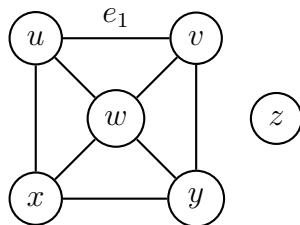
12 Тема 12

12.1 Подграфи. Индуцирани подграфи

Определение. Нека $G = (V, E)$ е граф. **Подграф** на G е всеки граф $G' = (V', E')$, такъв че $V' \subseteq V$ и $E' \subseteq E$.

Бележки. За да бъде G' подграф на G , не е достатъчно да бъде изпълнено $V' \subseteq V$ и $E' \subseteq E$. Всяко ребро в E' трябва да има за краища върхове, които са във V' . Това прави G' граф.

Пример. За графа G_1 имаме негов подграф $H' = (u, v, w, y, z, e_1, e_5)$:



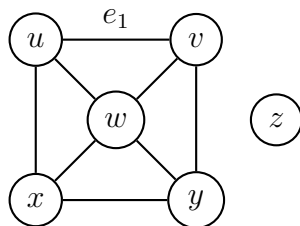
Нека $H'' = (u, v, w, y, z, e_6)$. Тогава H'' не е подграф на G_1 понеже единият край на реброто e_6 , а именно връх x , не е в множеството u, v, w, y, z . С други думи, H'' изобщо не е граф.

Определение. Нека $G = (V, E)$ е граф и $U \subseteq V$. Подграфът на G , **индуциран от U** , е графът $G' = (U, E')$, където $E' = \{(u, v) \in E \mid u \in U \wedge v \in U\}$.

Бележки. Индуцираният подграф е графът, чието множество върхове е U и чието множество ребра са точно тези ребра на G , на които и двата края са в U .

Определение. Нека $G = (V, E)$ е граф и $E' \subseteq E$. Подграфът на G , **индуциран от E'** , е графът $G' = (U, E')$, където $U = \{u \in V \mid \exists e \in E' \exists x \in V : e = (u, x)\}$.

Пример. Нека имаме подм-вото от върхове u, w, y . Тогава подграфът, индуциран от $\{u, w, y\}$, е $(\{u, w, y\}, \{e_2, e_4, e_7\})$.



12.2 Свързаност и свързани компоненти в неориентирани графи

Определение. Нека $G = (V, E)$ е граф. За всеки два върха $u, v \in V$ казваме, че u и v са **свързани**, ако съществува $u - v$ път.

G е **свързан**, ако всеки два върха в него са свързани.

Бележки. Нека $Q_G \subseteq V \times V$ е следната релация:

$$\forall u, v \in V : uQ_Gv \iff u \text{ и } v \text{ са свързани.}$$

Тази релация е **релация на достижимост** в/у G .

Лема. Релацията на достижимост е транзитивна.

Доказателство. Ще покажем, че за всеки 3 върха u, v, w е изпълнено, че ако има $u - v$ път p и $v - w$ път q , то има $u - w$ път r .

Б.О.О., нека p е най-къс $u - v$ път и q е най-къс път $v - w$ път. Нека връх b е най-близкият до връх u в p от $V(p) \cap V(q)$. Тогава b е най-близкият до връх w в q от $V(p) \cap V(q)$. Нека p' е подпътят на p между b и u включително. Тогава $r = p' \cup q$ е прост път между u и w , тъй като $V(p') \cap V(q) = \{b\}$. \square

Бележки. Нека $R_G \subseteq V \times V$ е следната релация:

$$\forall u \in V : uR_Gv \iff u \text{ и } v \text{ са съседни}$$

Тази релация се нарича **релация на съседство** в/у граф G , която е антирефлексивна, симетрична и не е транзитивна.

Лема. Релацията Q_G е рефлексивно и транзитивно затваряне на R_G .

Бележки. Щом R_G е симетрична и Q_G е рефлексивно и транзитивно затваряне на R_G , то Q_G е рефлексивна, симетрична и транзитивна. Тогава Q_G е релация на еквивалентност. Нейните класове на еквивалентност са множества от върхове, във всяко от които всеки два върха са свързани, но никои два върха от различни класове не са свързани.

Определение. Нека $G = (V, E)$ е граф и Q_G е релация на достижимост в/у G . Подграфите на G , индуцирани от класовете на еквивалентност на Q_G , се наричат **свързани компоненти** на G .

Алтернативно определение: свързаните компоненти на граф са максималните по включване свързани графи.

Пример.

12.3 Силна и слаба свързаност, силно свързани компоненти в ориентирани графи

Определение. Нека $G = (V, E)$ е граф. За всеки два върха $u, v \in V$ казваме, че u и v са **свързани**, ако съществува път от u до v и съществува път от v до u .

G е **силно свързан**, ако всеки два върха в него са силно свързани.

Пример.

Бележки. Релацията на силна свързаност е релация на еквивалентност, защото е:

- рефлексивна, защото всеки връх е силно свързан със себе си чрез тривиален път с дължина 0
- симетрична
- транзитивна, защото ако u и v са силно свързани и v и w са силно свързани, то u и w също са силно свързани

Определение. Нека $G = (V, E)$ е ориентиран граф. Подграфите на G , индуцирани от класовете на еквивалентност на релацията на силна свързаност, се наричат **силно свързани компоненти** на G .

Алтернативно определение: **силно свързаните компоненти** са максималните по включване силно свързани подграфи.

Пример.

Определение. Нека $G = (V, E)$ е ориентиран граф. Нека H е съответния му неориентиран граф. Подграфите на G , индуцирани от класовете на еквивалентност на релацията на силна свързаност в/у H , се наричат **слабо свързани компоненти** на G .

Алтернативно определение: **слабо свързаните компоненти** са максималните по включване подграфи на G , м/у върховете на които няма пътища в никаква посока.

Пример.

12.4 Оцветяване на графи

Нека $G = (V, E)$ е граф.

Определение. Оцветяване на върховете на G (или просто оцветяване на G) е функция $f : V \rightarrow C$, където C е множество от цветове и е изпълнено, че $\forall (u, v) \in E : f(u) \neq f(v)$.

Бележки. Има смисъл оцветяването да е сюрекция, за да няма неизползвани цветове.

Определение. Минималният брой цветове, с които можем да оцветим даден граф G , се нарича **хроматично число** на G (бележим го с $\chi(G)$).

Определение. Оцветяване на ребрата на G е ф-я $h : E \rightarrow C$, където C е множество от цветове и е изпълнено, че $\forall e \in E \forall e' \in J(e) : h(e) \neq h(e')$.

Определение. Минималният брой цветове, с които можем да оцветим ребрата на даден граф G , се нарича **хроматичен индекс** на G и се бележи с $\chi'(G)$.

12.5 Планарност на графи

Определение. Планарно вписване на мултиграф е всяка наредена двойка (U, E) , където $U = \{u_1, \dots, u_n\}$ е непразно множество от точки в равнината, наречени планарни върхове, а $E = \{s_1, \dots, s_m\}$ е множество от отворени или затворени криви в равнината, наречени планарни ребра, като трябва да бъдат изпълнени следните условия:

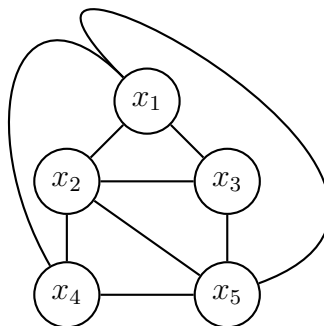
- за всяко планарно ребра, ако е отворена крива, то двата му края съвпадат с точно два от планарните върхове, а ако е затворена крива, то точно една точка от него съвпада с някой планарен връх
- планарните ребра не се пресичат с изключение на това, че може да имат общи планарни върхове

Определение. Нека $G = (V, E)$ е мултиграф. G е планарен тогава и само тогава, когато съществува планарно вписване на мултиграф (U, S) такова, че:

- съществува биекция $\Phi : V \rightarrow U$
- съществува биекция $\Psi : E \rightarrow S$, такава че $\forall e \in E$:
 - ако реброто е не е примка и е инцидентно с върховете x и y , то $\Phi(x)$ и $\Phi(y)$ са краищата на $\Psi(e)$ в равнината.
 - ако реброто е е примка, инцидентна с върха x , то единственият планарен връх, принадлежащ на $\Psi(e)$, е $\Phi(x)$
- за всеки две различни планарни ребра е изпълнено, че нямат общи точки с изключение на общи планарни върхове ???

Определение. Нека G е планарен граф и B е някое негово планарно вписване. Премахването на всички всички планарни върхове и ребра от равнината води до разпадането ѝ на свързани райони, които наричаме лицата на B . Точно едно от лицата е неограничено - външното, а останалите са вътрешните лица.

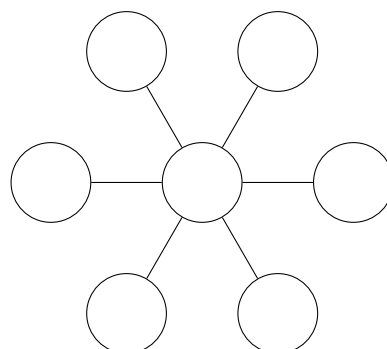
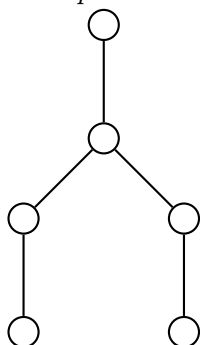
Пример. Например, следното планарно вписване на K_5 — е има лица f_1, \dots, f_6 . Външното лице е f_1 :



13 Тема 13

13.1 Дървета. Индуктивна и неиндуктивна дефиниция на „дърво“. Еквивалентност на тези две дефиниции

Определение (не-индуктивна дефиниция). *Дърво е всеки граф, който е свързан и ацикличен.*



Определение (индуктивна дефиниция). *Множеството от дърветата се дефинира така:*

База: *всеки тривиален граф е дърво.*

Индуктивна стъпка: *ако $T = (V, E)$ е дърво и u е връх в T и w е връх, който не е в T , то $T' = (V \cup \{w\}, \{(u, w)\} \cup E)$ е дърво.*

Лема. *Индуктивна и не-индуктивна дефиниция са еквивалентни.*

Доказателство.

I) Ще докажем, че всеки граф, генериран от индуктивната дефиниция, е свързан и ацикличен.

База: разглеждаме граф $(\{u\}, \emptyset)$, който очевидно е свързан и ацикличен.

Индукционно предположение: допускаме, че $T = (V, E)$ от индуктивната стъпка е свързан и ацикличен.

Индукционна стъпка: за да бъде свързан, трябва за всеки два върха $x, y \in V(T')$ да е изпълнено, че има път между тях. Но $V(T') = V \cup \{w\}$, тогава:

- нито един от x, y не е връх от w . Но тогава е вярно, че $x, y \in V$. Съгласно индуктивното предположение, между всеки два върха в T има път, от което следва, че в T' има път между всеки два върха от V

- точно единият от x и y е връх w . Б.О.О., нека това е връх x . Тогава задължително $y \in V$. Но тогава и y , и w са върхове в T . Съгласно И.П., в T има път p между тях. Тогава p е път между y и u в T' , от което следва, че при слепването на p , реброто (u, w) и върха w се получава път между y и $x = w$ в T' .
- $x = y = w$. Тогава между x и y има тривиален път с дължина 0.

Така доказахме, че T' е свързан.

Нито един връх от T' не може да участва в цикъл, понеже:

- връх w е от степен 1, а всеки връх, който е в цикъл, е от степен поне 2
- останалите върхове на T' са върховете на T , а съгласно И.П. T е ацикличен и добавянето на реброто (u, w) не може да създаде цикъл от върховете на $V(T)$.

Така доказахме, че T' е свързан. Следователно T' е дърво.

II) Ще докажем, че всяко дърво може да бъде конструирано от процедурата на индуктивната дефиниция.

Нека D е произволно дърво съгласно неиндуктивната дефиниция. Ако D има точно един връх, то D може да бъде конструирано от базата на индуктивната дефиниция. В противен случай, в D има поне един висящ връх u_1 .

Нека $D_1 = D - u_1$. Ако D_1 има точно един висящ връх, то D_1 може да бъде конструирано от базата на индуктивната дефиниция. В противен случай, в D_1 има поне един висящ връх u_2 .

Нека $D_2 = D_1 - u_2$. Ако D_2 има точно един връх, то D_2 може да бъде конструирано от базата на индуктивната дефиниция. И т.н.

При всяко от изтриванията на висящ връх, графът остава свързан и ацикличен, тоест дърво. Следователно има редица от дървета D, D_1, D_2, \dots, D_k за някое k . Последователното изтриване на върхове може да се направи само краен брой пъти, защото началното дърво D има краен брой върхове. И така за някое k е вярно, че D има точно един връх. Изтритите върхове са u_1, \dots, u_k в реда на триенето. Тогава графът с точно един връх D_k може да бъде конструирано от базата на индуктивната дефиниция, а след това $|V(D)| - 1$ пъти добавяме изтритите върхове в обратния ред на изтриването им, като свързваме всеки от тях към точно този връх, който е бил единственият му съсед точно преди изтриването. Така получаваме началното дърво D . \square

13.2 Теорема за: връзката между броя на ребрата и на върховете и за единственост на път между два върха в дърво

Теорема (за единственост на път между два върха). *Граф е дърво тогава и само тогава, когато между всеки два върха има точно един път.*

Доказателство.

\Rightarrow) Разглеждаме произволно дърво T и произволни $u, v \in V(T)$. Ще докажем, че има точно един път $u - v$ път.

От свързаността на T следва, че има $u - v$ път, а от това, че е ацикличесен следва, че няма повече от един $u - v$ път.

Да допуснем, че между u и v има поне два пътя p и q . Връх u се явява край и на p , и на q . Разглеждаме p и q като крайни редици от върхове, като търсим първия връх от u нататък, който е различен за p и q . Такъв трябва да има, иначе p и q биха били един и същи път. Б.О.О., нека w е първият връх от u нататък в p , който не се среща в q . Нека a е върхът преди w в посока от u нататък в p , тоест a е последният от u нататък в p , който е общ за p и q . Нека b е първият връх след a в p в посока от u нататък, който е връх и в q . Такъв общ връх трябва да има, понеже p и q имат друг (освен u) общ край, а именно връх v , така че няма как след a , в посока от u нататък, да имат само върхове, които не са общи. Така в p има подпът p' с краища a и b , който не е подпът на q . Аналогично, в q има подпът q' с краища a и b , който не е подпът на p . Единият от p' и q' може да няма вътрешни върхове, но това няма значение. Тогава $p' \cup q'$ е цикъл в T , а в дърветата няма цикли.

Следователно, допускането, че има поне два различни $u - v$ пътя, е грешно.

\Rightarrow) Да разглеждаме произволен граф G , в който между всеки два върха има точно един път. Оттук следва, че G е свързан.

Ако допуснем, че в G има поне един цикъл следва, че в G има поне два върха, между които има два различни пътя, което е невъзможно спрямо направеното допускане, че между всеки два върха има точно един път.

Тогава допускането, че в G съществува цикъл е погрешно. Следователно G е ацикличесен, а оттам и дърво. \square

Теорема (за връзката между броя на ребрата и на върховете). *Във всяко дърво е изпълнено, че $m = n - 1$. (n - брой върхове, m - брой ребра).*

Доказателство. (със структурна индукция)

База: разглеждаме граф само с един връх ($n = 1$) без ребра ($m = 0$). Тогава твърдението е изпълнено $m = n - 1 \iff 0 = 1 - 1 = 0$.

Индукционно предположение: нека твърдението е изпълнено за дървото T , т.е. $|E(T)| = |V(T)| - 1$

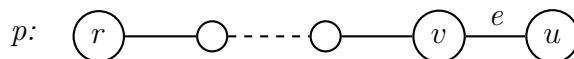
Индукционна стъпка: ще докажем твърдението за дървото T' , т.е. $|E(T')| = |V(T')| - 1$.

Имаме, че $|E(T')| = |E(T)| + 1$ и $|V(T')| = |V(T)| + 1$, откъдето получаваме, че $|E(T)| + 1 = |V(T)| + 1 - 1 \implies |E(T)| = |V(T)| - 1$, което е точно изпълнено за дървото T от И.П. \square

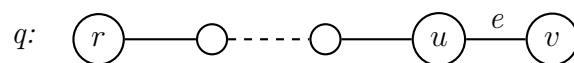
13.3 Коренови дървета. Височина и разклоненост на кореновите дървета. Представяния на дървета

Определение. Нека $T = (V, E)$ е дърво. Избираме произволен връх $r \in V$ и го наричаме **корен**. След избора на корен, T става **кореново дърво**. Изборът на корен еднозначно определя релация на **родителство** върху всяко ребро. Нека $e \in E$ е произволно ребро и нека $e = (u, v)$. Тогава съществува точно един път p между r и u и съществува точно един път q между r и v . Още:

- или $V(p) = V(q) \cup \{u\}$, в който случай v е предпоследният връх преди u в p и казваме, че v е **родителят** на u , а u е **дете** на v :



- или $V(q) = V(p) \cup \{v\}$, в който случай v е предпоследният връх преди v в q и казваме, че u е **родителят** на v , а v е **дете** на u :



Определение. Нека T е кореново дърво с корен r и u произволен връх в него. За всеки връх v казваме, че v е **предшественик** на u , ако v е връх от $u - r$ път. За всеки връх v казваме, че v е **наследник** на u , ако u е предшественик на v .

Определение. Нека T е кореново дърво с корен r . Нека u е произволен връх в T . **Височината** на u е максималното разстояние m/u и u кое да е листо в $T[u]$. Височината на T е височината на r .

Дълбочината на u е разстоянието m/u и r .

Бележки. Поддърво на дърво T , вкоренено във връх w , се смята за кореново дърво с корен w и се бележи с $T[w]$.

Определение. Нека T е кореново дърво. **Разклонеността** на T е максималният брой деца на който да е връх в дървото.

13.4 Покриващо дърво. Теорема за съществуване на покриващо дърво

Определение. Нека $G = (V, E)$ е свързан граф. Покриващо дърво на G е всяко дърво $T = (V, E')$, където $E' \subseteq E$.

Теорема. За всеки граф $G = (V, E)$ има поне едно покриващо дърво тогава и само тогава, когато G е свързан.

Доказателство.

\Rightarrow) Ако G има покриващо дърво, то G е свързан, понеже между всеки два върха има път, което влече съществуване на път между тези два върха на G .

\Leftarrow) Ако G е свързан, то следният алгоритъм строи покриващо дърво на G :

Вход: свързан граф $G = (\{v_1, \dots, v_n\}, E)$

Изход: покриващо дърво на G

1. Ако G няма цикли, върни G и край
2. В противен случай, нека c е произволен цикъл в G и e е произволно ръбро от c
3. Правим $G \leftarrow G - e$ и отиваме на 1)

□

(Д-во за коректност?)

14 Тема 14

Схема (за обхождане на графи). *Имаме:*

Вход: ориентиран мултиграф G

Променливи: m -во от върхове S , връх x и булев масив $visited[1, \dots, n]$

Инициализирай $visited$ с $FALSE$: $S \leftarrow \{1\}, visited[1] \leftarrow TRUE$

1. Ако $S = \emptyset$, прекрати алгоритъма
2. В противен случай, извади елемент от S и го сложи в x
3. За всяко ребро (x, y) , ако $visited[y] = FALSE$:
 - (а) то слагаме y в S и правим $visited[y] \leftarrow TRUE$
 - (б) иначе, прескачаме y
4. Отиваме на 1)

14.1 Обхождания на графи – в дълбочина и ширина. Дърво на обхождането

Описание. *Breadth-First Search (BFS)* е алгоритъм за обхождане на графи в ширина. Изграден е от алгоритмичната схема за обхождане на графи, като m -вото S е реализирано чрез абстрактен тип данни опашка (FIFO). Алгоритъмът започва от даден стартов връх, обхожда неговите съседни, като при това обхожда ребрата, с които ги достига, после обхожда съседите на съседите (различни от стартовия връх), и т.н., обхождайки върховете по нарастване на разстоянията от стартовия връх.

BFS изгражда така нареченото **дърво на обхождане**. Ако графът е неориентиран, то това е покриващо дърво за свързаната компонента, съдържаща стартовия връх, което е кореново дърво с корен стартовия връх, а ребро е от графа влиза в дървото тогава и само тогава, когато *BFS* открива непосетен връх чрез е. С други думи, дървото на обхождане показва как *BFS* е откривал непосетени върхове. Това дърво касае само обхождането на върховете. Всяко ребро бива обхождано от *BFS*, но не всяко ребро влиза в дървото на обхождане.

Описание. *Depth-First Search (DFS)* е алгоритъм за обхождане за на графи (и по-специално дървета) в дълбочина. При него се избира даден връх, който се обозначава като корен (връх без предшественици) и обхождането започва от него. Последователно се посещават всички

следващи върхове до достигането на връх без наследници (листо), след което се осъществява **търсене с връщане назад** до достигане на нова крайна точка или цялостно реализирано обхождане - към корена.

14.2 Ойлерови/Хамилтонови обхождания/графи

Определение. Нека G е неориентиран свързан мултиграф.

Ойлеров цикъл в G е цикъл (не непременно прост), който съдържа всяко ребро точно веднъж.

Ойлеров път в G е път (не непременно прост), който съдържа всяко ребро точно веднъж.

Граф G е **Ойлеров**, ако има Ойлеров цикъл.

Определение. Нека е даден граф G .

Хамилтонов цикъл в G е всеки цикъл в G , който съдържа всички върхове на G .

Хамилтонов път в G е всеки път в G , който съдържа всички върхове на G .

Граф G е **Хамилтонов**, ако има Хамилтонов цикъл.

Бележки. Няма как в един граф едновременно да има Ойлеров път и Ойлеров цикъл.

Ойлеров път (НДУ: графът да е свързан и всички върхове да имат четна степен с изключение на два от тях)

≠

Ойлеров цикъл (НДУ: графът да е свързан и всички върхове да са с четна степен)

14.3 Теорема за съществуване на Ойлеров цикъл и Ойлеров път в неориентиран и ориентиран мултиграф

Теорема (за съществуване на Ойлеров цикъл в неориентиран свързан мултиграф). Неориентиран свързан мултиграф G има Ойлеров цикъл тогава и само тогава, когато всеки връх има четна степен.

Доказателство.

⇒) Да допуснем, че G има Ойлеров цикъл.

Да разгледаме произволен връх $w \in V(G)$. Тогава $w \in V(c)$, където c е Ойлеров цикъл в G .

1. Ако w няма примки, то няма как два съседни върха в c да са w . Следователно, на всяка поява на w в c съответстват точно 2 ребра - съседните елементи на w в цикъла - като за всеки 2 различни появи на w , двете бройки ребра нямат общ елемент. Следователно, множеството от всички тези двойки ребра, върху всички появи на w в c , е точно $J(w)$. Нека w се появява точно t пъти в c . Тогава $|J(w)| = 2.t$. От $d(w) = |J(w)|$ следва, че степента на w е четно число.
2. Нека w има q примки e_1, \dots, e_q и w се появява точно t пъти в c . Тогава $t \geq q$. При наличието на примки на w има съседни появи на w в c , тоест в c има точно q подредици $we_iw, 1 \leq i \leq q$, като някои от тези подредици може да имат общ край w . Всяка такава триелементна подредица, отговаряща на дадена примка, има принос $+2$ към степента на w . Максималните по включване подредици са от вида $we_{j_1}, \dots, e_{j_r}w$, където $e_{j_1}, \dots, e_{j_r} \in \{e_1, \dots, e_q\}$, са точно $t - q$ на брой. Нека E' е м-вото от всички ребра, инцидентни с w , които не са примки. Тъй като тези максимални по включване подредици никога не са съседни, тоест между всеки две от тях в c има поне един връх, който не е w , като $|E'| = 2.(t - q)$. Но $d(w) = |E'| + 2.q = 2.(t - q) + 2.q = 2.t$, което е четно число.

\Leftarrow) Да допуснем, че всеки връх в G е от четна степен.

Ще докажем, че съществува Ойлеров цикъл конструктивно чрез следния алгоритъм:

Алгоритъм (на Hierholtzer). *Имаме:*

Вход: свързан мултиграф G с поне едно ребро

Изход: Ойлеров цикъл c в G

Променливи: w и x - върхове, s - цикъл

1. $c \leftarrow \epsilon$ (празната редица). Маркирай всички ребра на G като неизползвани
2. Избери произволен връх a , инцидентен с неизползвано ребро
3. Присвои $x \leftarrow a, w \leftarrow a, s \leftarrow a$
4. Ако w има поне едно инцидентно неизползвано ребро $e = (w, v)$:
 - (а) присвои $s \leftarrow s, e, v$ и маркирай e като използвано
 - (б) присвои $w \leftarrow v$ и иди на 4)
5. В противен случай, вмъкни s в c , тоест:

- ако s е празен, то присвои $s \leftarrow s$
 - в противен случай s съдържа поне една поява на върха u , който е начало и край на s . Замени коя да е поява на u в s с редицата s
6. Ако няма неизползвани ребра, върни s и прекрати алгоритъма
7. В противен случай, избери произволен връх b от s , инцидентен с неизползвано ребро
8. Присвои $x \leftarrow b, w \leftarrow b, s \leftarrow b$ и иди на 4)

□

Бележки. Идеята на алгоритъма е следната - в началото е неизползвано, а s е празен (празната редица). Използваме временен цикъл s и текущ връх w . Започвайки от произволен връх x , който е инцидентен с поне едно неизползвано ребро, инициализираме $w \leftarrow x, s \leftarrow x$. После изпълняваме, докато е възможно, следното: избираме произволно неизползвано ребро $e \in J(w)$, маркираме e като използвано и "преминаваме" през e , тоест, ако другият край на e е v , добавяме e и v към s като $s \leftarrow s, e, v$, текущият връх w става v , тоест правим $w \leftarrow v$. Правим това, докато можем, а не докато стигнем до текущ връх w , който няма инцидентно необходимо ребро. Тъй като ребрата са краен брой и ние променяме статусите на ребрата от неизползвани в използвани, то рано или късно ще се окажем във връх w , който няма неизползвани инцидентни ребра. В този момент ще точно този връх x , от който започнахме обхождането. В този момент s е цикъл. Вмъкваме s в s . Ако всички ребра са използвани, връщаме s и терминираме алгоритъма. В противен случай продължаваме по следния начин - тъй като G е свързан, в s задължително има връх b , който е инцидентен с поне едно необходимо ребро. Тогава присвояваме $w \leftarrow b, s \leftarrow b$ и отново изпълняваме итерационното добавяне на ребра и върхове към s , докато можем.

Теорема (за съществуване на Ойлеров път в неориентиран свързан мултиграф). Свързан неориентиран мултиграф G има Ойлеров път, който не е цикъл, тогава и само тогава, когато точно 2 върха са от нечетна степен.

Доказателство.

\Rightarrow) Нека G има път p , който съдържа всяко ребро точно веднъж и има различни краища u и v . Ще покажем, че $d(u)$ и $d(v)$ са нечетни, а всички останали върхове имат четни степени.

Имаме $p = u, \dots, v$. Добавяме едно ново ребро e между u и v , получавайки мултиграф G' . Тогава G' има Ойлеров цикъл c , състоящ се от p и новото ребро e , т.е. $c = p, e, u$. Тогава всички върхове в G' са от четна степен. Имаме, че $d_{G'}(u) = d_G(u) + 1, d_{G'}(v) = d_G(v) + 1$ и $\forall x \in V(G) \setminus \{u, v\} : d_{G'}(x) = d_G(x)$, откъдето следва, че $d_G(u)$ и $d_G(v)$ са нечетни, а останалите върхове в G са с четни степени.

\Leftarrow) Нека в G има точно два върха от нечетна степен. Ще покажем, че в G има Ойлеров $u - v$ път.

Добавяме едно ново ребро e между u и v , получавайки мултиграф G'' . Тогава в G'' всички върхове са от четна степен, откъдето следва, че G'' има Ойлеров цикъл c . Изтриваме e от c и получаваме Ойлеров $u - v$ път. \square

Теорема (за съществуване на Ойлеров цикъл в ориентиран свързан мултиграф). *Краен ориентиран свързан мултиграф $G = (V, E, f_G)$ е Ойлеров тогава и само тогава, когато за всеки връх полустепенята на входа и изхода съвпадат.*

Доказателство. (???) Нека ребрата на G образуват Ойлеров цикъл. Тогава за всеки връх полустепенята на входа и изхода съвпадат, защото графът е Ойлеров, а ако не съвпадат, то няма да могат да се обхоят всички ребра. \square

Теорема (за съществуване на Ойлеров път в ориентиран свързан мултиграф). *Краен ориентиран свързан мултиграф $G = (V, E, f_G)$ съдържа Ойлеров път тогава и само тогава, когато само за два от върховете му полустепените на входа и изхода не съвпадат, като в единия връх полустепенята на изхода е с единица по-голяма от полустепенята на входа, а при другия обратно.*

Доказателство. Нека ребрата на G образуват Ойлеров път от v_i до v_j . Добавяме реброто $e \notin E$ и додефинираме $f_{G'}(e) = (v_i, v_j)$. Пътят се превръща в Ойлеров цикъл за новополучения мултиграф G' и следователно в него всички върхове имат еднаква полустепен на входа и изхода. Добавянето на реброто (v_i, v_j) е увеличило с 1 само полустепенята на изхода на v_j и полустепенята на входа на v_i . Следователно в G всички върхове имат еднаква полустепен на входа и изхода, освен два от върховете, за които единия има с единица по-голяма полустепен на входа отколкото на изхода, а при другия обратно. \square

15 Тема 15

15.1 Тегловни графи. Минимално покриващо дърво на тегловен граф. МПД свойство.

Определение. *Тегловен ориентиран мултиграф* е наредена четворка $G = (V, E, f_G, w)$, където V е непразно множество от върхове, E е множество от ребра, $V \cap E = \emptyset$, $f_G : E \rightarrow V \times V$ е свързваща функция и $w : E \rightarrow \mathbb{R}$ е тегловната функция.

Бележки. Стойността $w(e)$ за $e \in E$, наричаме цена или тегло на реброто e .

Цена на покриващо дърво $T = (V, E')$, $E' \subseteq E$ е сумата $w(T) = \sum_{e \in E'} w(e)$

Определение. Покриващото дърво T на G , наричаме **минимално (максимално)**, ако $w(T) \leq w(T')$ (съответно $w(T') \geq w(T)$) за всяко друго покриващо дърво T' на G .

Теорема (МПД-свойство). Нека $G = (V, E)$ е свързан граф с тегловна функция $w : E \rightarrow \mathbb{R}$, $U \subseteq V$, $U \neq \emptyset$ и $e = \{u, v\} \in E$ е такова, че $u \in U$, $v \in V \setminus U$ и измежду всички ребра $e' = \{u', v'\}$ за $u' \in U$, $v' \in V \setminus U$, реброто e е с най-ниска цена, т.е. $w(e) \leq w(e')$. 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 : $u = u_0, u_1, \dots, u_k = v$. 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 $v, u = u_0, u_1, \dots, u_k = v$. Тогава графът $D'' = (V, (E_0 \cup \{e\}) \setminus \{e'\})$ е свързан и има покриващо дърво (V, E_1) , където $e \in E_1 \subseteq (E_0 \setminus \{e'\}) \cup \{e\}$. По условие $w(e) \leq w(e')$, следователно:

$$\sum_{e \in E_1} w(e) \leq \sum_{e \in (E_0 \cup \{e\}) \setminus \{e'\}} w(e) \leq \sum_{e \in E_0} w(e)$$

□

15.2 Алгоритми на Прим и Крускал. Коректност на тези алгоритми.

Алгоритъм (на Прим). Алгоритъмът на Прим строи МПД на G .

Вход: свързан граф $G = (V, E)$ и ф-я $w : E \rightarrow \mathbb{R}$, задаваща тегла на ребрата му

Изход: МПД $D(V, E')$ с корен зададен връх $r \in V$ на G

1. Построяваме дървото $D_0(V_0, E_0)$, $V_0 = \{r\}$, $E_0 = \emptyset$, $k = 0$
2. Нека сме построили $D_k(V_k, E_k)$. Търсим реброто $e = (v_i, v_j)$, $v_i \in V_k$, $v_j \in V \setminus V_k$ с минимално тегло и построяваме $D_{k+1}(V_{k+1}, E_{k+1})$, където $V_{k+1} = V_k \cup \{v_j\}$, $E_{k+1} = E_k \cup \{e\}$ и $k = k + 1$
3. Ако $V_k = V$, то полученото дърво $D(V, E')$, $E' = E_k$ е оптималното и терминираме алгоритъма, иначе отиваме на 2).

Доказателство за коректност. За първата стъпка на алгоритъма избираме $U = \{r\}$. Тогава трябва да изберем най-лекото ребро, излизащо от r и алгоритъмът прави точно това. Щом избраното ребро на тази стъпка може да участва в МПД, значи то образува сигурно за G м-во, а от друга страна е дърво - началото на бъдещото МПД. От тук нататък, нека на всяка стъпка избираме за м-во U върховете V_i на построената до момента част от МПД, а за A - участващите в него ребра E_i . Тогава най-лекото ребро от U към $V \setminus U$ е сигурно за $A = E_i$ и може да продължим с него построяването на МПД. Това гарантира, че построеното от алгоритъма дърво е минимално. \square

Алгоритъм (на Крускал). *Алгоритъмът на Крускал строи МПД на G .*

Вход: свързан граф $G = (V, E)$ и ф-я $w : E \rightarrow \mathbb{R}$, задаваща тегла на ребрата му

Изход: МПД $D = (V, E')$ на G

1. Сортираме ребрата на G в нарастващ ред по цената им и нека този ред е e_1, \dots, e_m
2. От всеки връх v на графа образуваме тривиално дърво $D_V(\{v\}, \emptyset)$.
3. За всяко ребро $e_i = (v_{i_1}, v_{i_2})$, $i \in I_m$ правим следното: ако v_{i_1}, v_{i_2} са в различни дървета, $D'(V', E')$ и $D''(V'', E'')$ съответно, съединяваме двете в дървото $D(V' \cup V'', E' \cup E'' \cup \{(v_{i_1}, v_{i_2})\})$.

Доказателство за коректност. Да допуснем, че алгоритъмът не е коректен, т.е. не съществува дърво с по-малка тегловност от този в алгоритъма.

Нека алгоритъмът бърка за реброто e_t , което е било добавено и свързва две дървета T' и T'' .

1. Алгоритъмът е взел e_t , защото между двете дървета няма друго ребро с по-малка тежест от полученото \implies противоречие с допускането
2. Ако $w(e_i) \neq w(e_j)$ за всяко $i \neq j \implies$ съществува единствено МПД, но ако има ребра с еднаква тежест, то ще има м-во от дървета.

□

16 Тема 16

16.1 Най-къси пътища в графи.

Определение. Нека $G = (V, E)$ е свързан граф, а $w : E \rightarrow \mathbb{R}^+$ е тегловна ϕ -я на ребрата с положителни стойности. **Претеглена дължина** на пътя $p = v_{i_0}, v_{i_1}, \dots, v_{i_t}$ в графа ще наричаме

$$w(p) = \sum_{j=0}^{t-1} w(v_{i_j}, v_{i_{j+1}})$$

Пътят от v_{i_0} до v_{i_t} с най-малка претеглена дължина наричаме **най-къс път** от v_{i_0} до v_{i_t} .

Бележки. За тривиалния път от v до v за всяко $v \in V$ имаме претеглена дължина 0.

16.2 Най-къси пътища в тегловни граф.

Теорема. Нека $G = (V, E)$ е свързан граф с тегловна ϕ -я $w(e) = 1, \forall e \in E$ и D е покриващо дърво на G с корен v_0 , построено в ширина. Пътищата в D от корена до останалите върхове на G са най-къси пътища от върха v_0 до тези върхове.

Доказателство. С индукция по нивата $L_i, i = 0, 1, \dots, t$ на построеното в ширина дърво ще докажем, че дължината на минималния път от корена v_0 до всеки връх от ниво L_i е точно i .

База: Дължината на най-късия път от v_0 до v_0 е 0 и тъй като той е единствен връх в L_0 , то твърдението е в сила за L_0 .

Индукционно предположение: Да допуснем верността за нивата L_0, L_1, \dots, L_i .

Индукционна стъпка Ще покажем, че най-късите пътища от v_0 до всеки връх от L_{i+1} в покриващото дърво са с дължина $i + 1$.

Да допуснем, че $\exists v \in L_{i+1}$, такъв че v_0, \dots, w, v е най-къс път от v_0 до v с дължина $k < i + 1$. Тогава v_0, \dots, w е най-къс път от v_0 до w и дължината му е $k - 1 < i$. Съгласно И.П. $w \in L_{k-1}$ и алгоритъмът трябваше да постави v в $L_k, k < i + 1$, което е противоречие с $v \in L_{i+1}$. Следователно, твърдението е в сила и за L_{i+1} . \square

16.3 Алгоритъм на Дейкстра.

Алгоритъм (на Дейкстра). Алгоритъмът на Дейкстра строи всички най-къси пътища от даден стартов връх до останалите върхове на даден свързан граф.

Вход: свързан граф $G = (V, E)$ с тегловна ф-я по ребрата $w : E \rightarrow \mathbb{R}^+$ и начален връх $v_0 \in V$

Изход: дърво на минималните пътища от v_0 до всички останали върхове в G

1. Разширяваме $w : E \rightarrow \mathbb{R}^+$ до $w^* : V \times V \rightarrow \mathbb{R}^+$
2. Нека $dist[0] = 0, part[0] = -1$ и $U = \{0\}$, а $dist[i] = w^*(0, i)$ и $part[i] = 0$ за $i \in I_n$
3. Повтаряме $n - 1$ пъти следните стъпки:
 - (а) Избираме връх $j \notin U$, за който $dist[j]$ е минимално и $U = U \cup \{j\}$
 - (б) За всяко $k \notin U$ пресмятаме $dist[k] = \min(dist[k], dist[j] + w^*(j, k))$. Ако \min е $dist[j] + w^*(j, k)$, тогава $part[k] = j$.

17 Тема 17

17.1 Булеви функции (на една и две променливи). Съществени и несъществени променливи.

Бележки. $J_2 = \{0, 1\}$, $J_2^n = \underbrace{J_2 \times J_2 \times \dots \times J_2}_{n \text{ множителя}}$

Определение. *Булева ф-я на n променливи е всяка ф-я $f : J_2^n \rightarrow J_2$ за някое $n \geq 1$.*

Булевите ф-ии на 0 променливи се отъждествяват с булевите константи 0 и 1, защото 0-кратното декартово произведение е $()$, откъдето домейнът е едноелементен и има точно две булеви ф-ии на 0 променливи.

Определение. *Нека $f = (x_1, \dots, x_n)$ е булева ф-я.*

*Променливата x_i се нарича **фиктивна (несъществена)**, ако*

$$f(x_1, x_2, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n) = f(x_1, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n)$$

за всяка стойност на $(n - 1)$ -вектора $x_1 x_2 \dots x_{i-1} x_{i+1} \dots x_n$.

*Променлива, която не е фиктивна, се нарича **съществена**.*

17.2 Формула над множество булеви функции. Булева функция, съответна на дадена формула.

17.3 Свойства на функциите на една и две променливи.

1. Комутативност

$$xy = yx$$

$$x \vee y = y \vee x$$

$$x \oplus y = y \oplus x$$

2. Асоциативност

$$(xy)z = x(yz)$$

$$(x \vee y) \vee z = x \vee (y \vee z)$$

$$(x \oplus y) \oplus z = x \oplus (y \oplus z)$$

3. Идемпотентност

$$\begin{aligned}xx &= x \\x \oplus x &= \tilde{0} \\x \vee x &= x\end{aligned}$$

4. Свойство на отрицанието

$$\begin{aligned}x\bar{x} &= \tilde{0} \\x \vee \bar{x} &= \tilde{1} \\x \oplus \bar{x} &= \tilde{1} \\\overline{\bar{x}} &= x\end{aligned}$$

5. Свойство на константите

$$\begin{aligned}x\tilde{0} &= \tilde{0} \\x\tilde{1} &= \tilde{1} \\x \vee \tilde{1} &= \tilde{1} \\x \oplus \tilde{1} &= \bar{x} \\x \oplus \tilde{0} &= x \\x \vee \tilde{0} &= x\end{aligned}$$

6. Закони на де Морган

$$\begin{aligned}\overline{x \vee y} &= \bar{x} \wedge \bar{y} \\\overline{x \wedge y} &= \bar{x} \vee \bar{y}\end{aligned}$$

Бележки. M -вото от всички булеви \mathcal{F} -и на n променливи е F_2^n .

M -вото от всички булеви \mathcal{F} -и е $F_2 = \cup_{n \in \mathbb{N}} F_2^n$.

Елементите на J_2^n са булевите вектори с дължина n . Записваме ги като $a = (a_1, \dots, a_n)$ или $a = a_1 a_2 \dots a_n$.

Нека $x, y \in J_2$, $x = \bar{y}$ тогава и само тогава, когато

18 Тема 18

18.1 Пълни множества БФ. Теорема на Бул.

Определение (неформално). M -вото $F \subseteq F_2$ е **пълно**, ако всяка булева ϕ -я $f \in F_2$ може да бъде представена като композиция на ϕ -ите от F .

Определение (формално). Нека $[F]$ означава затварянето на F спрямо композиция, което може да се дефинира чрез следната индуктивна дефиниция - $[F]$ е най-малкото m -во, такова че:

- $[F]$ съдържа всички ϕ -и от F
- Нека f е ϕ -я, която се съдържа в $[F]$ и има $n \geq 1$ променливи. Нека идентифицираме някои от применливите на f . Получената ϕ -я се съдържа в $[F]$.
- Нека f и g са произволни ϕ -и от $[F]$ и f има $n \geq 1$ променливи. Тогава композицията на g на мястото на i -тата променлива на f също се съдържа в $[F]$ за $1 \leq i \leq n$.

Така F е **пълно m -во**, ако $[F] = F_2$.

Теорема (на Бул). M -вото от трите булеви ϕ -и конюнкция, дизюнкция и отрицание $F = \{\vee, \wedge, \neg\}$ е пълно.

18.2 Пълнота на множество БФ чрез свеждане до известно пълно множество.

Лема. Нека $F, G \subseteq F_2$ са такива, че $F \subseteq [G]$. Тогава $[F] \subseteq [G]$ и G е пълно m -во.

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

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

Нека $G = \cup_{n \in \mathbb{N}} G_n$, където $G_0 = G \cup \{I_k^n | 1 \leq k \leq n\}$ и

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

Ще докажем, че $\forall n : F_n \subseteq [G]$.

По условие имаме, че $F \subseteq [G]$, тогава $\{I_k^n | 1 \leq k \leq n\} \in G_0 \subseteq [G]$. Следователно $F_0 \subseteq [G]$.

Нека $F_n \subseteq [G]$ и $h(x_1, \dots, x_n) = f(g_1(x_1, \dots, x_n), \dots, g_k(x_1, \dots, x_n))$, където $f, g_1, \dots, g_k \in F_n$.

Съгласно И.П. $f \in [G] = \cup_{n \in \mathbb{N}} G_n$. 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 $m = \max(m_0, \dots, m_k)$. Тогава $f, g_1, \dots, g_k \in G_m$ и $h \in G_{m+1}$. Следователно $h \in [G]$ и $F_{n+1} \subseteq [G]$. \square

18.3 Литерали, конюнктивни и дизюнктивни клаузи, свършена ДНФ.

Нека са фиксирани краен брой булеви променливи $x_1, \dots, x_n, n \geq 1$.

Определение. *Литерал* ще наричаме всяко име на променлива (без или с черта отгоре - отрицание). Тези без черта отгоре се наричат положителни, а другите - отрицателни.

Литералите са формули и като такива са качествено различни от самите променливи, понеже формулите са понятия от синтактичното ниво, а променливите са от по-високото - семантичното ниво.

Пример. Положителни литерали са x_1, x_2 и т.н., а отрицателни - $\overline{x_1}, \overline{x_3}$ и т.н.

Определение. *Конюнктивна клауза* е всяка непразна формула, която се състои от конкатенация на литерали, такива че всяко име на променлива се появява най-много веднъж (без значение като положителна или отрицателна).

Пример. Ако x_1, \dots, x_6 са променливи, то конюнктивни клаузи са

$$\begin{aligned} & x_1 x_3 x_5, \\ & x_1 \overline{x_6} \\ & \overline{x_2 x_4 x_6} \end{aligned}$$

и т.н.

Определение. *Дизюнктивна клауза* е всяка непразна формула, която се състои от литерали, свързани чрез дизюнкция, такива че всяко име на променлива се появява най-много веднъж (без значение като положителна или отрицателна).

Пример. Ако x_1, \dots, x_6 са променливи, то дизюнктивни клаузи са

$$\begin{aligned}x_1 \vee x_2 \\ x_1 \vee \overline{x_4} \\ x_3\end{aligned}$$

и т.н.

Определение. *Пълна конюнктивна клауза* е конюнктивна клауза, която съдържа точно n литерала. Тя е непразна формула, която се състои от конкатенация на литерали, такива че всяко име на променлива се среща точно веднъж (без значение като положителна или отрицателна).

Пример. Ако x_1, \dots, x_6 са променливи, то пълни конюнктивни клаузи са

$$\begin{aligned}x_1x_2x_3x_4x_5x_6 \\ x_1x_2x_3x_4x_5\overline{x_6}\end{aligned}$$

и т.н.

Определение. *Пълна дизюнктивна клауза* е дизюнктивна клауза, която съдържа точно n литерала. Тя е непразна формула, която се състои от литерали, свързани чрез дизюнкция, такива че всяко име на променлива се среща точно веднъж (без значение като положителна или отрицателна).

Пример. Ако x_1, \dots, x_6 са променливи, то пълни дизюнктивни клаузи са

$$\begin{aligned}x_1 \vee x_2 \vee \overline{x_3} \vee x_4 \vee x_5 \vee \overline{x_6} \\ x_1 \vee x_2 \vee x_3 \vee x_4 \vee x_5 \vee x_6\end{aligned}$$

Определение. *Конюнктивна нормална форма (КНФ)* е формула, която се състои от една или повече различни конюнктивни клаузи, свързани чрез конюнкция. (Ако дизюнктивните клаузи са повече от една, то всяка от тях се огражда в скоби).

Пример. Ако x_1, \dots, x_6 са променливи, то КНФ са

$$\begin{aligned}x_1 \vee x_2 \vee x_6 \\ (x_1 \vee \overline{x_5})(\overline{x_6} \vee x_1)\end{aligned}$$

и т.н.

Определение. *Дизюнктивна нормална форма (ДНФ)* е формула, която се състои от една или повече различни конюнктивни клаузи, свързани чрез дизюнкция.

Пример. Ако x_1, \dots, x_6 са променливи, то ДНФ са

$$\begin{aligned} & x_2 \overline{x_3} x_4 \\ & x_1 x_4 \vee x_2 \overline{x_5} \vee \overline{x_3} \end{aligned}$$

и т.н.

Определение. *Съвършена конюнктивна нормална форма (Съв-КНФ)* е конюнктивна нормална форма, в която участват само пълни дизюнктивни клаузи.

Пример. Ако x_1, \dots, x_6 са променливи, то СвКНФ са

$$(x_1 \vee x_2 \vee x_3 \vee \overline{x_4} \vee x_5 \vee \overline{x_6})(\overline{x_1} \vee x_2 \vee x_3 \vee x_4 \vee \overline{x_5} \vee x_6)$$

и т.н.

Определение. *Съвършена дизюнктивна нормална форма (Съв-ДНФ)* е дизюнктивна нормална форма, в която участват само пълни конюнктивни клаузи.

Пример. Ако x_1, \dots, x_6 са променливи, то СвДНФ са

$$\begin{aligned} & x_1 x_2 x_3 x_4 x_5 x_6 \vee \overline{x_1} x_2 \overline{x_3} x_4 \overline{x_5} x_6 \\ & \overline{x_1} x_2 \overline{x_3} x_4 \overline{x_5} x_6 \vee x_1 \overline{x_2} x_3 \overline{x_4} x_5 \overline{x_6} \end{aligned}$$

и т.н.

Бележки. Семантиката на литералите, конюнктивните клаузи, ДНФ и КНФ е следната:

- семантиката на всеки положителен литерал x_i е ф-ята идентитет - x_i , а на всеки отрицателен литерал $\overline{x_i}$ е ф-ята отрицание на x_i .
- семантиката на всяка конюнктивна клауза $\lambda_1 \lambda_2 \dots \lambda_k$, където λ_i са литерали за $1 \leq i \leq k$, е композицията на $f_{con}(f_1, f_2, \dots, f_k)$, където f_{con} е обобщената конюнкция на k променливи, а f_i е семантиката на λ_i за $1 \leq i \leq k$.

- семантиката на всяка дизюнктивна клауза $\lambda_1 \vee \lambda_2 \vee \dots \vee \lambda_k$, където λ_i са литерали за $1 \leq i \leq k$, е композицията на $f_{dis}(f_1, f_2, \dots, f_k)$, където f_{dis} е обобщената дизюнкция на k променливи, а f_i е семантиката на λ_i за $1 \leq i \leq k$.
- семантиката на всяка КНФ $(\phi_1)(\phi_2)\dots(\phi_k)$, където ϕ_i е дизюнктивна клауза за $1 \leq i \leq k$, е $f_{con}(f_1, f_2, \dots, f_k)$, където f_{con} е обобщената конюнкция на k променливи, а f_i е семантиката на ϕ_i за $1 \leq i \leq k$.
- семантиката на всяка ДНФ $\phi_1 \vee \phi_2 \vee \dots \vee \phi_k$, където ϕ_i е конюнктивна клауза за $1 \leq i \leq k$, е $f_{dis}(f_1, f_2, \dots, f_k)$, където f_{dis} е обобщената дизюнкция на k променливи, а f_i е семантиката на ϕ_i за $1 \leq i \leq k$.

18.4 Полиноми на Жегалкин – съществуване, единственост и алгоритми за получаване.

Определение. Φ -я 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**.

0	0
1	1
x	x (или $x \oplus 1$)
xy	xy
$x \vee y$	$xy \oplus x \oplus y$
$x \rightarrow y$	$xy \oplus x \oplus 1$
$x \iff y$	$x \oplus y \oplus 1$
$x \oplus y$	$x \oplus y$
$x y$	$xy \oplus 1$
$x \downarrow y$	$xy \oplus x \oplus y \oplus 1$

Теорема (за съществуване и единственост на полинома на Жегалкин).
Всяка булева Φ -я може да се представи по единствен начин чрез полинома на Жегалкин (т.е. има единствен полином на Жегалкин).

Доказателство.

I) Комбинаторно д-во

Нека разгледаме общия вид на полинома на Жегалкин на n променливи:

$$a_0 \oplus \bigoplus_{1 \leq i \leq n} a_i x_i \oplus \bigoplus_{1 \leq i < j \leq n} a_{ij} x_i x_j \oplus \dots \oplus a_{12\dots n} x_1 x_2 \dots x_n$$

Различните ф-ии на n аргумента имат различни представяния чрез полинома на Жегалкин, като различните полиноми се получават от различните стойности на коефициентите, чиито брой е:

- 1 - свободния член
- n - коефициента пред линейните събираеми
- $\binom{n}{3}$ - по един коефициент за всяка тройка променливи
- ...
- $\binom{n}{k}$ - по един за всяка k -торка променливи
- ...
- $\binom{n}{n} = 1$ - пред $x_1 x_2 \dots x_n$

Общо $\sum_{i=0}^k \binom{n}{i} = 2^n$, съгласно теоремата на Нютон. Всеки коефициент може да има стойност 0 или 1. Общо различните полиноми на Жегалкин са 2^{2^n} , колкото и булевите ф-ии. Следователно всяка булева ф-я има единствен полином на Жегалкин.

II) Да допуснем, че f има две различни представяния:

$$\begin{aligned} f(x_1, \dots, x_n) &= a_0 \oplus \bigoplus_{1 \leq i \leq n} a_i x_i \oplus \bigoplus_{1 \leq i < j \leq n} a_{ij} x_i x_j \oplus \dots \oplus a_{12\dots n} x_1 x_2 \dots x_n \\ &= b_0 \oplus \bigoplus_{1 \leq i \leq n} b_i x_i \oplus \bigoplus_{1 \leq i < j \leq n} b_{ij} x_i x_j \oplus \dots \oplus b_{12\dots n} x_1 x_2 \dots x_n \end{aligned}$$

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 $f(c_1, \dots, c_n) = C \oplus a_{i_1 \dots i_k} = C \oplus b_{i_1 \dots i_k}$, което противоречи на допускането, че $a_{i_1 \dots i_k} \neq b_{i_1 \dots i_k}$. \square

Алгоритъм (за получаване на полинома на Жегалкин).

I) от СвДНФ

Негираните променливи се заместват съответно с тяхната ненегирана форма, като всяка от променливите се събира по модул 2 с единица, за да се запази смисълът на формулата (т.е. използва се еквивалентност на негация за $\{\tilde{1}, \tilde{2}, \wedge, \oplus\}$). Тъй като в СвДНФ има само един елемент със стойност единица е допустимо заместването на дизюнкцията със сума по модул 2.

Пример.

$$\begin{aligned}\overline{xy} \vee \overline{x}y \vee xy &= (1 \oplus x)(1 \oplus y) \vee ((1 \oplus x)y) \vee xy \\ &= (1 \oplus x)(1 \oplus y) \oplus (1 \oplus x)y \oplus xy \\ &= 1 \oplus x \oplus y \oplus y \oplus xy \\ &= 1 \oplus x \oplus xy\end{aligned}$$

II) Чрез заместване

Замествайки всички възможни вектори за променливите в общата формула на полинома на Жегалкин се получават коефициентите пред променливите и след това се заместват в общата формула.

Пример.

$$\begin{aligned}f(x, y) &= a_0 + a_1x + a_2y + a_3xy \\ \begin{cases} f(0,0) = & 1 \\ f(0,0) = a_0 \oplus a_1 \cdot 0 \oplus a_2 \cdot 0 \oplus a_3 \cdot 0 \cdot 0 = a_0 \end{cases} & \implies a_0 = 1 \\ \begin{cases} f(0,1) = & 1 \\ f(0,1) = 1 \oplus a_1 \cdot 0 \oplus a_1 \oplus a_3 \cdot 1 \cdot 0 = 1 \oplus a_2 = a_2 \end{cases} & \implies a_2 = 0 \\ \begin{cases} f(1,0) = & 0 \\ f(1,0) = 1 \oplus a_1 \cdot 1 \oplus a_2 \cdot 0 \oplus a_3 \cdot 1 \cdot 0 = 1 \oplus a_1 \end{cases} & \implies a_1 = 1 \\ \begin{cases} f(1,1) = & 1 \\ f(1,1) = 1 \oplus 1 \cdot 1 \oplus 0 \cdot 1 \oplus a_3 \cdot 1 \cdot 1 = 1 \oplus 1 \oplus a_3 = 0 \oplus a_3 \end{cases} & \implies a_3 = 1\end{aligned}$$

Следователно полинома на Жегалкин е $1 \oplus x \oplus xy$.

III) Чрез еквивалентни преобразувания

Дадените операции се заместват с техните съответстващи от $\{\tilde{0}, \tilde{1}, \wedge, \oplus\}$.

Пример.

$$x \rightarrow y \equiv // \text{ св-во на импликацията}$$

$$\bar{x} \vee y \equiv // \text{ закон за двойното отрицание}$$

$$\overline{\bar{x} \vee y} \equiv // \text{ закон на де Морган}$$

$$\overline{\overline{xy}} \equiv // \text{ закон за двойното отрицание}$$

$$\begin{aligned}\overline{xy} &\equiv \overline{x(1 \oplus y)} \equiv 1 \oplus (x(1 \oplus y)) \\ &= 1 \oplus x \oplus xy\end{aligned}$$

19 Тема 19

19.1 Функционални елементи. Дефиниция на схема от ФЕ. Построяване на схема от ФЕ от СъвДНФ.

Нека са дадени устройства, всяко от които има 0 или повече входове и точно един изход. На входовете се подават булеви стойности. За всяка комбинация от булеви стойности на входовете, на изхода "излиза" булева стойност, еднозначно определена от това, което е подадено от входовете.

Определение. Ако броят на входовете е n , то всяко такова устройство реализира някаква булева функция на n променливи, като всеки вход се смята за една булева променлива. Всяко такова устройство се нарича **функционален елемент**.

19.2 Пример с двоичен суматор

Булевите функции в СЪВДНФ:

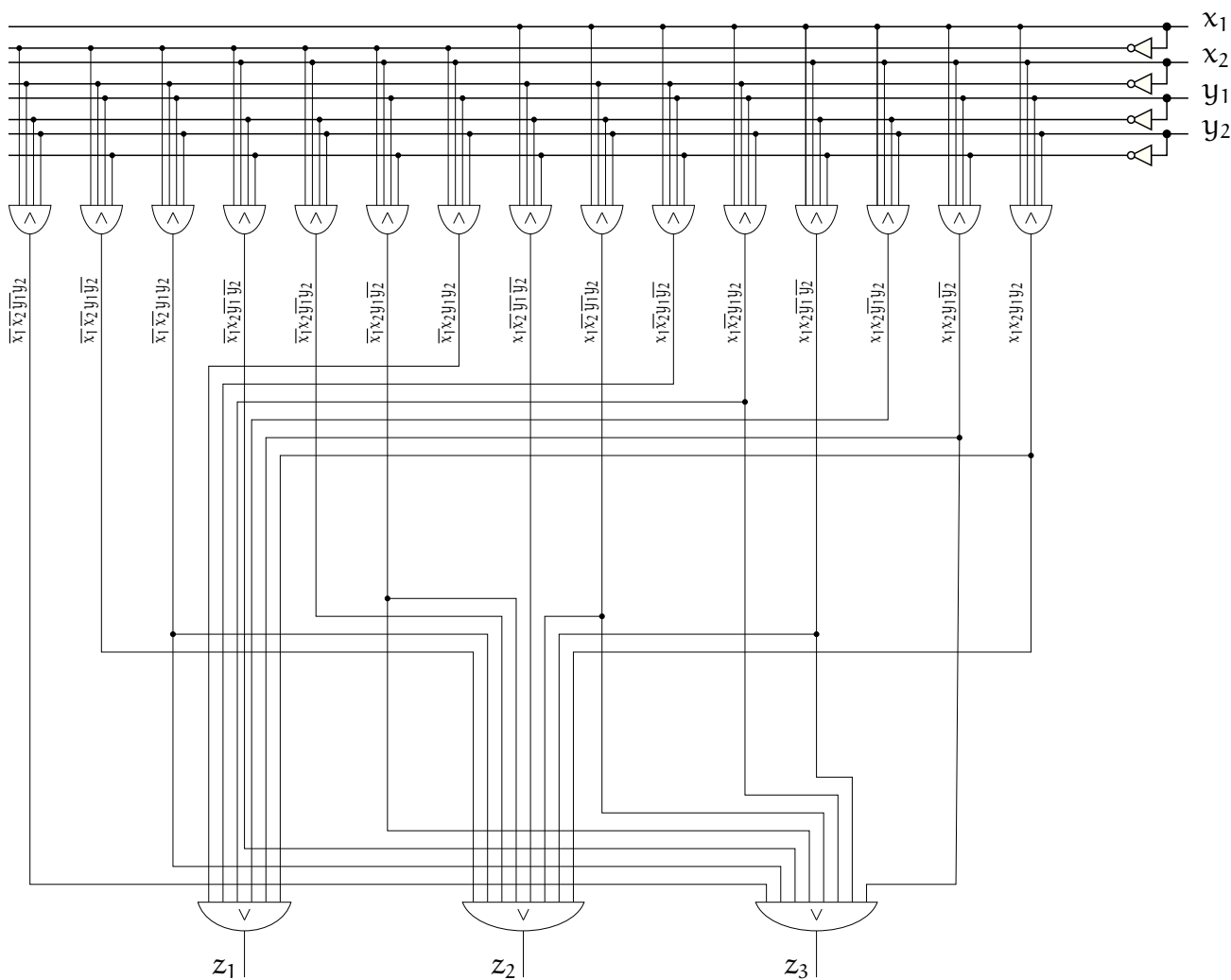
x_1	x_2	y_1	y_2	z_1	z_2	z_3
0	0	0	0	0	0	0
0	0	0	1	0	0	1
0	0	1	0	0	1	0
0	0	1	1	0	1	1
0	1	0	0	0	0	1
0	1	0	1	0	1	0
0	1	1	0	0	1	1
0	1	1	1	1	0	0
1	0	0	0	0	1	0
1	0	0	1	0	1	1
1	0	1	0	1	0	0
1	0	1	1	1	0	1
1	1	0	0	0	1	1
1	1	0	1	1	0	0
1	1	1	0	1	0	1
1	1	1	1	1	1	0

$$z_1 = \overline{x_1}x_2y_1y_2 \vee x_1\overline{x_2}y_1\overline{y_2} \vee x_1\overline{x_2}y_1y_2 \vee x_1x_2\overline{y_1}y_2 \vee x_1x_2y_1\overline{y_2} \vee x_1x_2y_1y_2$$

$$z_2 = \overline{x_1}\overline{x_2}y_1\overline{y_2} \vee \overline{x_1}\overline{x_2}y_1y_2 \vee \overline{x_1}x_2\overline{y_1}y_2 \vee \overline{x_1}x_2y_1\overline{y_2} \vee x_1\overline{x_2}\overline{y_1}\overline{y_2} \vee x_1\overline{x_2}\overline{y_1}y_2 \vee x_1x_2\overline{y_1}\overline{y_2} \vee x_1x_2y_1y_2$$

$$z_3 = \overline{x_1}\overline{x_2}\overline{y_1}y_2 \vee \overline{x_1}\overline{x_2}y_1y_2 \vee \overline{x_1}x_2\overline{y_1}\overline{y_2} \vee \overline{x_1}x_2y_1\overline{y_2} \vee x_1\overline{x_2}\overline{y_1}y_2 \vee x_1\overline{x_2}y_1y_2 \vee x_1x_2\overline{y_1}\overline{y_2} \vee x_1x_2y_1\overline{y_2}$$

Двоичният суматор:



20 All you need to know...

Комбинаторика

Графи