НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

Домашня робота №1

Роботу виконав:
Юрчук Олексій, ФІ-52мн

27 лютого 2026 р.
м. Київ

ЗМІСТ

Завдання № 1

1.1 Умова

Побудувати граф скінченного автомата та визначити, чи є цей автомат оборотним за Гаффманом, якщо

1. $X = S = Y = \{0, 1\}$, $h(s, x) = s \cdot x \oplus s \oplus 1$, $f(s, x) = s \cdot x$;
2. $X = Y = \{0, 1\}, S = \{0, 1, 2, 3\}$, $f(s, x) = 0 \, \forall s \in S$, $x \in X$, окрім $f(3, 1) = 1$, $h(0, 0) = h(2, 0) = 0$, $h(0, 1) = h(2, 1) = 1$, $h(1, 0) = h(3, 0) = 2$, $h(1, 1) = h(3, 1) = 3$.

1.2 Розв'язання

Простими словами (з лекції) оборотність автомата за Гаффманом визначалася так: коли за будь-якою вихідною послідовністю та парою станів (початковим і фінальним) можна однозначно відновити відповідну їм вхідну послідовність.

Або іншими словами: автомат називатиметься **оборотним за Гаффманом**, якщо для кожного стану $s \in S$ функція виходу $f(s, \cdot) : X \to Y$ є ін'єктивною, тобто:

$$\forall s \in S, \, \forall x_1, x_2 \in X : \quad f(s, x_1) = f(s, x_2) \Rightarrow x_1 = x_2$$

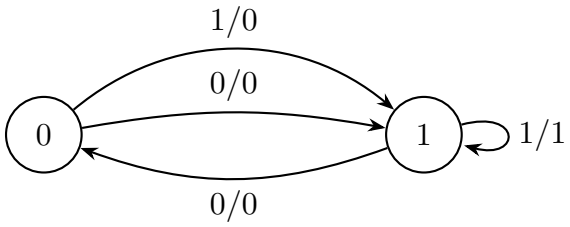
Пункт 1

У нас задано вхідний алфавіт, множину станів, множина виходів (вихідний алфавіт), функцію переходів та функцію оновлення стану
$X = S = Y = \{0, 1\}, \quad h(s, x) = s \cdot x \oplus s \oplus 1, \quad f(s, x) = s \cdot x.$

Таблиця переходів *h* та виходів *f*

s	x	$h(s, x)$	$f(s, x)$
0	0	$0 \cdot 0 \oplus 0 \oplus 1 = 1$	$0 \cdot 0 = 0$
0	1	$0 \cdot 1 \oplus 0 \oplus 1 = 1$	$0 \cdot 1 = 0$
1	0	$1 \cdot 0 \oplus 1 \oplus 1 = 0$	$1 \cdot 0 = 0$
1	1	$1 \cdot 1 \oplus 1 \oplus 1 = 1$	$1 \cdot 1 = 1$

Можна зобразити автомат графічно:



Перевіримо оборотність за Гаффманом

Маємо перевірити ін'єктивність $f(s,\cdot)$ для кожного стану:

- **Стан** $s=0$**:** $f(0,0)=0$ і $f(0,1)=0$. Різні входи ($x=0$ і $x=1$) дають однаковий вихід — не ін'єктивно.
- **Стан** $s=1$**:** $f(1,0)=0$ і $f(1,1)=1$. Різні входи x дають різні виходи — ін'єктивно.

Отже, автомат **не є оборотним за Гаффманом**, оскільки для стану $s=0$ функція виходу не є ін'єктивною.

Пункт 2

Задано $X=Y=\{0,1\}$, $S=\{0,1,2,3\}$.

Функція переходів (всі можливі випадки перебрані):

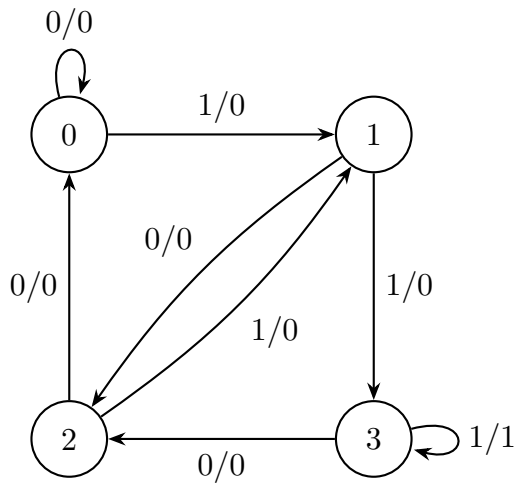
$$\begin{aligned} h(0,0)&=0, \quad h(0,1)=1,\\ h(1,0)&=2, \quad h(1,1)=3,\\ h(2,0)&=0, \quad h(2,1)=1,\\ h(3,0)&=2, \quad h(3,1)=3. \end{aligned}$$

Функція виходу: $f(s,x)=0$ для всіх (s,x), окрім $f(3,1)=1$.

Згрупуємо все в таблицю:

s	x	$h(s,x)$	$f(s,x)$
0	0	0	0
0	1	1	0
1	0	2	0
1	1	3	0
2	0	0	0
2	1	1	0
3	0	2	0
3	1	3	1

Так само зобразимо графічно:



Перевіримо оборотність за Гаффманом

Перевіряємо ін'єктивність $f(s, \cdot)$ для кожного стану:

- **Стан** $s = 0$**:** $f(0,0) = 0$ і $f(0,1) = 0$ — **не ін'єктивно**.
- **Стан** $s = 1$**:** $f(1,0) = 0$ і $f(1,1) = 0$ — **не ін'єктивно**.
- **Стан** $s = 2$**:** $f(2,0) = 0$ і $f(2,1) = 0$ — **не ін'єктивно**.
- **Стан** $s = 3$**:** $f(3,0) = 0$ і $f(3,1) = 1$ — ін'єктивно.

Отже, автомат **не є оборотним за Гаффманом**, оскільки для станів $s \in \{0,1,2\}$ функція виходу не є ін'єктивною.

Завдання № 2

2.1 Умова

Нехай Γ – генератор гами з множиною станів V_n та вихідним алфавітом V_2, який виробляє за початковим станом s_0 вихідну послідованість $\Gamma_L(s_0)$ довжини L. Покажіть, що існує статистичний критерій, який дозволяє відрізнити цю послідовність, отриману за випадковим рівноймовірним початковим станом, від суто випадкової двійкової послідовності довжини L із середньою ймовірністю помилки p_e, використовуючи T двійкових операцій, якщо $\Gamma_{2N} : s_0 \to (s_0, s_0)$, $p_e = 2^{-N-1}$, $T = N$.

2.2 Розв'язання

З умови можна зробити висновок, що послідовність $\Gamma_{2N} : s_0 \to (s_0, s_0)$ довжини $2N$ має вигляд:

$$\Gamma_{2N}(s_0) = (\gamma_1, \gamma_2, \dots, \gamma_N, \gamma_1, \gamma_2, \dots, \gamma_N)$$

Тобто **перші N біт повторюються в наступних N бітах**.

Побудова статистичного критерію

Критерій: Для послідовності $x = (x_1, x_2, \dots, x_{2N})$ перевіряємо рівність:

$$D(X) = \sum_{i=1}^{N} x_i \oplus x_{N+i} = \begin{cases} 0, \Leftrightarrow x_i = x_{N+i}, \quad \forall\, i,\, i = \overline{1, N} \quad \Rightarrow x \in \Gamma_L \\ \neq 0, -\, random\, sequence \end{cases}$$

Висунемо такі гіпотези:

- H_0: послідовність від генератора Γ
- H_1: суто випадкова, рівноймовірна послідовність

Помилка I роду (хибне відхилення H_0):

$$\alpha = P(H_1 \mid H_0) = 0$$

Нуль, бо генератор **завжди** видає $(x_1, \dots, x_N) = (x_{N+1}, \dots, x_{2N})$ за умовою.

Помилка II роду (хибне прийняття H_0):

$$\beta = P(H_0 \mid H_1) = P(x_i = x_{N+i}, \forall i \mid \text{випадкова})$$

Для випадкової послідовності біти є незалежними одне від одного, тому:

$$\beta = \prod_{i=1}^{N} P(x_i = x_{N+i}) = \prod_{i=1}^{N} \frac{1}{2} = 2^{-N}$$

Середня ймовірність помилки обчислюється за Байєсом:

$$p_e = \frac{1}{2}(\alpha + \beta) = \frac{1}{2} \cdot 0 + \frac{1}{2} \cdot 2^{-N} = 2^{-N-1}$$

Обчислювальна складність цього критерію:

N XOR-ів: $x_i \oplus x_{N+i}$ для $i = 1, \dots, N$, тобто загальна кількість двійкових операцій $T = N$

У висновку можна сказати, що критерій експлуатує детерміновану структурну слабкість генератора – періодичність з періодом N, яка неможлива для справді випадкової послідовності з ймовірністю $1 - 2^{-N}$.

Завдання № 3

3.1 Умова

3.2 Розв’язання