Lybid organization of Khvarints of Ishkiru

Things compilation

Library

Pinky Krista Dvina

Main Department of Galerado
Kacheto-44

17 січня 2025 р.

Зміст

Розділ 1

Introduction

The book is a compilation of different, useful and not, lections from the university. It shoud be a ukrainian book, but there might be some english parts. The main reason is to create a book, which will be staying on a shelf, and collecting dust. My relatives are saing that the university will be useful and knowledge isn't something you will be carign on my back. I want to prove that it is not a true. The main theme of the book is math and cryptography. Hovewer, there will be a lot of monothone useless chapters of some unrelated subjects, only because it was easy to append. If one want to read a useful book on cryptography, just google some other or choose "The graduate course in cryptography" of Boneh et.al. [BS15]. It is a good book.

Розділ 2

Дискретна математика 1

Contents

2.1 Метод математичної індукції.

Definition 2.1.1 (Аксіоматика Парно). *Аксіоматика Парно – це аксіоматика що задовільняє наступним умовам.*

1. $1 \in \mathbb{N}$,
2. $a \in \mathbb{N} \Rightarrow S(a) \in \mathbb{N}$,
3. $\nexists a \in \mathbb{N} : S(a) = 1$,
4. $S(a) = C \wedge S(b) = c \Leftrightarrow a = b$,
5. $P(1) \wedge P(k) \Rightarrow P(S(k)) \Rightarrow \forall n \in \mathbb{N} : P(n)$,

де S *– функція наступного числа* ($S(x) = x + 1$), P *– предикат,* $P(1)$ *– база індукції,* $P(S(k))$ *– перехід.*

Definition 2.1.2 (Метод математичної індукції)**.** *Метод математичної індукції – це алгоритм, що виглядає наступним чином.*

1. *Перевірити, що твержденння виконується для* 1*.*
2. *Припустити, що твердження виконується для деякого* k*, довести, що воно виконується для* $k+1$*.*

Example 2.1. *Довести що* $n^3 + 5n \vdots 6$ *для будь якого* n*.*

Доведення. Доведемо методом математичної індукції.

1. $n = 1, \quad 1^3 + 5 = 6 \vdots 6.$
2. Нехай вірно для k, тоді $k^3 + 5k \vdots 6.$
3. Доведемо, що $(k+1)^3 + 5(k+1) \vdots 6.$

$k^3 + 3k^2 + 3k + 1 + 5k + 5 = (k^3 + 5k) + (1 + 5) + 3k(k+1)$, де $(k^3 + 5k) \vdots 6$, $(1+5) \vdots 6$, $3k(k+1) \vdots 6$ □

Example 2.2. *Довести, наступне твердження.*

$$1^2 + 2^2 + 3^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Доведення. Доведемо методом математичної індукції.

1. $n = 1, \quad 1^2 = \dfrac{1(1+1)(2 \cdot 1 + 1)}{6}.$
2. Нехай вірно для k, тоді
$$1^2 + 2^2 + 3^2 + ... + k^2 = \frac{k(k+1)(2k+1)}{6}.$$
3. Доведемо, для $(k+1)$.

$$\begin{aligned} 1^2 + 2^2 + 3^2 + ... + (k+1)^2 &= \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6} \\ &= \frac{(k+1)(k+2)(2k+3)}{6} \end{aligned}$$

$$\frac{k(k+1)(2k+1)}{6} + (k+1) = \frac{(k+1)(k+2)(2k+3)}{6}$$

$$\begin{aligned} (k+1)(k+2)(2k+3) + 6k^2 + 12k + 6 &= (k^2 + 3k + 2)(2k+3) \\ &= (k^2 + k)(2k+1) + 6k^2 + 12k + 6 \\ &= 2k^3 + 3k^2 + 6k^2 + 9k + 4k + 6 \\ &= 2k^3 + k^2 + 2k^2 + k + 6k^2 + 12k + 6 \end{aligned}$$

□

Example 2.3. *Довести, що для довільного* $n \geqslant 3$, $2^n > 2n + 1$.

Доведення. Доведемо методом математичної індукції.

1. Для $n = 3$, $2^3 > 7 \Leftarrow 8 > 7$.
2. Нехай вірно для k, тоді $2^k > 2k + 1$.
3. Доведемо, що $2^{k+1} > 2(k + 1) + 1$.

$$2^{k+1} + 1 = 2k + 3 = (2k + 1) + 2$$

$$2^k + 2 > (2k + 1) + 2, 2^{k+1} > 2^k + 2, 2^k > 2, k \geqslant 3$$

□

2.2 Теорія множин

Definition 2.2.1 (Множина)**.** *Множина (set) – це певна сукупність об'єктів, які ми можемо розрізнити між собою, які не повторюються, та об'єднані в одне ціле нашим бажанням.*

Існують наступні способи подання множин.

1. Явний, $A = \{a, b, ..., z\}$.
2. Не явний, нехай $P(x)$ – певна властивість (предикат),

$$X = \{x : P(x)\} = \{x \mid P(x)\}.$$

3. Графічний (діаграма Ойлера Венна).

Ось список стандартних числових множин.

- $\varnothing$ – порожня множина.
- $\mathbb{U}$ – універсум (всі об'єкти).
- $\mathbb{N} = \{1, 2, 3, ...\}$ –натуральні числа (не 0).
- $\mathbb{N}_0 = \{0, 1, 2, 3, ...\}$ – усі невід'ємні цілі числа.
- $\mathbb{Z} = \{0, \pm 1, \pm 2, ...\}$ – усі цілі числа.
- $\mathbb{Q} = \{\frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N}\}$ – раціональні числа.
- $\mathbb{R}$ – дійсні числа.
- $\mathbb{C}$ – комплексні числа.

Основні позначення в теорії множин.

- Належність $a \in A$.
- Не належність $a \notin A$.
- Включення $A \subseteq B$ (всі елементи A належать B).

$$(A \subseteq B) \Leftrightarrow (\forall a \quad a \in A \Rightarrow a \in B).$$

- Строге включення $A \subset B$ (всі елементи A належать B).

$$(A \subset B) \Leftrightarrow (A \subseteq B)\&(\exists b \in B : b \notin A)$$

- Рівність $A = B$, якщо A і B складається з однакових елементів.

$$(A = B) \Leftrightarrow (A \subseteq B)\&(B \subseteq A).$$

Основні операції над множинами.

1. Об'єднання:
$$C = A \cup B = \{x : (x \in A) \vee (x \in B)\}.$$
2. Перетин:
$$D = A \cap B = \{x : (x \in A) \wedge (x \in B)\}.$$
3. Різниця:
$$E = A \backslash B = \{x : (x \in A) \wedge (x \notin B)\}.$$
4. Симетрична різниця:
$$F = A \Delta B = (A \backslash B) \cup (B \backslash A) = (A \cup B) \backslash (B \cap A).$$
5. Доповнення (до універсуму $\mathbb{U}$):
$$\overline{A} = \{x : x \notin A\}.$$

Claim 2.1 (Парадокс Бертрана)**.** *Нехай $Y = \{X : X \notin X\}$, де X – це множина множин і/чи елементів, що не належить собі. Тоді, з'являється питання $Y \in Y$?*

Алгебраїчні властивості операцій над множинами

1. Ідемпотентність
$$A \cup A = A$$
$$A \cap A = A$$
2. Інволютивність
$$\overline{\overline{A}} = A$$
3. Комутативність
$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$
$$A \triangle B = B \triangle A$$
4. Асоціативність
$$A \cup (B \cup C) = (A \cup B) \cup C$$
$$A \cap (B \cap C) = (A \cap B) \cap C$$
$$A \triangle (B \triangle C) = (A \triangle B) \triangle C$$
5. Дистрибутивність
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$$
6. Правило поглинання
$$A \cup (A \cap B) = A$$
$$A \cap (A \cup B) = A$$
7. Закон Деморгана
$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$
$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$
8. Інші
$$A \cup \mathbb{U} = \mathbb{U} \quad A \cap \mathbb{U} = A$$
$$A \cup \varnothing = A \quad A \cap \varnothing = \varnothing$$
$$A \backslash A = \varnothing \quad A \triangle A = \varnothing$$
$$A \cup \overline{A} = \mathbb{U} \quad A \cap \overline{A} = \varnothing$$

Claim 2.2 (Принцип двоїстості). *Якщо є істинне твердження, що використовує об'єднання та доповнення множин, і в цьому твердженні ми замінимо всі об'єднання на перетини, а універсуми на порожні множини, то одержимо істинне твердження.*

Приклад доведень тверджень

Example 2.4. *Доведіть твердження* $A \backslash B = A \cap \overline{B}$.

Доведення.

$$\forall x : \quad x \in A \backslash B \Leftrightarrow \begin{cases} x \in A \\ x \notin B \end{cases} \Leftrightarrow \begin{cases} x \in A \\ x \in \overline{B} \end{cases} \Leftrightarrow x \in A \cap \overline{B} \Rightarrow A \backslash B = A \cap \overline{B}$$

□

Example 2.5. *Доведіть наступні два твердження.*

$$A \triangle B = (A \backslash B) \cup (B \backslash A)$$
$$A \triangle B = (A \cup B) \backslash (B \cap A)$$

Доведення.

$$\begin{aligned} A \triangle B &= (A \backslash B) \cup (B \backslash A) \\ &= (A \cap \overline{B}) \cup (B \cap \overline{A}) \\ &= ((A \cap \overline{B}) \cup B) \cap ((A \cap \overline{B}) \cup \overline{A}) \\ &= ((B \cup A) \cap (B \cup \overline{B})) \cap ((\overline{A} \cup A) \cap (\overline{A} \cup \overline{B})) \\ &= (A \cup B) \cap (\overline{A} \cup \overline{B}) \\ &= (A \cup B) \cap (\overline{A \cap B}) \\ &= (A \cup B) \backslash (A \cap B) \end{aligned}$$

□

Example 2.6. *Довести, що* $A \cup (A \cap B) = A$.

Доведення. а) Доведемо $A \cup (A \cap B) \subset A$, тобто $\forall x$, $x \in A \cup (A \cap B)$:

$$x \in A \cup (A \cap B) \Rightarrow \begin{cases} x \in A \\ x \in A \cap B \end{cases} \Rightarrow \left[\begin{array}{l} x \in A \\ \begin{cases} x \in A \\ x \in B \end{cases} \end{array} \right.$$

$$\Rightarrow \left[\begin{array}{l} x \in A \\ x \in A \end{array} \right. \Rightarrow x \in A \Rightarrow A \cup (A \cap B) \subseteq A$$

б) Доведемо $A \subset A \cup (A \cap B)$, тобто $\forall x$, $x \in A$:

$$x \in A \Rightarrow \begin{cases} x \in A \\ x \in \mathbb{U} \end{cases} \Rightarrow \begin{cases} x \in A \\ \left[\begin{array}{l} x \in B \\ x \in \overline{B} \end{array} \right. \end{cases} \Rightarrow \left[\begin{array}{l} \begin{cases} x \in A \\ x \in B \end{cases} \\ \\ \begin{cases} x \in A \\ x \in \overline{B} \end{cases} \end{array} \right.$$

$$\Rightarrow \left[\begin{array}{l} \begin{cases} x \in B \\ x \in A \end{cases} \\ x \in A \end{array} \right. \Rightarrow \left[\begin{array}{l} x \in A \cap B \\ x \in A \end{array} \right. \Rightarrow x \in A \cup (A \cap B)$$
$$\Rightarrow A \subseteq A \cup (A \cap B)$$

в) Доведемо фінальне твердження.

$$\begin{cases} A \subseteq A \cup (A \cap B) \\ A \cup (A \cap B) \subseteq A \end{cases} \Rightarrow A = A \cup (A \cap B).$$

$\square$

Example 2.7. *Показати, що* $A \cup (B \triangle C) \neq (A \cup B) \triangle (A \cup C)$

Доведення. Доведемо правильність даного твердження навівши контрприклад

$$A = \{1, 2, 3\}, B = \{2, \bigstar\}, C = \{3, \heartsuit\}.$$

$$A \cup (B \triangle C) = \{1, 2, 3\} \cup \{2, 3, \bigstar, \heartsuit\} = \{1, 2, 3, \bigstar, \heartsuit\}.$$

$$(A \cup B) \triangle (A \cup C) = \{1, 2, 3, \bigstar\} \cup \{1, 2, 3, \heartsuit\} = \{\bigstar, \heartsuit\}.$$

$\square$

2.2.1 Потужність скінченної множини

Definition 2.2.2 (Потужність скінченної множини)**.** *Потужність скінченної множини A ($|A|$, $\#A$ (октотор A)) – це кількість елементів множини A.*

Definition 2.2.3 (Дизюнктне об'єднання множин)**.** *Об'єднання двох множин називають дизюнктним, якщо ці множини не перетинаються.*

$$C = A \sqcup B \Leftrightarrow \begin{cases} C = A \cup B \\ A \cap B = \varnothing \end{cases}$$

Theorem 2.1 (Потужність дизюнктного об'єднання)**.**

$$C = A \sqcup B \Rightarrow |C| = |A| + |B|$$

Corollary 2.1.1 (Потужність дизюнктного об'єднання)**.**

$$A_1 \bigsqcup_{...} A_n = A_1 \sqcup A_2 \sqcup ... \sqcup A_n \Rightarrow |A| = \sum_{i=1}^{n} |A_i| = |A_1| + |A_2| + ... + |A_n|$$

Theorem 2.2 (Потужність різниці множин)**.**

$$|A \backslash B| = |A| - |A \cap B|$$

Доведення.

$$X = A \backslash B \quad Y = A \cap B.$$

$$X \cup Y = (A \backslash B) \cup (A \cap B) = (A \cap \overline{B}) \cup (A \cap B) = A \cap (\overline{B} \cup B) = A \cap \mathbb{U} = A.$$

$$X \cap Y = (A \backslash B) \cap (A \cap B) = A \cap \overline{B} \cap A \cap B = A \cap \varnothing = \varnothing.$$

$$\Rightarrow A = X \sqcup Y \Rightarrow |A| = |X| + |Y| = |A \backslash B| + |A \cap B|.$$

$$|A| = |A \backslash B| + |A \cap B|.$$

$$|A \backslash B| = |A| - |A \cap B|.$$

□

Theorem 2.3 (Потужність об'єднання двож множин)**.**

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

Доведення.

$$A \cup B = B \sqcup (A \backslash B) \Rightarrow |A \cup B| = |B| + |A \backslash B| = |B| + |A| - |A \cap B|$$

□

Theorem 2.4 (Теорема включень-виключень)**.**

$$\left| \bigcup_{i=1}^{n} A_1 \right| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leqslant i \leqslant j \leqslant n} |A_i \cap A_j| + \sum_{1 \leqslant i \leqslant j \leqslant k \leqslant n} |A_i \cap A_j \cap A_k| - ... + (-1)^{n-1} |A_1 \cap ... \cap A_n|$$

Доведення. TODO: Доведення не наведено в повній мірі. доробити.

$n = 1 \quad |A_1| = |A_1|$

$n = 2 \quad |A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$

Нехай для n формула вірна

$$B = \bigcup_{i=1}^{n} A_i$$

$|B \cup A_{n+1}| = |B| + |A_{n+1}| - |B \cap A_{n+1}| = \left|\bigcup\limits_{i=1}^{n} A_i\right| + |A_{n+1}| - \left|(\bigcup\limits_{i=1}^{n} A_i) \cap A_{n+1}\right| = \left|\bigcup\limits_{i=1}^{n} A_i\right| +$
$|A_{n+1}| - \left|\bigcup\limits_{i=1}^{n} A_i \cap A_{n+1}\right| = -\sum\limits_{i=1}^{n} |A_i \cap A_{n+1}| + \sum\limits_{1 \leqslant i \leqslant j \leqslant n} |A_i \cap A_{n+1} \cap A_j| - \sum\limits_{1 \leqslant i \leqslant j \leqslant k \leqslant n} |A_i \cap$
$A_{n+1} \cap A_j \cap A_k| + ... + (-1)^n |A_1 \cap A_2 \cap ... \cap A_{n+1}|$

... □

Example 2.8. *Скільки чисел від 1 до N ділиться на 2, 3 або 5 ($N \vdots 36$)*

$$\frac{N}{2} + \frac{N}{3} + \frac{N}{5} - \frac{N}{6} - \frac{N}{10} - \frac{N}{15} + \frac{N}{30} \approx N \cdot 0.7333$$

Example 2.9. *Скільки існує чисел від* 1 *до* N*, які взаємно прості з* N

$$\varphi(N) = |\{x \in \mathbb{N} \mid 1 \leqslant x \leqslant N, \gcd(x, N) = 1\}|$$

де φ – це Функція Ейлера, $N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$ – канонічний розклад числа на прості множники.

$$A_i = \{x \in \mathbb{N} \mid 1 < x \leqslant N, x_i \vdots p_i\}$$

$$\varphi(N) = N - |A_1 \cup A_2 \cup ... \cup A_n|$$

$$|A_i| = \frac{n}{p_i} \quad |A_i \cap A_j| = \frac{N}{p_i p_j} \quad |A_i \cap A_j \cap A_k| \frac{N}{p_i p_j p_k}$$

$$\begin{aligned}\varphi(N) &= N - \sum_{i=1}^{t} \frac{N}{p_i} + \sum_{1 \leqslant i \leqslant j \leqslant t} \frac{N}{p_i p_j} - \sum_{1 \leqslant i \leqslant j \leqslant k \leqslant t} \frac{N}{p_i p_j p_k} + ... + (-1)^t \frac{N}{p_1 p_2 ... p_t} \\ &= N(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})(1 - \frac{1}{p_3}) \cdot ... \cdot (1 - \frac{1}{p_t})\end{aligned}$$

Definition 2.2.4 (Булеан множини)**.** *Булеан множини A (Boolean) – множина всіх підмножин A. Позначають 2^A, $B(A)$.*

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

Theorem 2.5 (Про потужність булеану)**.** *Якщо A – скінченна, то $|2^A| = 2^{|A|}$. Тобто, якщо $|A| = n$ то $|2^A| = 2^n$.*

Доведення. 1-й спосіб

$$n = 0 \quad 2^{\varnothing} = \{\varnothing\}, |2^{\varnothing}| = 1 = 2^0$$

Нехай для всіх множин A де $|A| = n$, це вірно.

$$B = \{b_1, b_2, ..., b_n, b_{n+1}\}$$

Якщо $B_1 \subseteq B$ і $b_{n+1} \notin B$ то $\#B_1 = 2^n$ за припущенням

Якщо $B_2 \subseteq B$ і $b_{n+1} \in B_2$ то $B_2 \backslash \{b_{n+1}\} \backslash \{b_1, ..., b_n\} \Rightarrow \#B_2 = 2^n$ за припущенням індукції $\Rightarrow |2^B| = 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$

□

Доведення. 2-й спосіб

$$A = \{a_1, a_2, ..., \cancel{a_n}\}$$

$$\begin{cases} B \subseteq A & \bigcirc \mid \bigcirc \mid ... \mid \\ C \subseteq A & \underbrace{\bigcirc \bigcirc \bigcirc \mid ... \mid}_{n} \quad \Rightarrow |2^A| = 2^n \end{cases}$$

□

Definition 2.2.5 (Перекриття множини)**.** *Перекриття множини A (over) – це система множин* $\Delta \subseteq 2^A$, $\Delta = \{T_1, T_2, ..., T_n\}$, *що задовільняє наступним властивостям.*

1. $T_2 \neq \varnothing$.
2. $\bigcup\limits_{i=1}^{n} T_i = A$.

Definition 2.2.6 (Розбиття множини)**.** *Розбиття множини A (partion) – це система множин* $\Pi = \{T_1, T_2, ..., T_n\}$, $\Pi \subseteq 2^A$, *що задовільняє наступним властивостям.*

1. Π *– покриття.*
2. $\forall i \neq j \quad T_j \cap T_j = \varepsilon$.

Example 2.10.

$$\mathbb{N} = 2\mathbb{N} \sqcup (2\mathbb{N} - 1)$$

1. $\Pi = \{2\mathbb{N}, 2\mathbb{N} - 1\}$ *– Розбиття N*
2. $\mathbb{N} =$ *прості числа* $\sqcup$ *складені числа* $\sqcup \{1\}$
3. $A_0 = \{3k \mid k \in \mathbb{Z}\}$, $A_1 = \{3k + 1 \mid k \in \mathbb{Z}\}$, $A_2 = \{3k + 2 \mid k \in \mathbb{Z}\}$, $\{A_0, A_1, A_2\}$ *– розбиття* $\mathbb{Z}$.
4. $C_1 = \{[k, k + 1] \mid k \in \mathbb{Z}\}$ *– покриття* $\mathbb{R}$
   $C_2 = \{[k, k + 1) \mid k \in \mathbb{Z}\}$ *– розбиття* $\mathbb{R}$
   $C_3 = \{(k, k + 1) \mid k \in \mathbb{Z}\}$ *– ні те ні те, бо невистачає елементів множини* $\mathbb{Z}$ *(в основному, цілих чисел).*

2.2.2 Декартів добуток множин

Definition 2.2.7 (Декартовий добуток множин). *Декартовий добуток множин A та B – множина всіх пар виду (a, b), де $a \in A$, $b \in B$.*

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

Definition 2.2.8 (Декартів добуток множин). *Декартів добуток множин A_1, A_2, ..., A_n це:*

$$A_1 \times A_2 \times ... \times A_n = \{(a_1, a_2, ..., a_n) \mid a_1 \in A_1, a_2 \in A_2, ..., a_n \in A_n\}$$

Definition 2.2.9 (Декартів степінь). *Декартів степінь множини A*

$$A^n = \underbrace{A \times A \times ... \times A}_{n}$$

Example 2.11. *Площина:* $\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$

Example 2.12. *Простір* $\mathbb{R}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$

Example 2.13. *n-вимірний простір* $\mathbb{R}^n$

Example 2.14. *Множина раціональних чисел $\mathbb{Q}$. $\mathbb{Q}$ – це дорби скорочень.* $\left(\frac{1}{2} \neq \frac{2}{4}\right)$.

$$\mathbb{Q} = \left\{ \frac{m}{n} \;\middle|\; \begin{array}{l} m \in \mathbb{Z} \\ n \in \mathbb{N} \end{array} \right\}, \mathbb{Q} \sim \mathbb{Z} \times \mathbb{N}.$$

Theorem 2.6 (Про потужність декартового добутку). *Якщо A та B – скінченні то*

$$|A \times B| = |A| \times |B|.$$

Corollary 2.6.1. $|A_1 \times A_1 \times ... \times A_1| = |A_1| \times |A_1| \times ... \times |A_1|$.

Corollary 2.6.2. $|A^n| = |A|^n$.

Definition 2.2.10 (Алфавіт). *Алфавіт A – довільна множина елементів.*

Definition 2.2.11 (Символ). *Символ a ($a \in A$) – це довільний елемент алфавіту A.*

Definition 2.2.12 (Слово). *Слово довжини n – це довільна послідовність символів алфавіту A довжини n. Позначають як $(a_1, a_2, ..., a_n)$ або просто $a_1 a_2 ... a_n$.*

Definition 2.2.13 (Словник слів заданої довжини). *A^n – множина всіх слів довжини n.*

Definition 2.2.14 (Порожнє слово). *ε – порожнє слово (слово що не містить жодної літери)*

Remark 2.1. $A^0 = \{\varepsilon\}$.

Definition 2.2.15 (Замикання алфавіту (зірка Клікі)). *Замикання алфавіту (зірка Клікі) (Kleene closure, Kleene star) – це наступна множина.*

$$A^* = A^0 \cup A^1 \cup A^2 \cup ... = \bigcup_{n=0}^{\infty} A^n$$

Definition 2.2.16 (Формальна мова). *Формальна мова над алфавітом A – це множина $L \subseteq A^*$.*

2.3 Теорія відношень

Definition 2.3.1 (m-арне відношення). *m-арне відношення на множинах A_1, A_2, ..., A_n – це множина:*

$$R \subseteq A_1 \times A_2 \times ... \times A_m.$$

Definition 2.3.2 (m-арне відношення). *m-арне відношення на множині A – це множина $R \subseteq A^m$.*

Definition 2.3.3 (Унітарне відношення). *Унітарні відношення: $R \subseteq A$, $m = 1$*

Example 2.15 (Унітарне відношення). *Прості числа в $\mathbb{N}$.*

Definition 2.3.4 (Бінарне відношення). *Бінарні відношення: $R \subseteq A \times B$, $m = 2$.*

Example 2.16 (Бінарні відношення). *Бінарні відношення, які часто використовуються.*

- $<, =, \neq$ – *на числах.*
- $\subseteq, \subset$ – *на множинах.*
- $\in$ – *на елементах та множинах.*
- $\|, \perp$ – *на прямих чи на площинах.*

Definition 2.3.5 (Тернарне відношення). *Тернарне відношення: $R \subseteq A \times B \times C$, $m = 3$.*

Для двох відношень однакової арності, на однакових множинах, можна застосувати операції $\cup$, $\cap$, $\setminus$, $\triangle$, в результаті, одержавши відношення.

Універсум (Область визначення, домен), в даному випадку, це множина:

$$A_1 \times A_2 \times ... \times A_m$$

2.3.1 Способи поданчі бінарних відношень:

Явний

$$A = \{a, b, c, d\},$$
$$B = \{0, 1, 2\},$$
$$A = \{(a, 0), (a, 1)(b, 2)\}.$$

Стрілкова діаграма

Матричне представлення

	0	1	2
a	1	1	0
b	0	0	1
c	0	0	1
d	0	0	0

2.3.2 Операції над бінарними відношеннями

Remark 2.2. Якщо a стоїть у відношенні з b, тобто $(a, b) \in R$, то замість $(a, b) \in R$ можна написати aRb.

Нехай $R \subseteq A \times B$.

Definition 2.3.6 (Обернене відношення). *Обернене відношення (reverce)*

$$R^{-1} \subseteq B \times A$$

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

Нехай $R_1 \subseteq A \times B$, Нехай $R_2 \subseteq B \times C$.

Definition 2.3.7 (Композиція відношень). *Композиція (composition) відношень R_1 та R_2 – це відношення:*

$$R_3 = R_1 \circ R_2 \subseteq A \times C$$

$$R_3 = R_1 \circ R_2 = \{(a, c) \mid \exists b \in B : aR_1b, bR_2c\}$$

Example 2.17.

$$A = \{a, b, c, d\}, B = \{0, 1, 2\}, C = \{\zeta, \varkappa, \varpi, \Xi\}$$

$$R_1 = \{(a, 0), (a, 1), (b, 2), (c, 2)\}$$
$$R_2 = \{(0, \zeta), (1, \varpi), (1, \Xi)\}$$
$$R_3 = \{(a, \zeta), (a, \varpi), (a, \Xi)\}$$

Definition 2.3.8 (Степінь відношення). *Степенем відношення $R \subseteq A^2$:*

$$R^n = R \circ R \circ ... \circ R$$

2.3.3 Властивості бінарних відношень

1. Рефлексивність $\forall a \in A \quad aRa$
2. Іррефлексивність $\forall a \in A \quad a\overline{R}a$
3. Нерефлексивність $\exists a \in A \quad a\overline{R}a$
4. Симетричність $\forall a, b \in A : aRb \Rightarrow bRa$
5. Антисиметричність $\forall a, b \in A : aRb, bRa \Rightarrow a = b$

6. Асиметричність $\forall a, b \in A : aRb \Rightarrow b\overline{R}a$
7. Несиметричність $\exists a, b \in A : aRb \Rightarrow b\overline{R}a$
8. Транзитивність $\forall a, b, c \in A : aRb, bRc \Rightarrow aRc$
9. Нетранзитивність $\forall a, b, c \in A : aRb, bRc \Rightarrow a\overline{R}c$
10. Зв'язність $\forall a, b \in A : aRb \vee bRa$
11. Слабка зв'язність $\forall a, b \in A \quad a \neq b \to aRb \vee bRa$

Definition 2.3.9 (Діагональ множини)**.** *Діагональ множини – це множина:*

$$i_A = \Delta_A = \{(a, a) \mid \forall a \in A\}$$

Theorem 2.7. $R \subseteq A^2$ *– рефлексивне* $\Leftrightarrow i_A \subseteq R$ $R \subseteq A^2$ *– іррефлексивне* $\Leftrightarrow i_A \cap R = \varnothing$

Lemma 2.1. $R \subseteq A^2$ *– симетричне* $\Leftrightarrow R = R^{-1}$ $R \subseteq A^2$ *– антисиметричне* $\Leftrightarrow R \cap R^{-1} \subseteq i_A$ $R \subseteq A^2$ *– асиметричне* $\Leftrightarrow R \cap R^{-1} \subseteq \varnothing$

Theorem 2.8. $R \subseteq A^2$ *– транзитивне* $\Leftrightarrow R^2 \subseteq R$

Example 2.18. $< \mathbb{Z}, \equiv_n >$, *(де* $\equiv_n$ *– рівність за модулем* n*, тобто* $(x \equiv_n y) \Leftrightarrow (x \equiv y \mod n)$*).*

рефлексивність

$$x \equiv_n x \Leftrightarrow (x - x) \Leftrightarrow 0 \equiv n$$

симетричність $x \equiv_n y \Rightarrow y \equiv_n x$

$$\begin{aligned} x \equiv_n y &\Rightarrow (x - y) \vdots n \\ &\Rightarrow \exists k \in \mathbb{Z} \quad (x - y) = kn \\ &\Rightarrow \exists k \in \mathbb{Z} \quad (y - x) = -kn \\ &\Rightarrow (y - x) \vdots n \\ &\Rightarrow y \equiv_n x \end{aligned}$$

транзитивність $x \equiv_n y, y \equiv_n z \Rightarrow x \equiv_n z$

$$\begin{aligned} x \equiv_n y, y \equiv_n z \quad &\Rightarrow \quad \begin{cases} x - y = kn \\ y - z = tn \end{cases} \\ &\Rightarrow \quad (x - z) = (x - y) + (y - z) = (k + t)n \\ &\Rightarrow \quad x \equiv_n z \end{aligned}$$

Example 2.19. $< \mathbb{N}_1, \vdots >, (x \vdots y) \Leftrightarrow (\exists k \in \mathbb{N} \quad x = ky)$

рефлексивність $x = 1x \Rightarrow x \vdots x$

антисиметричність

$$\begin{aligned} x \vdots y, y \vdots x \quad &\Rightarrow \quad \exists a, b \in \mathbb{N} : x = ay, y = bx \\ &\Rightarrow \quad y = bay \\ &\Rightarrow \quad 1 = ba \\ &\Rightarrow \quad b = 1, a = 1 \\ &\Rightarrow \quad x = y \end{aligned}$$

Theorem 2.9. $R \subseteq A^2$ *– антисиметричне* $R \cap R^{-1} \subseteq i_A$

Доведення. ($\Rightarrow$) Нехай R – антисиметричне відношення

$$\forall a, b \in A \quad aRb, bRa \Rightarrow a = b$$

$$\begin{aligned} \forall (a,b) \in R \quad (a,b) \in R \cap R^{-1} \quad &\Rightarrow \quad \begin{matrix} (a,b) \in R \\ (a,b) \in R^{-1} \end{matrix} \\ &\Rightarrow \quad \begin{matrix} aRb \\ bRa \end{matrix} \\ &\Rightarrow \quad a = b \\ &\Rightarrow \quad (a,b) \in i_A \end{aligned}$$

Отже:

$$R \cap R^{-1} \subseteq i_A$$

($\Leftarrow$) Нехай $R \cap R^{-1} \subseteq i_A$.

$$\begin{aligned} \forall a, b \in A \quad aRb, bRa \quad &\Rightarrow \quad \begin{matrix} aRb \\ aR^{-1}b \end{matrix} \\ &\Rightarrow \quad (a,b) \in R \cap R^{-1} \\ &\Rightarrow \quad (a,b) \in i_A \\ &\Rightarrow \quad a = b \end{aligned}$$

Отже R – антисиметричне.

□

Theorem 2.10. $R \subseteq A^2$ *– транзитивне* $\Leftrightarrow R \circ R \in R$.

Доведення. ($\Rightarrow$) Нехай R – транзитивне

$$\forall a, b, c \in A \quad aRb, bRc \Rightarrow aRc$$

$$\begin{aligned} \forall (a,c) \in R^2 \exists b \in A : aRb, bRc \quad &\Rightarrow \quad aRc \\ &\Rightarrow \quad (a,c) \in R \end{aligned}$$

Отже $R^2 \subseteq R$.

($\Leftarrow$) Нехай $R^2 \subseteq R$.

$$\forall a, b, c \in A \quad aRb, bRc \quad \Rightarrow \quad aR^2c$$

А отже: R – транзитивне. □

2.3.4 Відношення еквівалентності

Definition 2.3.10 (Відношення еквівалентності)**.** *Бінарне відношення $R \subseteq A^2$ – це відношення еквівалентності, якщо воно рефлексивне, симетричне і транзитивне. Часто позначають як $\sim$ тильда*

$a \sim b$, або, ще: a, b – еквівалентні, або a еквівалентне b.

Definition 2.3.11 (Клас еквівалентності)**.** *Клас еквівалентності елементу $a \in A$:*

$$[a] = \{b \in A \mid b \sim a\}$$

Definition 2.3.12 (Фактор множина)**.** *Фактор множина це:*

$$A / \sim\, = \{[a] \mid \forall a \in A\}$$

Example 2.20. $< \mathbb{N}, =>, \quad [x] = \{x\}$

$$\mathbb{N} / = \; = \{\{1\}, \{2\}, \{3\}, ...\}$$

Example 2.21. $< \mathbb{Z}, \equiv_n>, \quad x \equiv_n y \Leftrightarrow (x - y) \,\vdots\, n$

$$[0] = \{0, \pm n, \pm 2n, \pm 3n, ...\}$$

$$\left.\begin{array}{r} [0] = \{kn \mid k \in \mathbb{Z}\} \\ [1] = \{kn + 1 \mid k \in \mathbb{Z}\} \\ [2] = \{kn + 2 \mid k \in \mathbb{Z}\} \\ \vdots \\ [n-1] = \{kn + n - 1 \mid k \in \mathbb{Z}\} \end{array}\right\} \textit{Лишки}$$

$$\mathbb{Z} / \equiv_n \; = \{[0], [1], ..., [n-1]\} = \mathbb{Z}_m$$

Example 2.22. $\mathbb{L}$ *– множина прямих на площині*

$< \mathbb{L}, \| >$

$l = ax + by + c = 0$

$$[l] = \{ax + by + d = 0 \mid \forall d \in \mathbb{R}^2\}$$
$$\mathbb{L} / \| \; = \{[l_{ab}] \forall a, b \in \mathbb{R}\}$$

page 21

Lemma 2.2. $a \sim b \Leftrightarrow [a] = [b]$

Доведення.

$$a \sim b \Leftrightarrow a \sim b = b \sim a \Leftrightarrow [a] = [b]$$

$\square$

Theorem 2.11. *Нехай* $\sim$ *це відношення еквівалентності на* A*, то* ${}^{A}\diagup_{\sim}$ *– розбиття* A*.*

Доведення. 1) $a \in [a] \to [a] \subseteq \varnothing$.

$\bigcup\limits_{a \in A} [a] = A$.

3) $a, b \in A$. Нехай $[a] \cap [b] \neq \varnothing$.

$\exists x \in [a] \cap [b] \Rightarrow \begin{matrix} x \sim a \\ x \sim b \end{matrix} \Rightarrow \begin{matrix} a \sim x \\ x \sim b \end{matrix} \Rightarrow a \sim b \Rightarrow [a] = [b]$.

Якщо $a \not\sim b$, то $[a] \cap [b] = \varnothing$. $\square$

Theorem 2.12. *Нехай* $A = T_1 \sqcup T_2 \sqcup ... \sqcup T_k$ *то існує відношення еквівалентності* $\sim$*, що*

$$ {}^{A}\diagup_{\sim} = \{T_1, T_2, ..., T_k\}$$

Definition 2.3.13. *Нехай* $a \sim b \Leftrightarrow \exists i : a \in T_i, b \in T_i$.

рефлексивність: $a \in t_i, a \in T_i \Rightarrow a \sim a$ *симетричність:* $a \sim b \Rightarrow \exists a \in T_i, b \in T_i \Rightarrow b \sim a$
транзитивність: $\forall a, b, c \quad a \sim b, b \sim c \Rightarrow \exists i, j : \left| \begin{matrix} a \in T_i \\ b \in T_i \end{matrix} \right| \begin{matrix} b \in T_j \\ c \in T_j \end{matrix} \Rightarrow i = j \Rightarrow a \sim c$

Example 2.23.

$$A^2 = \{(a, b) \mid \forall a, b \in A\}$$

R *– бінарне відношення на* A^2*.*

$(a, b)R(x, y) \Leftrightarrow \left[\begin{matrix} (a, b) = (x, y) \\ (a, b) = (y, x) \end{matrix} \right.$

$[(a, b)] = \{(a, b), (b, a)\}$

$[a, a] = \{(a, a)\}$

$A^{(2)}$ *– множина невпорядкованих пар.*

$A^{(2)} = {}^{A^2}\diagup_{R}.$

Example 2.24. $\mathbb{Z} \times \mathbb{N} \quad \sim: (m_1, n_1) \sim (m_2, n_2) \Leftrightarrow m_1 \cdot n_2 = m_2 \cdot n_1$.

$\mathbb{Q} = {}^{(\mathbb{Z} \times \mathbb{N})}\diagup_{\sim}$

2.3.5 Замикання відношення

Definition 2.3.14 (Замикання)**.** *Замикання об'єкта за властивістю – це інший об'єкт, що включає в себе даний об'єкт та має цю властивість, якщо можливо.*

Definition 2.3.15 (Рефлексивне замикання)**.** *Рефлексивне замикання*

$$R^{=} = R^{r} = i_A \cup R.$$

Definition 2.3.16 (Симетричне замикання)**.** *Симетричне замикання*

$$R^{S} = R \cup R^{-1}.$$

Definition 2.3.17 (Транзитивне замикання)**.** *Транзитивне замикання*

$$R^{+} = R^{t} = R \cup R^2 \cup ... \cup R^n = \bigcup_{n=1}^{\infty} R^n.$$

Remark 2.3. Якщо для деякого k, $R^k = R^{k+1}$ то

$$R^t = \bigcup_{n=1}^{k} R^n$$

Definition 2.3.18 (Замикання передпорадку)**.** *Замикання передпорадку*

$$R^{*} = R^{rt}$$

Definition 2.3.19 (Замикання еквівалентності)**.** *Замикання еквівалентності*

$$R^{\equiv} = R^{\varepsilon} = R^{rst}$$

Claim 2.3.

$$R^{rt} = R^{tr}$$

Claim 2.4.

$$R^{rs} = R^{sr}$$

Claim 2.5.

$$R^{st} \supseteq R^{ts}.$$

Claim 2.6. *Відношення $R^{\equiv}$ – мінімальне відношення еквівалентності, що включає R.*

Example 2.25. $< R, (<) >$

$$(<)^r = (\leqslant)$$

$$(<)^s = (\neq)$$

$$(<)^t = (<)$$

Example 2.26 (Транспортна мережа). *R – відношення сусудства R^r – відношення самодосяжності R^s – відношення пов'язаності R^t – відношення досяжності*

R^E – задає розбиття на компоненти зв'язності

R^* – розбиття на компоненти сильної зв'язності

2.3.6 Функціональні відношення

$f \subseteq A \times B$

Definition 2.3.20 (Область визначення). *Область визначення відношення*

$$Dom(f) = \{\overline{a} \in A \mid \exists b \in B \quad (a, b) \in f\}$$

Definition 2.3.21 (Область значень). *Область значень*

$$Range(f) = Im(f) = \{b \in B \mid a \in f \quad a, b \in f\}$$

Definition 2.3.22 (Образ елемента). *Образ елемента*

$$a \in Af(a) = \{b \in B \mid (a, b) \in f\}$$

Definition 2.3.23 (Повністю визначене бінарне відношення). *Повністю визначене бінарне відношення (left - total)*

$$f \subseteq a \times B$$

$$Dom(f) = A$$

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

Definition 2.3.24 (Функціональне відношення). *Функціональне відношення*

$$\forall a \in A|f(a)| \leqslant$$

$$\forall a \in A(\exists! b \in B(a, b) \in f) \vee (\nexists b \in B(a, b) \in f)$$

Definition 2.3.25 (Відображення). *Відображення (mapping) – повністю визначене функціональне відношення*

Замість $(a, b) \in f$ або afb , пишемо $b = f(a)$.

Замість $f \subseteq A \times B$, пишемо $f : A \to B$.

Definition 2.3.26 (Функція). *Функція це часткове відображення*

Definition 2.3.27 (Кардинальний степінь). *Кардинальний степінь A^B:*

$$A^B = \{f \mid f : B \to A \text{ – відображення }\}$$

Theorem 2.13 (Про потужність кардинального степеня). *Якщо A та B – скінченні, то*

$$|A^B| = |A|^{|B|}$$

2.3.7 Властивості відношень

Definition 2.3.28 (Ін'єктивність). *Ін'єктивність*

$$\forall x_1, x_2 \quad x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2).$$

Definition 2.3.29 (Сюр'єктивність). *Сюр'єктивність*

$$f : A \to B \quad Im(f) = B.$$

або

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

Definition 2.3.30 (Бієктивність). *Бієктивність – це інєктивність та сюр'єктивність одночасно.*

Example 2.27. $f : R \to R$ *– відображення,* $f : [-\frac{\pi}{2}; \frac{\pi}{2}] \to R$ *– інєктивне,* $f : [-\frac{\pi}{2}; \frac{\pi}{2}] \to [-\frac{\pi}{2}; \frac{\pi}{2}]$ *– бієктивне,* $f : [0; \pi] \to [0; 1]$ *– сюр'єктивне.*

Операції

Definition 2.3.31 (Обернене функціональне відношення). f^{-1} *– обернене функціональне відношення, не обовязково є функціональним.*

Definition 2.3.32 (Композиція). *Композиція* $f \circ g$

$$h(x) = z \Leftrightarrow \exists y : (f(x) = y)\&(g(y) = z).$$

Theorem 2.14 (Про бієктивні відображення). *1) Якщо f – бієкція, то f^{-1} також бієкція.*

2) Якщо f та g – бієкція, то $h = f \circ g$ – бієктивне.

Доведення. 1)

$$\begin{aligned} \text{Нехай } f : A \to B - \text{бієкція} \quad &\Rightarrow \begin{cases} \forall a_1, a_2 \in A \quad a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2) \\ \forall b \in B \quad \exists a \in A \quad f(a) = b \end{cases} \\ &\Rightarrow \begin{cases} \forall b_1, b_2 \in B \quad b_1 \neq b_2 \Rightarrow f^{-1}(b_1) \neq f^{-1}(b_2) \\ \forall a \in A \quad \exists b \in B f^{-1}(b) = a \end{cases} \\ &\Rightarrow f^{-1} - \text{бієкція} \end{aligned}$$

2) Нехай f і g – бієкції, $h = f \circ g$:

$$\begin{aligned} \begin{cases} h = \{(a, c) \mid \exists b \quad b = f(a) \quad c = g(b)\} \\ f, g - \text{бієкції} \end{cases} \quad &\Rightarrow h = \{(a, c) \mid \exists! b \quad b = f(a) \quad c = g(b)\} \\ &\Rightarrow \begin{cases} \forall a_1, a_2 \quad a_1 \neq a_2 \Rightarrow h(a_1) \neq h(a_2) \\ \forall c \quad \exists a \quad h(a) = c \end{cases} \\ &\Rightarrow h - \text{бієкція}. \end{aligned}$$

□

Theorem 2.15 (Теорема Ф)**.** *Нехай A та B – скінченні множини, тоді:*

Якщо $\exists f : A \to B$ – інєкція, то $|A| \leqslant |B|$. Якщо $\exists f : A \to B$ – сюрекція, то $|A| \geqslant |B|$. Якщо $\exists f : A \to B$ – бієкція, то $|A| = |B|$.

Theorem 2.16. *A та B – еквівалентні (в тому числі і рівнопотужні), якщо $\exists F : A \to B$ – бієкція.*

Definition 2.3.33 (Нескінченна множина (за Додекіндом))**.** *A – це нескінченна множина (за Додекіндом), якщо A еквівалентна власній підмножині*

$$A \text{ – нескінченна } \Leftrightarrow \exists B \quad (B \subset A)\&(A \sim B)$$

Definition 2.3.34 (Скінченна множина)**.** *Скінченна множина – це множина, що не еквівалентна своїм підмножинам (жодній з них)*

Definition 2.3.35 (Потужність множини (кардинальне число))**.** *Потужність множини (або кардинальне число) – це клас еквівалентності за $\sim$ до якого відноситься множина.*

Для скінченних множин потужність позначається натуральним числом. Для нескінченних множин – трансфінітні числа: $\aleph$ – алеф

Claim 2.7. *$\mathbb{N}$ – нескінченна множина*

Доведення.

$$2\mathbb{N} = \{2n \mid \forall x \in \mathbb{N}\} \subset \mathbb{N}$$

$$f(n) = 2n \quad f : \mathbb{N} \to 2\mathbb{N}$$

$$f \text{ – бієкція.}$$

□

Remark 2.4.

$$|\mathbb{N}| = \aleph_0$$

Definition 2.3.36 (Злічення множина)**.** *Злічення множина – це множина, що еквівалентна множині $\mathbb{N}$.*

Theorem 2.17. *Довільна під множина натуральних чисел або скінченна або злічення (не більш ніж злічення)*

$$\forall B : (B \subseteq \mathbb{N}) \Rightarrow |B| \leqslant \aleph_0$$

2.3.8 Відношення часткового порядку

$R \subseteq A^2$

Definition 2.3.37 (Передпорядок)**.** *R – (рефлексивне та транзитивне) це передпорядок (preorder) або квазіпорядок (quasiorder).*

Definition 2.3.38 (Частковий порядок)**.** *R – частковий порядок, якщо воно рефлексивне, антисиметричне і транзитивне.*

Definition 2.3.39 (Строгий порядок)**.** *– строгий порядок (strict partial order), якщо воно іррефлексивне і транзитивне.*

Lemma 2.3. *Якщо $R \subseteq A^2$ – іррефлексивне і транзитивне, то R – асиметричне.*

Доведення. Нехай R – симетричне

($\forall a, k \in A \quad aRb, bRa \Rightarrow aRa \Rightarrow$ протиріччя)

$\Rightarrow R$ – не симетричне.

Нехай R – антисиметричне ($\forall a, b \quad aRb, bRa \Rightarrow a = b \Rightarrow$ протиріччя)

$\Rightarrow R$ – не антисиметричне

Нехай R – несиметричне

(($\exists a, b \quad aRb \Rightarrow a\overline{R}b \& aRb) \Rightarrow aRa \Rightarrow$ протиріччя)

$\Rightarrow R$ – не несиметричне

R – асиметричне ☐

$< A, R >$ – (Частково) впорядкована множина (partially ordered set (or [[paset]]))

Example 2.28. *1) $< 2^{A^*}, \pi > L_A \pi L_2 \Leftrightarrow$ переклад довільного тексту L_1 на L_2*

π – передпорядок

Example 2.29. *$< R, \leqslant >$ – частковий порядок $< R, < >$ – строгий порядок*

Example 2.30. *$< 2^A, \subseteq >$ – частковий порядок $< 2^A, \subset >$– строгий порядок*

Example 2.31. *$< \mathbb{Z}, \vdots >$ – частковий порядок*

Claim 2.8. *Якщо R це частковий порядок на A, то R^{-1} – також частковий порядок на A.*

Доведення. Нехай R – частковий порядок на A, тоді

$$\begin{aligned} R \text{ – частковий порядок на } A \quad &\Rightarrow \begin{cases} \forall a \in A \quad aRa \\ \forall a, b \in A \quad aRb, bRa \Rightarrow a = b \\ \forall a, b, c \in A \quad aRb, bRc \Rightarrow aRc \end{cases} \\ &\Rightarrow \begin{cases} \forall a \in A \quad aR^{-1}a \\ \forall a, b \in A \quad aR^{-1}b, bR^{-1}a \Rightarrow a = b \\ \forall a, b, c \in A \quad aR^{-1}b, bR^{-1}c \Rightarrow aR^{-1}c \end{cases} \\ &\Rightarrow R^{-1} \text{ – частковий порядок} \end{aligned}$$

☐

2.3.9 Діаграма Хассе (Гессе) (Hasse)

1. Не малюємо петель
2. Малюємо зв'язок тільки між сусідніми елементами
   Елементи a та b – сусідні (за $\mathbb{R}$) якщо:
   (а) aRa.
   (б) $\nexists c \quad c \neq b, c \neq a \Rightarrow aRc, cRb$.

Example 2.32. $\mathbb{N}_6 = \{1, 2, 3, 4, 5, 6\}$

$< \mathbb{N}_6, | > \quad x \mid d \Leftrightarrow d \,\vdots\, x$

Example 2.33. $< \mathbb{N}_6, \leqslant >$

$< A, R >$ – частково впорядкована множина

$a \in A$ – мінімальний $\Leftrightarrow \nexists b \in A \quad bRa$

$a \in A$ – найменший $\Leftrightarrow \forall b \in A \quad aRb$

$a \in A$ – максимальний $\Leftrightarrow \nexists b \in A \quad aRb$

$a \in A$ – найбільший $\Leftrightarrow \forall b \in A \quad bRa$

Example 2.34. *мінімальне – 1*

найменше – 1

максимальне – 4, 6, 5

найбільше – undefined

Claim 2.9. *Впорядкована множина $< A, R >$ має не більше одного найбільшого (найменшого) елементу*

Доведення. Нехай a та a' ($a \neq a'$) – найменші елементи $A \Rightarrow$

$$\begin{cases} aRa' \\ a'Ra \end{cases} \Rightarrow a = a' \Rightarrow \text{ протиріччя}$$

□

2.3.10 Індуковані порядки

Нехай $< A_i, \leqslant_i >, i = \overline{1, n}$ – впорядковані множини $A = A_1 \times A_2 \times ... \times A_n$.

Definition 2.3.40. *Відношення домінування $< A, \leqslant >$.*

$$(a_1, ..., a_n) \leqslant (b_1, ..., b_n) \Leftrightarrow a_i \leqslant b_i.$$

Definition 2.3.41. *Строге домінування $< A, \prec >$.*

$$(a_1, ..., a_n) \prec (b_1, ..., b_n) \Leftrightarrow ((a_1, ..., a_n) \leqslant (b_1, ..., b_n))\&(\exists i \quad a_i \neq b_i).$$

Definition 2.3.42 (Лексикографічний порядок)**.** *Лексикографічний порядок задається множиною A та відображенням $\leqslant_l$: $\langle A, \leqslant_l \rangle$.*

$$(a_1, ..., a_n) \leqslant_l (b_1, ..., b_n) \Leftrightarrow (a_1 \leqslant b_1) \vee ((a_1 = b_1) \wedge (a_1 \leqslant b_1)) \vee ...$$

$$... \vee ((a_1 = b_1) \wedge ... \wedge (a_{n-1} = b_{n-1}) \wedge (a_n \leqslant a_n)).$$

Claim 2.10. *Відношення домінування є відношенням строгого порядку*

Доведення. Нехай R – відношення домінування на A, тоді

$$((a_1, ..., a_n) \leqslant (b_1, ..., B_n) \Leftrightarrow \forall i \quad a_i \leqslant b_i)) \Rightarrow \forall a \in A \quad aRa \Rightarrow r - \text{рефлексивне}$$

$$(\forall a, b, c \quad aRb, bRc \Rightarrow aRc) \Rightarrow R - \text{транзитивне}$$

$$((a_1...a_n) \leqslant (b_1...b_n) \Leftrightarrow \forall i \quad a_i \leqslant b_i) \Rightarrow$$
$$(\neq ((a_1...a_n) \leqslant (b_1...b_n)) \Leftrightarrow \forall i \quad b_i \leqslant a_i) \Rightarrow$$
$$\forall a, b \quad aRb, bRa \Rightarrow a = b \Rightarrow R\text{– антисиметричне.}$$

□

Claim 2.11. *R – відношення часткового порядку.*

Доведення. Нехай R – лексикографічний порядок на A.

$$\Big((a_1, ..., a_n) \leqslant_l (b_1, ..., b_n) \Leftrightarrow (a_1 \leqslant b_1) \vee ((a_1 = b_1)\&(a_1 \leqslant b_1)) \vee ...$$
$$... \vee ((a_1 = b_1)\&...\&(a_{n-1} = b_{n-1})\&(a_n \leqslant a_n))\Big) \Rightarrow$$
$$\forall a \in A \quad aRa \Rightarrow R\text{– рефлексивне}$$

З означення випливає, що якщо елементи різні, то вони співставляються один з одним знаком $\leqslant \Rightarrow aRb, bRa \Rightarrow a = b \Rightarrow R.$ – антисиметричне.

З означення випливає, що якщо $\forall a, b, c \quad aRb, bRc$, то $aRc \Rightarrow R$ – транзитивне.

R – відношення часткового порядку □

2.3.11 Порядки

Definition 2.3.43 (Лінійний порядок)**.** *Лінійні порядки – зв'язний частковий порядок.*

Definition 2.3.44 (Строгий лінійний порядок)**.** *Строгий лінійний порядок – слабкозвязний строгий порядок.*

Example 2.35. $<\mathbb{N},\leqslant>$ *– лінійний порядок.*

Example 2.36. $<2^A,\subseteq>$ *– не лінійний порядок.*

Example 2.37. $\leqslant$ *– не зберігає лінійність.*

Example 2.38. $\leqslant_l$ *– зберігає лінійність.*

Definition 2.3.45. $<A,R>$ *– цілком впорядкована (wel-ordered set), якщо*

1. R *– частковий порядок.*
2. $\forall B \subseteq A$ *– має найменший елемент за* R*.*

Example 2.39. $<\mathbb{N},\leqslant>$ *– цілком впорядкована.*

Example 2.40. $<\mathbb{Z},\leqslant>$ *– не цілком впорядкована множина.*

Lemma 2.4. $<A,R>$ *– цілком впорядкована, тоді* R *– лінійний порядок.*

Доведення. Якщо A – цілком впорядкована множина $\Rightarrow R$ – частковий порядок.

Так як $\forall B \subseteq A$ – має найменший елемент $\Rightarrow R$ – лінійний порядок □

Theorem 2.18 (Теорема Цермело)**.** *Довільну множину можна цілком впорядкувати.*

Claim 2.12. $<A,R>$ *– скінченна множина, частково впорядкована, тоді завжди можна довизначити до лінійного.*

Нехай $<A,R>$ – цілком впорядкована множина

a_0 – найбільний елемент A.

$P(a) \quad a \in A$ – твердження

Theorem 2.19 (Про трансфінітну індукцію)**.** *Якщо*

1. $P(a_0)$ *– істинне*
2. $\forall x \in A \quad ((\forall (y,x) \in R \quad y \neq x \Rightarrow P(y) \text{істинне}) \Rightarrow P(x) \text{істинне})$*.*
   Тоді $\Rightarrow P(a)$ *– істинне* $\forall a \in A$*.*

Доведення.

$$
\begin{aligned}
A^- = \{\overline{a} : P(a) - \text{хибне } \} \subseteq A \quad &\Rightarrow \quad \exists \overline{a} \in A^- - \text{найменший} \\
&\Rightarrow \quad \overline{a} \neq a_0 \\
&\Rightarrow \quad \forall b \quad bR\overline{a} \\
&\Rightarrow \quad P(b) - \text{істинне} \\
&\Rightarrow \quad P(\overline{a}) - \text{істинне} \\
&\Rightarrow \quad \text{протиріччя}
\end{aligned}
$$

□

2.3.12 Спеціальні види функціональних відношень

Definition 2.3.46 (Послідовність над множиною). *Послідовність над множиною A, (де A можливо скінченна):*

$$f : \mathbb{N}_n \to A$$

$$f : \mathbb{N} \to A$$

$$f : \mathbb{N}_0 \to A$$

$$f(n) = f_n$$

Definition 2.3.47 (матриця над множиною). *$p \times q$ – матриця над множиною $\mathbb{L}$*

$$m : \mathbb{N}_p \times \mathbb{N}_q \to A$$

$$m(i, j) = m_{ij}$$

$$M = ||m_{ij}||_{j=\overline{1,q}}^{i=\overline{1,p}}$$

$$M = (m_{ij})_{j=\overline{1,q}}^{i=\overline{1,p}}$$

Definition 2.3.48 (m-арна операція). *m-арна операція над A, це відображення виду:*

$$\circledast : A^m \to A.$$

Definition 2.3.49 (m-арний предикат). *m-арний предикат над A, це відображення виду:*

$$P : A^m \to \{0, 1\}.$$

Example 2.41 (Нуль-арна операція). *Нуль-арна операція – це певна константа*

Example 2.42 (Унарна операція). *Унарна операція: $++$, $-x$, x^2, $\overline{A}$, $ditA$.*

Example 2.43 (Бінарні операції). *Бінарні операції: $+$, $-$, $\div$, $\cap$, $\setminus$, $\wedge$, $\oplus$.*

Example 2.44 (Тернарні операції). *Тернарні операції: $x?y : z$.*

Example 2.45 (Дужки Айверсона). *Нехай P – деяке твердження (предикат).*

$$[P] = \begin{cases} 1- \textit{істина} \\ 0- \textit{хиба} \end{cases}.$$

Example 2.46 (Дельта Кронекера). *Дельта Кронекера:*

$$\sigma_{xy} = \begin{cases} 1 & x = y \\ 0 & x \neq y \end{cases} = [x = y].$$

Definition 2.3.50 (алгебра (алгебраїчна система)). *Нехай A – множина, W – множина операцій над A (можливо $\varnothing$), R – множина відношень над A (можливо $\varnothing$), але W і R не порожні одночасно, тоді $< A, W, R >$ – алгебра (алгебраїчна система) над A.*

Example 2.47. $< A, \{\cup, \cap, \setminus, \triangle, \overline{B}\}, \{\subseteq, \subset, =, \neq\}, \{\varnothing, \mathbb{U}\} >$ *– алгебра множин.*

Example 2.48. $< \mathbb{Z}_n, +, \cdot >$*, де $+$ – додавання за модулем n, $\cdot$ – множення за модулем n.*

Example 2.49. $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

Example 2.50. $< \mathbb{C}, +, -, \cdot, \div >$*, де*

$$\mathbb{C} = \{a + ib \mid \forall a, b \in \mathbb{R}\} \quad \mathbb{C} \sim \mathbb{R}^2$$

Якщо $z_1 = a + ib$, $z_2 = c + id$ то:

$$z_1 \pm z_2 = (a \pm c) + i(b \pm d)$$

$$z_1 \cdot z_2 = (a + ib)(c + id) = (ac - bd) + i(bc + ad)$$

2.3.13 Характеристичі функції множини

Нехай $\mathbb{U}$ – універсум, $A \subseteq \mathbb{U}$.

Definition 2.3.51 (Характеристична функція). *Характеристична функція це функція вигляду $\chi_A(x) : \mathbb{U} \to \{0, 1\}$:*

$$\chi(a) = \begin{cases} 1 & a \in A \\ 0 & a \notin A \end{cases} = [a \in A].$$

Характеристичні функції – це інший спосіб представлення множин

Theorem 2.20.
1. $\chi_{A \cup B}(a) = \max\{\chi_A(a), \chi_B(a)\}$
2. $\chi_{A \cap B}(a) = \min\{\chi_A(a), \chi_B(a)\}$
3. $\chi_{\overline{A}}(a) = 1 - \chi_A(a)$
4. $\chi_{A \setminus B}(a) = \min\{\chi_A(a), 1 - \chi_B(a)\}$
5. $\chi_{A \triangle B}(a) = \max\{\min\{\chi_A(a), 1 - \chi_B(a)\}, \min\{1 - \chi_A(a), \chi_B(a)\}\}$

2.3.14 Зліченність і незліченність

Вважаємо, що $|\mathbb{N}| = \aleph_0$.

Definition 2.3.52 (Формальний порядок на потужностях). *Формальний порядок на потужностях:*

$$|X| \leqslant |Y| \Leftrightarrow \exists f : X \to Y \text{ – інєкція}$$

Theorem 2.21 (Кантор Берштейн). *X, Y – множини,*

$$\begin{cases} \exists f : X \to Y \text{ – інєкція} \\ \exists g : Y \to X \text{ – інєкція} \end{cases} \Rightarrow |X| = |Y|.$$

Remark 2.5.

$$X \subseteq Y \Rightarrow |X| \leqslant |Y|.$$

Theorem 2.22. *Нехай A та B – зліченні множини, тоді $A \times B$ – зліченна множина.*

Доведення. Номер пари = кількість кроків черепахи на шляху до пари. Отже, це бієкція на $\mathbb{N}$. □

Corollary 2.22.1.

$$\forall m \in \mathbb{N} \quad A_i\text{– зліченна}, i = \overline{1, m} \Rightarrow A_1 \times A_2 \times ... \times A_m\text{– зліченна множина}$$

Theorem 2.23.

$$A_1, A_2, ..., A_m\text{– зліченні} \Rightarrow \bigcup_{i=1}^{m} A_i\text{– зліченна множина.}$$

Theorem 2.24. *Нехай A_i – зліченна, $i < \aleph_0$, тоді $\bigcup\limits_{i=1}^{\infty} A_i$ – зліченна*

Доведення. Доведення випливає з аксіоматики теорії множин і аксіоми вибору. □

Claim 2.13 (Аксіома вибору). *$\{x\}$ – система множини $\Rightarrow \exists$ функція f, що $\forall X : f(X) \in X$.*

Claim 2.14 (Аксіома зліченного вибору). *$\exists$ функція f, що $\forall X : f(X) \in X \Rightarrow \{x\}$ – зліченна система множин.*

Corollary 2.24.1.

$$|\mathbb{Z}| = |\mathbb{N}| = \mathbb{N} \cup (-\mathbb{N}) \cup \{0\}.$$

$$|\mathbb{Q}| = |\mathbb{N}|, \quad \mathbb{Q} \subseteq \mathbb{Z} \times \mathbb{N}.$$

$$A \text{ – зліченна} \Rightarrow A[x] \text{ – зліченна}$$

$$\text{Де } A[x] = \{a_n x^n + a_{n+1} x^{n+1} + ... \mid n \in \mathbb{N}_a, a \in A\}$$

Definition 2.3.53 (Поліном). *Поліном – це многочлен, сума декількох одночленів.*

2.3.15 Зліченність та не зліченність

Claim 2.15. *A – зліченна $\Rightarrow A^*$ – зліченна.*

Definition 2.3.54 (Алгебраїчні числа)**.** *Алгебраїчні числа – корені всіх рівнянь виду*

$$q_n x^n + q_{n-1} x^{n-1} + ... + q_1 x + q_0, n \in \mathbb{N}_0, q_i \in \mathbb{Q}$$

Definition 2.3.55 (множина всіх алгебраїчних чисел)**.** *$\mathbb{A}$ – множина всіх алгебраїчних чисел.*

$\mathbb{A}$ – зліченна.

Definition 2.3.56 (Обчислювані числа)**.** *Обчислювані числа – існує алгоритм обчислення із наперед заданою точністю, – зліченна кількість кроків.*

Theorem 2.25 (Теорема Кантор)**.** *Множина $\{0,1\}^{\mathbb{N}}$ – назліченна.*

Доведення. Нехай $\{0,1\}^{\mathbb{N}}$ – зліченна, пронумеруїм їх

$b = b_1, b_2, b_3, ...$

Який номер має b.

$\forall i \quad b_i = 1 - a_i^{(i)}$

b – не співпадає з жодною $\overline{a}^{(i)}$ □

Corollary 2.25.1. *A – $\leqslant$ – зліченна $\Rightarrow A^{\mathbb{N}}$ – незліченна.*

Corollary 2.25.2. *A – зліченна множина.*

$$A[[x]] = \{\sum_{n=0}^{\infty} a_n x^n \mid a_n \in A\} \text{– незліченна}$$

Corollary 2.25.3. *A – зліченна $\Rightarrow 2^A$ – незліченна*

$$B \subseteq A \Leftrightarrow \chi_b$$

Corollary 2.25.4. *$\mathbb{R}$ – незліченна*

1. $\mathbb{R} \sim (0,1)$
2. $x \in (0,1) \Rightarrow x = 0, x_1, x_2, ..., \Rightarrow \mathbb{R} \sim 2^{\mathbb{N}}, \quad |\mathbb{R}| = 2^{\aleph}$

Corollary 2.25.5. *$\mathbb{I} = \mathbb{R} \backslash \mathbb{Q}$ – множина ірраціональних чисел.*

$\mathbb{R} = \mathbb{Q} \cup \mathbb{I} \Rightarrow \mathbb{I}$ – незліченна

$|\mathbb{R}| = \mathfrak{C}$ – потужність континум.

$A \sim \mathbb{R}$ множина потужність континум або конинуальна множина

Theorem 2.26 (Теорема Кантор)**.**

$$\forall A : |A| < |2^A|.$$

Розглянемо $B = \{\{a\} \mid a \in A\}$.

$$\begin{cases} B \sim A \\ B \subset 2^A \end{cases} |A| \subseteq |2^A|.$$

Нехай $A \sim 2^A \Rightarrow \exists \varphi : A \to 2^A$ – бієкція. $\forall a \in A \quad \varphi(a) \subseteq A$.

a – жовтий $\Leftrightarrow a \in \varphi(a)$.

b – блакитний $\Leftrightarrow a \notin \varphi(a)$.

$\varphi^{-1}(\varnothing)$ – блакитний $\varphi^{-1}(A)$ – жовтий

Нехай A_0 – множина всіх блакитних елементів $a_0 = \varphi^{-1}(A_0)$.

a – жовте $\Rightarrow a_0 \in \varphi(a_0) \Rightarrow a_0 \in A_0 \Rightarrow$ протиріччя

b – блакитне $\Rightarrow a_0 \notin \varphi(a_0) \Rightarrow a_0 \notin A_0 \Rightarrow$ протичіччя

Отдже $|A| < 2^A$.

Hypothesis 2.1 (Континум гіпотеза). *У множині дійсних чисел всі підмножини скінченні, зліченні або континуальні (між $\aleph_0$ та $\mathfrak{C} = 2^{\aleph_0}$ не існує жодних інших кардинальних чисел).*

Hypothesis 2.2 (Узагальнення континум гіпотези).

$$\forall A, B, \quad |A| > |B| \geqslant \aleph_0 \Rightarrow |A| \geqslant |2^B|.$$

Theorem 2.27 (Теорема К1). *Множина $\{0,1\}^{\mathbb{N}}$ – незліченна.*

Theorem 2.28 (Теорема К1.5). *Множина A – злічення $\Rightarrow 2^A$ булеан – незліченний.*

Theorem 2.29 (Теорема К1.75). *$\mathbb{R}$ – незліченна.*

Theorem 2.30 (Теорема К2). $\forall A : |2^A| > |A|$.

2.4 Узагальнення поняття множини

2.4.1 Мультимножини

1970 рік де Брюейн (Le Brujin)

Definition 2.4.1 (Мультимножини). *Мультимножини (mult set) $A =< A(A) : \chi_A >$.*

Definition 2.4.2 (множина носій). *$S(A)$ – множина носій.*

Definition 2.4.3 (функція кратності (кількість елементів)). *$\chi_A S(A) \Rightarrow \mathbb{N}_0$ – функція кратності (кількість елементів).*

Definition 2.4.4.

$$A = \{a, a, a, b, b, c\}$$
$$A = \{a^3, b^2, c^1\}$$
$$A = \{(a, 3), (b, 2), (c, 1)\}$$

2.4.2 Операції над мультипідмножинами

1. Об'єднання $A \cup B$:
$$\forall a \quad \chi_{A \cup B}(a) = \max\{\chi_A(a), \chi_B(a)\}.$$
2. Перетин $A \cap B$:
$$\forall a \quad \chi_{A \cap B}(a) = \min\{\chi_A(a), \chi_B(a)\}.$$
3. Різниця $A \backslash B$:
$$\forall a \quad \chi_{A \backslash B}(a) = \chi_A(a) \dot{-} \chi_B(a).$$
4. Симетрична різниця – не визначається
5. Доповнення мультмножини – не визначається
6. Сума $A + B$:
$$\forall a : \chi_{A+B}(a) = \chi_A(a) + \chi_B(a).$$
7. Включення
$$A \subseteq B \Leftrightarrow \forall a : \chi_A(a) \leqslant \chi_B(a).$$
$$A \subset B \Leftrightarrow (A \subseteq B) \& (\exists a : \chi_A(a) < \chi_B(a)).$$
8. Декартів добуток
$$C = A \times B \Leftrightarrow (S(c) = S(a) \times S(b)) \& (\chi_C(a, b) = \chi_A(a) \cdot \chi_B(b)).$$
9. Булеан $\mathcal{B}(A)$ – множина мультипідмножин.
10. Потужність мультимножини.
$$a = \sum_{a \in S(A)} \chi_A(a).$$

Theorem 2.31.
$$|\mathcal{B}(A)| = \prod_{a \in S(A)} (\chi_A(a) + 1).$$

Доведення. $a \in S(A)$ може входити $0, 1, ..., \chi_A(a)$ раз $\Rightarrow \chi_A(a) + 1$ способів. $\square$

Example 2.51.
$$C = \{a^6 m b^5 m c^5 n d^4\}.$$
$$|\mathcal{B}(C)| = 7 \cdot 6 \cdot 6 \cdot 5 = 1260.$$

2.4.3 Нечіткі множини

Definition 2.4.5 (Нечітка множина (fussy set)). *Нечітка множина (1965 рік, Лорті Зоде) – це впорядкована пара (fussy set)*

$$A =< S(A), \chi_A >,$$

$S(A)$ *– множина носій,* $\chi_a : S(A) \to [0, 1]$ *– степінь входження елемента.*

Сфера використання

1. Математична лінгвістика
2. Теорія прийняття рішень
3. Біоінформатика
4. Кластерний аналіз
5. Нечітка логіка

Способи подання

$$A = \{(a, 0.1), (b, 0.9), (c, 0.9998), (d, 0.5)\}$$

Класична множина – це чітка множина.

Операції над нечіткими множинами

1. Об'єднання $A \cup B$:
$$\forall a \quad \chi_A(a) = \max\{\chi_A(a), \chi_B(a)\}.$$
2. Перетин $A \cap B$:
$$\forall a \quad \chi_A(a) = \min\{\chi_A(a), \chi_B(a)\}.$$
3. Доповнення $\overline{A}$:
$$\forall a \quad \chi_{\overline{A}}(a) = 1 - \chi_A(a).$$
4. Різниця $A \backslash B$:
$$\chi_{A\backslash B}(a) = \chi_A(a) \dot{-} \chi_B(a).$$
$$A\backslash B = A \cap \overline{B} \quad \chi_{A\cap B}(a) = \min\{\chi_A(a), 1 - \chi_B(a)\}.$$
5. Добуток $A \cdot B$:
$$\forall a : \quad \chi_{A\cdot B}(a) = \chi_A(a) \cdot \chi_B(a).$$
6. Сума $A + B$:
$$\forall a \quad \chi_{A+B}(a) = \chi_A(a) + \chi_B(a) - \chi_A(a) \cdot \chi_B(a).$$
7. Включення:
$$A \subseteq B \Leftrightarrow \forall a \quad \chi_A(a) \leqslant \chi_B(a).$$
$$A \subset B \Leftrightarrow (A \subseteq B)\&(\exists a \quad \chi_A(a) < \chi_B(a)).$$
8. Нечітка рівність:
$$E(A \equiv_E B) = 1 - \max(\chi_A(a) - \chi_B(a))$$
9. Нечітке включення $A \subseteq_E B$

Claim 2.16.

$$C = A + B \Leftrightarrow \overline{C} = \overline{A} \cdot \overline{B}.$$

Доведення.

$$\begin{aligned}
\overline{C} = \overline{A} \cdot \overline{B} \quad &\Rightarrow \quad \forall a \quad \chi_C(a) = \chi_A(a) \cdot \chi_B(a) \\
&\Rightarrow \quad \forall a \quad 1 - \chi_C(a) = (1 - \chi_A(a)) \cdot (1 - \chi_B(a)) \\
&\Rightarrow \quad 1 - \chi_C(a) = 1 - \chi_A(a) - \chi_B(a)) + \chi_A(a) \cdot \chi_B(a)) \\
&\Rightarrow \quad \forall a \quad \chi_C(a) = \chi_A(a) + \chi_B(a)) - \chi_A(a) \cdot \chi_B(a)) \\
&\Rightarrow \quad C = A + B.
\end{aligned}$$

□

2.5 Вступ до комбінаторики

Definition 2.5.1 (Комбінаторика (Комбінаторний аналіз))**.** *Комбінаторика (Комбінаторний аналіз) – напрямок дискретної математики, що займається такими питаннями:*

1. *Існування об'єктів у заданій системі умов та обмежень.*
2. *Підрахунок кількості об'єктів.*
3. *Алгоритми ефективного перебору.*
4. *Комбінаторна оптимізація.*
5. *Екстримальні задачі.*

Комбінаторна конфігурація:

1. Процедура побудова об'єкту.
2. Результати роботи.

Claim 2.17 (Головні принципи комбінаторних операцій)**.**

1. *Правило суми: якщо A будується n способами а B – k способами, і способи не перетинаються, то A або B будується $n + k$ способами.*
2. *Правило добутку: якщо A будується n способами а B – k способами, то A і B будується $n = k$ способами.*
3. *Правило Діріхле: при розташуванні k об'єктів по n комірках ($k > n$) існує комірки з $\geqslant 2$ обектами.*

2.5.1 Основні комбінаторні конфігурації

Один зі способів опису комбінаторної конфігурації – розташування об'єктів по комірках.

Об'єкти та комірки можуть бути пронумеровані (розрізнювані) або ні.

У комірці може розташовуватись обмежена або не обмежена кількість об'єктів.

Definition 2.5.2 (Розміщення із повторенням)**.** $\overline{A}_n^k$ *– кількість розміщень з повторенням n об'єктів на k комірок*

$$\overline{A}_n^k = n^k.$$

Definition 2.5.3 (Розміщення без повторень). *$A_n^k = n^k$ – кількість без повторень n об'єктів по k комірках*

$$A_n^k = \frac{n!}{(n-k)!}.$$

Definition 2.5.4 (Перестановки: розміщення без повторень).

$$\overline{P}_n = A_n^n = \frac{n!}{0!} = n!$$

Definition 2.5.5 (Підстановка). *Підстановка – бієктивне відображення $\pi : X \to X$.*

Definition 2.5.6 (Перестановка з повторенням (Permutation)). *Нехай є мультимножина $A = \{a_2^{n_1}, a_2^{n_2}, ..., a_k^{n_k}\}$, тоді $P_n^{n_1 n_2 \dots n_k}$ – кількість перестановок.*

Claim 2.18.

$$P_n^{n_1 n_2 \dots n_k} = \frac{n!}{n_1! n_2! \dots n_k!}, \quad n = |A|$$

Доведення. нехай всі елементи A є різними $\mathcal{P}$ – множина всіх перестановок A

$$|\mathcal{P}| = n!$$

Введемо $\sim_1$ $\pi_1 \sim_1 \pi_2 \Leftrightarrow \pi_1$ і π_2 відрізняються взаємними розташуванням елементів $a_1 \Rightarrow$ Кожен клас еквівалентності містить $n!$ елементів.

$$\mathcal{P}' = {}^{\mathcal{P}}\!\big/_{\sim_1}, \quad |\mathcal{P}'| = \frac{n!}{n_1!}$$

вводимо $\sim_2$ – розташування об'єктів a_2.

$$\mathcal{P}'' = {}^{\mathcal{P}'}\!\big/_{\sim_2}, \quad |\mathcal{P}''| = \frac{n!}{n_1! n_2!}$$

□

Example 2.52. *Скільки існує шляхів від $(0, 0)$ до (n, k) якщо можна ходити вверх і вправо.*

Кількість шляхів:

$$P_{n+k}^{n,k} = \frac{(n+k)!}{n!k!}$$

Definition 2.5.7 (Вибірки без повторень). *Вибірки без повторень: розташування без повторень але комірки є нерозрізнюваними $\Rightarrow$ k-вибірки $\Rightarrow$ підмножина розміру k.*

C_n^k – кількість вибірок з n по k.

Claim 2.19.

$$C_n^k = \frac{n!}{k!(n-k)!}, \quad 0 \leqslant k \leqslant n$$

Доведення. Нехай $\mathcal{G}_n^k$ – множина всіх розміщень без повторень з n обєктів по k.

$$|\mathcal{G}_n^k| = A_n^k$$

вводимо $\sim$ відношення розпорядкування на d_n^k $a_1 \sim a_2 \Leftrightarrow$ розміщення a_1 і a_2 відрізняється лише взаємним порядком елементів $\Rightarrow$ кожен клас еквівалентності складається з P_k елементів $\Rightarrow C_n^k = |{}^{d_n^k}\!\diagup\!\sim| = \dfrac{A_n^k}{P_k} = \dfrac{n!}{k!(n-k)!}$ □

Definition 2.5.8 (Вибірки з повторенням)**.** *Можна обрати об'єкт кілька разів $\Rightarrow f$ – вибірка з повторенням = мультипідмножина потужності k у звичайній множині.*

Claim 2.20.

$$\overline{C}_n^k = c_{n+k-1}^k$$

Доведення.

$$A = \{a_1, a_2, ..., a_n\}$$

$$B \subseteq A \quad B = \{a_1^{k_1}, a_2^{k_2}, ..., a_n^{k_n}\} \quad \forall i : h_i \geqslant 0$$

$$k_1 + k_2 + k_3 + ... + k_n = k$$

$$\underbrace{111...1}_{k_1}\,0\,\underbrace{111...1}_{k_2}\,0\,\underbrace{111...1}_{k_3}\,0...0\,\underbrace{111...1}_{k_n}$$

k одиниць, $(n-1)$ нулів.

$\overline{C}_n^k$ - Кількість таких бітових векторів

$$\overline{C}_n^k = P_{n+k-1}^{n+1,k} = \frac{(n+k-1)!}{k!(n-1)!} = C_{n+k-1}^k$$

□

2.5.2 Представлення комбінаторних операцій через відображення

Табл. 2.1: Дванадцятковий шлях (Джак Карл Фота). Тут Y – це Комірки (місця), X – це об'єкти (мітки). X – це впорядкована або ні, Y – це впорядкована або ні, f – це довільне відображення, інєкція, сюрєкція.

Y	X	f-довільна	f-інєктивна	f-сюрєктивна

Y	X	f-довільна	f-інєктивна	f-сюрєктивна
вп	вп	Розміщення з повторенням n^k	Розміщення без повторення $A_n^k = \dfrac{n!}{(n-k)!}$	Впорядковані розбиття $M(n, k)$
	нвп	Вибірка з повторенням $\overline{C}_n^k$	Вибірка без повторення C_n^k	Вибірка з повторенням, включаючи всю Y $pass$
нвп	вп	Розбиття X на довільну кількість частин $B(k)$	Вироджений випадок $1 \to 1$	Розбиття X на n частин $S(k, n)$
	нвп	Розбиття числа на доданки (в n не більше) $pass$	Вироджений випадок $1 \to 1$	Розбиття натурального числа на доданків $pass$

Кількість сюрєктивних відображень на рисунку = кількість розташувань з повторенням які використовують всі об'єкти

Властивість $P_i : y_i \notin f(X)$

Сюрєктивна функція – не задовільняє P_i

Нехай $A_i = \{f : X \to Y \mid f \text{ задовольняє } P_i\}$

$\Rightarrow M(n, k) = |Y^X| - |A_1 \cup A_2 \cup ... \cup A_n|$

$\forall i \quad |A_i| = (n-1)^k$

$\forall i, j \quad |A_i \cap A_j| = (n-2)^k$

$|A_1 \cap ... \cap A_t| = (n-t)^k$

$$M(n,k) = n^k - C_n^1(n-1)^k + C_n^2(n-2)^k - C_n^3(n-3)^k + ...(-1)^n C_n^n(n-n)^k$$
$$= \sum_{t=0}^{n}(-1)^t C_n^t(n-t)^k.$$

Definition 2.5.9 (Число Моргана). *Число Моргана $M(n,k)$ це:*

1. *Кількість сюр'єктивних відображень з k елементної множини на n елементну множину.*
2. *Кількість впорядкованих розбиттів (композицій) k елементної множини на n частини.*

2.5.3 Кількість розбиттів

Definition 2.5.10 (Число Стірлінга II роду). *Число Стірлінга II роду $S(n,k)$ – це кількість розбиттів n елементної множини на k частин.*

$$S(n,k) = \frac{1}{k!}M(k,n).$$

Theorem 2.32.

$$S(n+1,k) = S(n,k-1) + kS(n,k)$$
$$S(n,1) = S(n,n) = 1$$

Доведення. $\Pi_1 = \{A\} \Rightarrow S(n,1) = 1$,

$\Pi_2 = \{\{a_1\},\{a_2\},...,\{a_n\}\} \Rightarrow S(n,n) = 1$,

$A' = \{a_1, a_2, ..., a_n, a_{n+1}\}$,

$S(n+1,k)$ – кількість розбиттів на k частин,

1. $\Pi = \{\{a_{n+1}\}$, розбиття $A = \{a_1, a_2, ..., a_n\}$на$k-1$ частин $\} \Rightarrow S(n,k-1)$ розбиттів
2. $\Pi = \{\{A_{n+1}, ...\}, ...\}$. Якщо вилучимо A_{n+1} розбиття A на k частин $\Rightarrow S(n,k)$. Повертаємо $A_{n+1} \to k \times S(n,k)$.
   $S(n+1,k) = S(n,k-1) + k + S(n,k)$

□

Definition 2.5.11 (Число Белла). *Число Белла $B(n)$ – це загальна кількість розбиттів елементної множини.*

$$B(n) = \sum_{k=1}^{n} S(n,k).$$

Theorem 2.33.

$$B(n+1) = \sum_{k=0}^{n} C_n^k B(n-k), \quad B(0) = 1$$

Доведення. $A = \{a_1, a_2, ..., a_{n+1}\}$

$\Pi = \{\{a_{n+1}, ...a_{n+t}\}, ...\}, \quad t \in \{0, 1, ..., n\}$.

Таких Π існує $C_n^t B(n-t)$.

Загальна кількість розбиттів $B(n+1) = \sum\limits_{t=1}^{n} C_n^t B(n-t)$ $\square$

Розбиття числа на доданки

- не існує аналітичної формули
- не існує скінченної рекурентної формули
- існує асимптотична формула

2.5.4 Лінійні діофантові рівняння

$$x_1 + x_2 = ... + x_k = n$$
$$x_1, x_2, ..., x_n \in \mathbb{Z}$$
$$n \in \mathbb{N}$$

1. $x \geqslant 1$
   Кількість розвязків = кількість способів розбити n на k доданків - впорядковано, тобто (1 + 2) та (2 + 1) – різні.
   Метод паличок
   $$\underbrace{\overbrace{III...I}^{x_1} + \overbrace{III...I}^{x_1} + ... + \overbrace{III...I}^{x_1}}_{N}$$
   треба переставити $(k-1)$ знак + на $(n-1)$ місце $\Rightarrow C_{n-1}^{k-1}$ розв'язків
2. $x \geqslant 0$ (де $1+0+2$ і $1+2+0$ – різні)
   можна поставити декілька + на одне місце. Отже маємо $(k-1)$ pyfr +, та $(n+1)$ місце, а отже:
   $\overline{C_{n+1}^{k-1}} = C_{n+1+k-1-1}^{k-1} = C_{n+k-1}^{k-1}$ розв'язків.

Remark 2.6. Альтернативне доведення другого пункту через перший:

$y_i = x_i + 1$, $y_i \geqslant 1$, $y_1 + y_2 + ... + y_n = n + k$.

Отже, маємо C_{n+k-1}^{k-1} розвязків.

2.5.5 Біном Ньютона

$$(a+b)^n = \sum_{k=1}^{n} C_n^k a^{n-k} b^k \tag{2.1}$$

C_n^k – біноміальні коефіціанти.

2.5.6 Властивості біноміальних коефіцієнтів

1. $C_n^k = C_n^{n-k}$.
$$\frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)!(n-(n-k))!}.$$
2. $C_n^k + C_n^{k+1} = C_{n+1}^{k+1}$.

2.5.7 Трикутник паскаля

1. Трикутник паскаля

$$\begin{array}{ccccccccc}
 & & & & 1 = C_0^0 & & & & \\
 & & & 1 = C_1^0 & & 1 = C_1^1 & & & \\
 & & 1 = C_2^0 & & 2 = C_2^1 & & 1 = C_2^2 & & \\
 & 1 = C_3^0 & & 3 = C_3^1 & & 3 = C_3^2 & & 1 = C_3^3 & \\
1 = C_4^0 & & 4 = C_4^1 & & 6 = C_4^2 & & 4 = C_4^3 & & 1 = C_4^4
\end{array}$$

2. $C_k^k + C_{k+1}^k + C_{k+2}^k + ... + C_n^k = C_{n+1}^{k+1}$.
3. $C_{n+2}^{k+2} = C_n^{k+2} + 2C_n^{k+1} + C_n^k$.

2.5.8 Згортка Вандермонда

$$C_{n+m}^k = \sum_{t=0}^{k} C_m^t C_n^{k-t} \tag{2.2}$$

- для $1 - C_m^0 C_n^k$
- для $2 - C_m^1 C_n^{k-1}$
- для $3 - C_m^2 C_n^{k-2}$
- для $t - C_m^t C_n^{k-t}$

$f(x) = (1+x)^n = \sum\limits_{k=0}^{n} C_n^k x^k$.

$x = 1 \quad 2^n = \sum\limits_{k=0}^{n} C_n^k$

$x = -1 \quad 0 = \sum\limits_{k=0}^{n} (-1)^k C_n^k \Rightarrow C_n^0 + c_N^2 = C_n^1 + C_n^3 + ...$

$f'(x) = n(1+x)^{n-1} = \sum\limits_{k=0}^{n} C_n^k k x^{k-1}$

$x = 1 \quad n2^{n-1} = \sum\limits_{k=1}^{n} k C_n^k$

$x = -1 \quad 0 = \sum\limits_{k=1}^{n} (-1)^k k C_n^k$

$\int x \, \mathrm{d}x = \frac{x^{n=1}}{n+1} + const$

$\int f(x)\,\mathrm{d}x = \frac{f(x)^{n+1}}{(n+1)}\Big|_0^x = \frac{(1+x)^n - 1}{n+1} = \sum\limits_{k=0}^{n} \frac{C_N^k - x^{n+1}}{k+1}$

$x = 1 \quad \sum\limits_{k=0}^{n} \frac{C_n^k}{k+1} = \frac{2^{n+1}-1}{n+1}$

$x = -1 \quad \sum\limits_{k=0}^{n} \frac{(-1)^{k+1} C_1^k}{k+1} = -\frac{1}{n+1}$

2.6 Булеві функції

Нехай $V_n = \{0,1\}^n$ – булевий вектор.

2.6.1 Булеві функції

Definition 2.6.1 (Одновиміна булева функція)**.** *Одновиміна булева функція від n змінних*

$$f : V_n \to \{0,1\} :$$

BF_n – множина всіх булевих функцій від n змінних

Definition 2.6.2 (m-вимірна булева функція)**.** *m-вимірна булева функція від n змінних:*

$$F : V_n \to V_m$$

$BF_{n,m}$– множина усіх булевих функцій

Remark 2.7. Кожна m-вимірна булева функція може бути подана як

$$F(x_1, x_2, ..., x_n) = (f(x_1, ..., x_n), f_2(x_1, ..., x_n), ..., f_m(x_1, ..., x_n))$$

де f_i – координати функції. Звідси

$$BF_{n,m} \sim \underbrace{BF_n \times BF_n \times ... \times BF_n}_{m}$$

Lemma 2.5.

$$|BF_n| = |\{0,1\}^{V_n}| = |\{0,1\}|^{|V_n|} = 2^{2^n}$$
$$|BF_{n,m}| = (2^m)^{2^m}$$

Definition 2.6.3 (Таблиця інцидентності)**.** *Таблиця інцидентності – це таблиця співставлення всіх можливих вхідних значень, та відповідних їм значень булевої функції*

Зазвичай види значень розташовані лексикографічно, наприклад як на таблиці 2.2.

Вектор значень $T_f = (t_0, t_1, t_2, ..., t_{2^n-1})$

$t_i = f$ (вектор, що відповідає запису числа i у двійковій системі числення)

1. Нульарна булева функція: 0 та 1.

x	y	z	maj
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Табл. 2.2: maj – повертає 1, якщо одиниць більше ніж нулів.

2. унарні булеві функції

x	0	1	x	$\overline{x}$
0	0	0	1	1
1	0	1	0	1

Remark 2.8. $\overline{x}$, $\neg x$, $notx$, $\overline{x} = 1 - x$.

3. Бінарні булеві функції

x	y	$x \vee y$	$x \wedge y$	$x \equiv y$	$x \oplus y$	$x \to y$	$x \leftarrow y$	$x \downarrow y$	$x \vert y$
x	y	OR	AND	$x \equiv y$	XOR	$IMPLY$	$x \leftarrow y$	NOR	$NAND$
0	0	0	0	1	0	1	1	1	1
0	1	1	0	0	1	1	0	0	1
1	0	1	0	0	1	0	1	0	1
1	1	1	1	1	0	1	1	0	0

- $x \vee y$ – дизюнкція (логічне або (OR), disjunction)
- $x \wedge y$ – конюкція (логічне та (AND), conjunction)
- $x \equiv y$, $x \sim y$, $x \leftrightarrow y$ – еквівалентність $(x \oplus y = \neg(x \sim y))$
- $x \oplus y$ – виключне або (exclusive or, (XOR)), додавання за модулем 2
- $x \to y$ – імплікація
- $x \leftarrow y$ – зворотна імплікація
- $x \downarrow y$ – стрілка Пірса (NOR) $(x \downarrow y = \neg(x \vee y))$
- $x|y$ – штрих Шефера (NAND)
- – константи 0 і 1
- – проектори $Pr_1(x, y) = x$, $Pr_2(x, y) = y$
- – заперечення проекторів $f(x, y) = \overline{x}$, $f(x, y) = \overline{y}$
- – заперечення імплікації

2.6.2 Алгебраїчні властивості бітових операцій

Definition 2.6.4 (Булева алгебра)**.** $\langle \{0, 1\}, \{\vee, \&, \sim, \to, \leftarrow, \downarrow, |, \neg, 0, 1, ...\} \rangle$ – *булева алгебра*

Remark 2.9. Булева алгебра дуже подібна до алгебри множин:

- $\cup \equiv \vee$
- $\cap \equiv \wedge$
- $\triangle \equiv \oplus$
- $\subseteq \equiv \to$
- $= \equiv \sim$
- $\mathfrak{U} \equiv 1$
- $\varnothing \equiv 0$
- $\overline{A} \equiv \neg$

1.

$$x \vee x = x \wedge x = x$$
$$\overline{\overline{x}} = x$$

2.

$$x \vee y = y \vee x$$
$$x \& y = y \& x$$
$$x \oplus y = y \oplus x$$
$$x \sim y = y \sim x$$

3.

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

4.

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

5.

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

6.

$$\overline{x \vee y} = \overline{x} \& \overline{y}$$
$$\overline{x \& y} = \overline{x} \vee \overline{y}$$

7.

$$X \vee 1 = 1, x \& 1 = x$$
$$X \vee 0 = x, x \& 0 = 0$$

8.

$$x \vee \overline{x} = 1, x \& \overline{x} = 0$$

9.

$$x \sim y = (x \to y) \& (x \leftarrow y)$$

Нехай $\mathcal{F} \subseteq BF_n$. Формула над $\mathcal{F}$ – символічний вираз який будується за такими правилами

1. Будь яка змінна – це формула (літерал)
2. Якщо $t \in \mathcal{F}$, а f_1, f_2, ..., f_n – це формули, то вираз $f(f_1, f_2, ..., f_n)$ це також формула (суперпозиція)
3. Інших формул не існує

Example 2.53.

$$f(x, y, z) = \underbrace{x \vee (y \& x)}_{\mathcal{F}} = \{\vee, \&\}$$
$$g_1(x, y) = x \vee y$$
$$g_2(x, y) = x \& y$$
$$f(x, y, z) = g_1(x, g_2(y, z))$$

Формула φ реалізує булеві функції f_i які мають однакові таблиці істиності. Еквівалентні формули реалізують одну булеву функцію.

Клас функцій $\mathcal{F} \subseteq BF_n$ має нормальну форму, якщо існує клас $\hat{\mathcal{F}} \subseteq BF_n$ $\forall f \in \mathcal{F}$ має унікальне представлення формулою над $\hat{\mathcal{F}}$. $\Rightarrow$ перевірка еквівалентності стає простою, – треба перевірити, що відповідні формули над $\hat{\mathcal{F}}$ співпадають

Формули над $\hat{\mathcal{F}}$ називають нормальними формами булевих функцій $f \in \mathcal{F}$

2.6.3 Нормальна форма булевих функцій

Нехай $x \in V_n$, $x = (x_1, x_2, ..., x_n)$, $f(x_1, x_2, ..., x_n) = f(x)$.

Підфункція булевої функції f – булева функція, яка одержана фіксацією певних вхідних змінних певним значенням.

$f \in BF_n$, f' – підфункція одержана фіксацією k зміних ($f' \in BF_{n-k}$).

$f \in BF_n$, $f_0(x_2, x_3, ..., x_n) = f(0, x_2, ..., x_n)$, $f_1(x_2, x_3, ..., x_n) = f(1, x_2, ..., x_n)$.

Theorem 2.34 (Розклад Шенона, Розклад Буля)**.** $\forall f \in BF_n$

$$f(x_1, x_2, ..., x_n) = x_1 f_1(x_2, x_3, ..., x_n) \vee \overline{x}_1 f_0(x_2, x_3, ..., x_n).$$

Доведення. Obvious by looking on the function table. □

Corollary 2.34.1. *Нехай* $a, b \in \{0, 1\}$*, тоді* $a^b = \begin{matrix} a, & b = 1 \\ \overline{a}, & b = 0 \end{matrix}$.

$$\Rightarrow f(x_1, x_2, ..., x_n) = \bigvee x_1^{a_1} x_2^{a_2} ... x_k^{a_k} f(a_1, ..., a_k, x_{k+1}, ..., x_n).$$

Corollary 2.34.2. *Нехай* $x, u \in V_n$*, тоді* $x^u = x_1^{u_1} x_2^{u_2} ... x_n^{u_n}$.

$$\Rightarrow f(x) = \bigvee_{u \in V_n} f(u) x^u$$

Definition 2.6.5 (Досконала диз'юнктивна нормальна форма (ДДНФ) функції)**.**

$$\Rightarrow f(x) = \bigvee_{u \in V_n} f(u) x^u \text{ – досконала диз'юнктивна нормальна форма функції}$$

Corollary 2.34.3. *Довільну булеву функцію можна представити формулою над системою* $\{\vee, \&, \neg\}$.

Доведення. Якщо $f(x) \not\equiv 0$, то такою формулою є ДДНФ. Якщо $f(x) \equiv 0$, то $f(x) = x_1 \& \overline{x}_1$. □

Definition 2.6.6 (Канонічний базис)**.** *Система* $\mathcal{F} = \{\vee, \&, \neg\}$ *– канонічний базис (базис ТА-АБО-НІ).*

2.6.4 побудова ДДНФ

1. Початкова формула порожня
2. Для всіх $u \in V_n$, для яких $f(u) = 1$, додає ще через V доданок x^u. Якщо $u_i = 1$ ставимо x_i. Якщо $u_i = 0$ ставимо $\overline{x_i}$.
3. Якщо формула залишилась 0, то f – константний нуль, що не має ДДНФ

Example 2.54.

$$maj(x_1, x_2, x_3) = \overline{x}_1 x_2 x_3 \vee x_1 \overline{x}_2 x_3 \vee x_1 x_2 \overline{x}_3 \vee x_1 x_2 x_3.$$

x_1	x_2	x_3	$maj(x_1, x_2, x_3)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Елементарна конюнкція – формула, яка містить лише змінні $\neg$, &.

Дизюнктивна нормальна форма – формула, яка складається з функцій елементарних конюкцій

ДДНФ є досконалою, якщо кожний доданок містить кожну змінну або її заперечення.

Lemma 2.6. *Існує 2^{3^n} ДНФ від n змінних але лише 2^{2^n} ДДНФ*

Існують алгоритми мінімізації ДДНФ

Example 2.55. $f(a, b, c) = (a \downarrow b) \oplus (a|b)$.

1. $a \downarrow b = \overline{a \vee b} = \overline{a} \wedge \overline{b} = \overline{a}\overline{b}$.
2. $a|b = \overline{a \wedge b} = \overline{a} \vee \overline{b}$.
3. $u \oplus v = \overline{u} \vee \overline{v}$.
4. $(a \downarrow b)(\overline{a} \vee \overline{c}) = \overline{(a \downarrow b)}(a|c) \vee (a \downarrow b)\overline{(a|c)} = (a \vee b)(\overline{a} \vee \overline{C}) \vee \overline{a}\overline{b}ac = (a \vee b)(\overline{a} \vee \overline{c}) \vee \overline{a}\overline{b}ac = a\overline{a} \vee a\overline{c} \vee b\overline{a} \vee \overline{b}\overline{c} = a\overline{c} \vee \overline{a}b \vee b\overline{c}$.
5. $a\overline{c} = a\overline{c}(b \vee \overline{b})$.

Definition 2.6.7 (Двоїста функція булевої функції)**.** *Двоїста функція булевої функції $f \in BF_n$.*

$$f^*(x_1, x_2, ..., x_n) = \neg f(\overline{x}_1, \overline{x}_2, ..., \overline{x}_n). \tag{2.3}$$

Example 2.56. *Двоїста функція булевої функції.*

1. $f(x) = \overline{x} \Rightarrow f^*(x) = \neg f(\overline{x}) = \neg(\overline{\overline{x}}) = \overline{x}$.
2. $f(x, y) = x \vee y \Rightarrow f^*(x, y) = \neg f(\overline{x}, \overline{y}) = \neg(\overline{x} \vee \overline{y}) = \overline{\overline{x}} \& \overline{\overline{y}} = xy$.

$\vee$ та & – пара двоїстих функцій.

Lemma 2.7.
$$f^{**}(x) = f(x)$$

Доведення.

$$f^*(x) = \neg f(\overline{x}) \Rightarrow f^{**}(x) = \neg f^*(\overline{x}) = \neg\neg f(\overline{\overline{x}}) = f(x).$$

□

2.6.5 Побудова двоїстої функції за таблицею істиності

1. Перевернути вектор значень догори ногами.
2. Інвертуємо всі значення.

Theorem 2.35 (Про двоїсті функції)**.** *Нехай $\mathcal{F} = \{f\}$, $\mathcal{F}^* = \{f^*\}$. Якщо φ – це формула над $\mathcal{F}$, яка реалізовує функцію F, то функція φ^* одержана шляхом заміни всіх f_i на f_i^* реалізує F^*.*

Доведення. Доводиться індукцією за побудовою суперпозиції □

Corollary 2.35.1. $\mathcal{F}_k^* = \mathcal{F}_k \Rightarrow$ *якщо в ДНФ функції f замінити всі "ТА" на "АБО" і навпаки, то одержимо формулу для f^**

$$f^*(x) = \bigvee_{u \in V_n} f^*(u) x^u = \bigvee_{u \in V_n} f^*(u) x_1^{u_1} x_2^{u_2} ... x_n^{u_n} \Rightarrow$$

$$\begin{aligned}
f(x) &= \bigwedge_{\substack{u \in V_n \\ f^*(u)=1}} (x_1^{u_1} \vee x_2^{u_2} \vee ... \vee x_n^{u_n}) \\
&= \bigwedge_{\substack{u \in V_n \\ f^*(\overline{u})=0}} (x_1^{u_1} \vee x_2^{u_2} \vee ... \vee x_n^{u_n}) \\
&= \bigwedge_{\substack{u \in V_n \\ f(\overline{u})=0}} (x_1^{u_1} \vee x_2^{u_2} \vee ... \vee x_n^{u_n}) \\
f^*(u) = 1 &\Rightarrow \neg f(\overline{u}) = 1 \Rightarrow f(\overline{u}) = 0 \\
&= \bigwedge_{\substack{u \in V_n \\ f(u)=0}} (x_1^{\overline{u_1}} \vee x_2^{\overline{u_2}} \vee ... \vee x_n^{\overline{u_n}}) \\
\Rightarrow f(x) &= \bigwedge_{\substack{u \in V_n \\ f(u)=0}} (\overline{x}_1^{u_1} \vee \overline{x}_2^{u_2} \vee ... \vee \overline{x}_n^{u_n})
\end{aligned}$$

– Досконала конюктивна нормальна форма булевої функції

2.6.6 Побудова ДКНФ

1. Початкова формула порожня
2. Для всіх $u \in V_n$ таких, що $f(u) = 0$, ми множимо формулу на множник виду:
   (а) якщо $u_i = 1$, то $\overline{x}_1$,
   (б) якщо $u_i =$, то x_1,
   Поєднуємо через АБО.
3. Якщо формула залишилась порожня, то формула – це константна 1 що не має ДКНФ.

Example 2.57.

$$maj(x,x_2,x_3) = (x_1 \vee x_2 \vee x_3)(x_1 \vee x_2 \vee \overline{x}_3)(x_1 \vee \overline{x}_2 \vee x_3)(\overline{x}_1 \vee x_2 \vee x_3)$$

x_1	x_2	x_3	maj
0	*0*	*0*	*0*
0	*0*	*1*	*0*
0	*1*	*0*	*0*
0	*1*	*1*	*1*
1	*0*	*0*	*0*
1	*0*	*1*	*1*
1	*1*	*0*	*1*
1	*1*	*1*	*1*

Example 2.58.

$$F(x_1, x_2) = x_1 \to x_2.$$

x_1	x_2	$x_1 \to x_2$
0	*0*	*1*
0	*1*	*1*
1	*0*	*0*
1	*1*	*1*

1. *ДДНФ* – $\overline{x}_1\overline{x}_2 \vee \overline{x}_1 x_2 \vee x_1 x_2$,
2. *ДКНФ* – $\overline{x}_1 \vee x_2$.

Definition 2.6.8 (Елементарна диз'юнкція)**.** *Елементарна диз'юнкція – формула, що містить лише змінні, заперечення та* $\vee$.

Definition 2.6.9 (Кон'юнктивна нормальна форма)**.** *Кон'юнктивна нормальна форма – формула, яка є кон'юнкцією елементарних диз'юнкцій.*

Definition 2.6.10 (КНФ досконала)**.** *КНФ досконала, якщо кожний множник містить змінну або її заперечення.*

2.6.7 Алгебраїчні нормальні форми

Definition 2.6.11 (Поліноміальний базис)**.** $\mathcal{F} = \{\&, \oplus, 1\}$ *– поліноміальний базис.*

Theorem 2.36. *Будь яку булеву функцію можна представити у вигляду формули над* $\mathcal{F}$.

Доведення.

$$xy \to xy$$
$$\overline{x} \to x \oplus 1$$
$$x \vee y \to x \oplus y \oplus xy$$

$\forall f \in BF_n$ – зображено формулою над $\mathcal{F}_K$ $\Rightarrow$ існує формула над $\mathcal{F}_K$ □

2.6.8 Поліном Жегалкіна

$$\begin{aligned} F(x_1, x_2, ..., x_n) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus ... \oplus a_n x_n \\ \oplus a_{1,2} x_1 x_2 \oplus a_{1,3} x_1 x_3 \oplus ... \oplus a_{n-1,n} x_{n-1} x_n \oplus \\ \oplus a_{1,2,3} x_1 x_2 x_3 \oplus ... \end{aligned}$$

де $a_n \in \{0, 1\}$.

Lemma 2.8. *існує 2^{2^n} різних поліномів Жегалкіна від n змінних.*

Доведення.
1. 2^n – доданків $\leqslant 2^{2^n}$ поліномів.
2. Два різних поліноми задають дві різні булеві функції
   (a) $\exists a \neq - \Rightarrow n \neq 0$.
   Беремо найкоротший доданок і ставимо його 1, інші 0 $\Rightarrow$ цей доданок 1, інші 0 $\Rightarrow$ поліном Жегалкіна = 1.
   Якщо два різні поліноми Жегалкіна ркалізують одну булеву функцію, то їх $\oplus = 0$, але сума різних поліномів Жегалкіна є поліномом жегалкіна із не нульовими коефіцієнтами $\Rightarrow$ сума $\neq 0$.

□

Theorem 2.37 (Жегалкіна)**.** *Кожна булева функція має представлення у виді полінома Жигалкіна.*

Це представлення – це алгебраїчна нормальна форма булевих функцій.

Кожний полінома Жигалкіна – булева функція

Кількість поліномів Жигалкіна = кількості булевих функцій

$\Rightarrow$ кожна булева функція має власний поліном Жигалкіна

2.6.9 Побудова АНФ за ДНФ

1. Будуємо ДНФ
2. Всі $\vee$ замінюємо на $\oplus$.
3. Всі $\overline{x}$ замінюємо на $(1 \oplus x)$.
4. Розкриваємо дужки

Lemma 2.9. $x, u, v \in V_n, \quad u \neq v$

$$x^u \& x^v = 0$$
$$x^u \vee x^v = x^u \oplus x^v$$

Доведення. 1. $u \neq v \Rightarrow x^u \neq x^v \Rightarrow x^u \& x^v = 0$
2. $u \neq v \Rightarrow x^u \neq x^v \Rightarrow x^u \vee x^v = 1,$
$u \neq v \Rightarrow x^u \neq x^v \Rightarrow x^u \oplus x^v = 1,$
$\Rightarrow x^u \vee xv = x^u \oplus x^v.$

□

Example 2.59.

$$\begin{aligned} maj(x_2, x_2, x_3) &= \overline{x}_1 x_2 x_3 \vee x_1 \overline{x}_2 x_3 \vee x_1 x_2 \overline{x}_3 \vee x_1 x_2 x_3 \\ &= (1 \oplus x_1) x_2 x_3 \oplus x_1 (1 \oplus x_2) x_3 \oplus x_1 x_2 (1 \oplus x_3) \oplus x_1 x_2 x_3 \\ &= x_2 x_3 \oplus x_1 x_2 x_3 \oplus x_1 x_3 \oplus x_1 x_2 x_3 \oplus x_1 x_2 \oplus x_1 x_2 x_3 \oplus x_1 x_2 x_3 \\ &= x_2 x_3 \oplus x_1 x_3 \oplus x_1 x_2 \end{aligned}$$

$$a, b \in \{0, 1\} \quad a^b = \begin{cases} a & b = 1 \\ \overline{a} & b = 0 \end{cases}$$

$$x, u \in V_n \quad x^u = x_1^{u_1} x_2^{u_2} ... x_n^{u_n}$$

$$a^{(b)} = \begin{cases} a & b = 1 \\ 1 & b = 0 \end{cases}$$

$$x, u \in V_n \quad x^{(u)} = x_1^{(u_1)} x_2^{(u_2)} ... x_n^{(u_n)}$$

Example 2.60. *1.* $x^{101} = x_1 \overline{x}_2 x_3.$
2. $x^{1000} = \overline{x}_1 \overline{x}_2 \overline{x}_3.$
3. $x^{(101)} = x_1 x_3.$
4. $x^{1000()} = 1.$

$$\Rightarrow f(x) = \bigoplus_{u \in V_n} a_u x^{(u)} \tag{2.4}$$

Claim 2.21 (Твердження Шенона для поліноміального базису)**.**

$$f(x_1, x_2, ..., x_n) = x_1 (f_1(x_2, ..., x_n) \oplus f_0(x_2, ..., x_n)) \oplus f_0(x_2, ..., x_n) \tag{2.5}$$

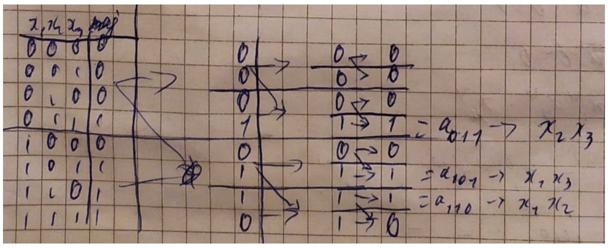

Рис. 2.1: Перетворення в АНФ

Доведення.

$$
\begin{aligned}
f &= x_1 f_1 \vee \overline{x}_1 f_0 \\
&= x_1 f_1 \oplus \overline{x}_1 f_0 \oplus x_1 \overline{x}_1 f_1 f_0 \\
&= x_1 f_1 \oplus \overline{x}_1 f_0 \\
&= x_1 f_1 \oplus (1 \oplus x_1) f_0 \\
&= x_1 (f_1 \oplus f_0) \oplus f_0
\end{aligned}
$$

□

Theorem 2.38 (Теорема Мебіуса)**.**

$$a_u = \bigoplus_{x \leq u} f(x), \qquad f(x) = \bigoplus_{u \leq x} a_u. \tag{2.6}$$

2.6.10 Побудова АНФ за таблицею істиності

1. Ділимо стовпчик значень навпіл,
2. Додаємо верхню частину до нижньої,
3. Повторюємо рекурсивно для верхньої і нижньої частин.

На виході: отримаємо вектор коефіцієнтів впорядкованих лексикографічно 2.1.

$$maj(x_1, x_2, x_3) = x_2 x_3 \oplus x_1 x_3 \oplus x_1 x_2.$$

Example 2.61. a_{101} - *? Вектор* 101 *домінує над* 000, 100, 001 *та* 101.

$\Rightarrow a_{101} = f(000) \oplus f(001) \oplus f(100) \oplus f(101) = 0 \oplus 0 \oplus 0 \oplus 1 = 1$

2.6.11 Замкнені класи булевих функцій

Замикання класу $\mathcal{F}$ – множина всіх булевих функцій які реалізуються формулами над $\mathfrak{F}$, $[\mathcal{F}]$

Замкнений клас: $[\mathfrak{F}] = \mathcal{F}$

Повний клас: $\mathcal{F} = BF_n$

Базис – повний клас і $\forall \mathcal{F}' \subset \mathcal{F}$, $([\mathcal{F}'] \neq [\mathcal{F}])$

BF_n – замкнений клас

$\mathcal{F}_A = \{\&, \oplus, 1\}$ – базис

$\mathcal{F}_K = \{\&, \vee, \neg\}$ – певний клас $x \vee y = \neg(x\&\overline{y})$.

$\{\&, \neg\}$ і $\{\vee, \neg\}$ – базиси.

2.6.12 Класи функцій

Клас функцій що зберігають нуль

$$T_0 = \{f | f(0, 0, ..., 0) = 0\}.$$

Клас функцій які збурігають одиницю

$$T_1 = \{f | f(1, 1, ..., 1) = 1\}.$$

Клас самодвоїстих функцій

$$S = \{f | f = f^*\}.$$

Клас афінних (лінійних) функцій

$$A = \{f | f(x_1, x_2, ..., x_n) = a_0 \oplus a_1 x_1 \oplus ... \oplus a_n x_n\}, a \in \{0.1\}.$$

Клас монотонних функцій

$$M = \{f | \forall x, y \in V_n x \prec y \Rightarrow f(x) \leq f(y)\}.$$

Lemma 2.10. *Класи T_0, T_1, S, A, M не вкладаються один у інший*

Example 2.62.

	T_0	T_1	S	A	M
0	+	-	-	+	+
1	-	+	-	+	+
$\overline{x}$	-	-	+	+	-
maj	+	+	+	-	+

2.6.13 Критерій повноти системи булевих функцій

Claim 2.22. *Класи T_0, T_1, S, A, M є замкнені.*

Доведення. page 72 ——————— □

– замкнений

– замкнений

– замкнений

– замкнений

– замкнений

– замкнений

Необхідна і достатня умова того, що система булевих функцій є повною

Якщо то з підстановкою або можна одержати константу

Приклад

Лемма 2 Якщо то підстановкою можна одержати

Монотонність Якщо та відрізняються лише у бітах, то можна побудувати послідовність

та , відрізняються в одному біті

Приклад

лемма3 Якщо тоді підстановкою або інвертуваннями її значення, можна отримати афінна АНФ містить доданок із не менше ніж з двома змінними.

Нехай це змінна та

Нехай так, щоб

Якщо то Якщо то

Приклади

Теорема Пост

– повна

Необхідність

Якщо Якщо – замкнений, то

Достатність Побудуємо константи 0 та 1

Якщо , то То

Якщо За леммою1 змінимо на заперечення отриману константу

За лемою 2 з констант ми можемо одержати заперечення

За лемою 3 з констант, заперечення та отримуємо

Наслідок1 Класи – передповні класи (що не є повні, але будуть кощдобавити одну функцію)

За теоремою Поста не вистачає для повноти

Наслідок 2 Всі замкнені класи ж підмножинами хоча б одног з класів

Наслідок 3 З повного класу можна обрати повний підклас у якому буде не тільки ніж у функції

Приклади

– базис

– базис

– базиси

Теорма Пост Існує 40 типів замкнених класів булевих функцій

Загальна кількість класів замкнених булевих функцій – зліченна

Лемма

Теорема Уорд Ланель

Клейтман та Марковських

2.7 Вступ до теорії графів

2.8 Абстрактні автомати

2.9 Формальні граматики

Бібліоґрафія

[BS15] Dan Boneh and Victor Shoup. A graduate course in applied cryptography, 2015.