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:

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

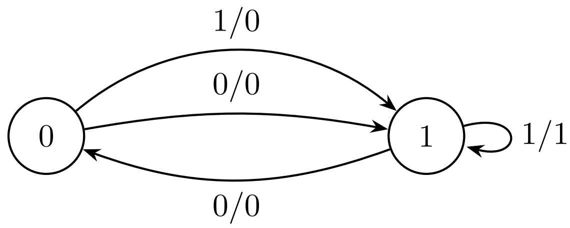
Пункт 1

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):

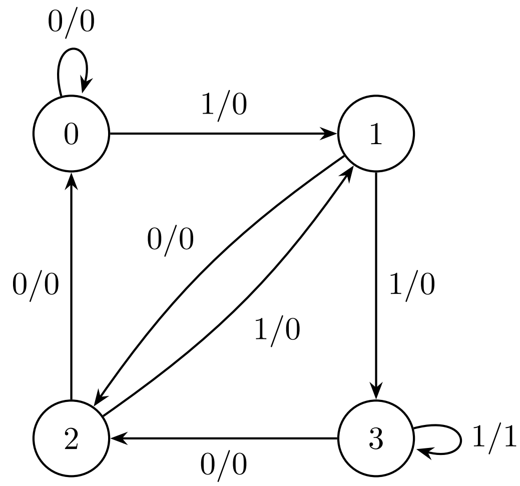
$$\begin{aligned} h(0,0) &= 0, \quad h(0,1) = 1, \\ h(1,0) &= 2, \quad h(1,1) = 3, \\ h(2,0) &= 0, \quad h(2,1) = 1, \\ h(3,0) &= 2, \quad h(3,1) = 3. \end{aligned}$$

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:

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

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

Розглянемо генератор гами Γ, який з початкового стану переходить у наступний стан, а далі звичайним чином виробляє гаму. Відновіть початковий стан генератора за відрізком гами γ, якщо Γ є комбінувальним генератором гами, що складається з двох ЛРЗ довжини 3 з поліномами зворотного зв'язку $p_1(x) = x^3 \oplus x \oplus 1$ і $p_2(x) = x^3 \oplus x^2 \oplus 1$ відповідно та комбінувальної функції $f(z_1, z_2) = z_1 z_2$, а відрізок гами γ дорівнює 1, 0, 1, 0, 0, 0.

3.2 Розв'язання

Крок 1. Рекурентні співвідношення

Виведемо для наших поліномів рекуренті співвідношення і намалюємо малюнок для зручності, виходячи з того, що для полінома $p(x) = x^3 + c_2 x^2 + c_1 x + c_0$ рекурентне йому співвідношення є наступним:

$$z_{n+3} = c_2 z_{n+2} \oplus c_1 z_{n+1} \oplus c_0 z_n$$

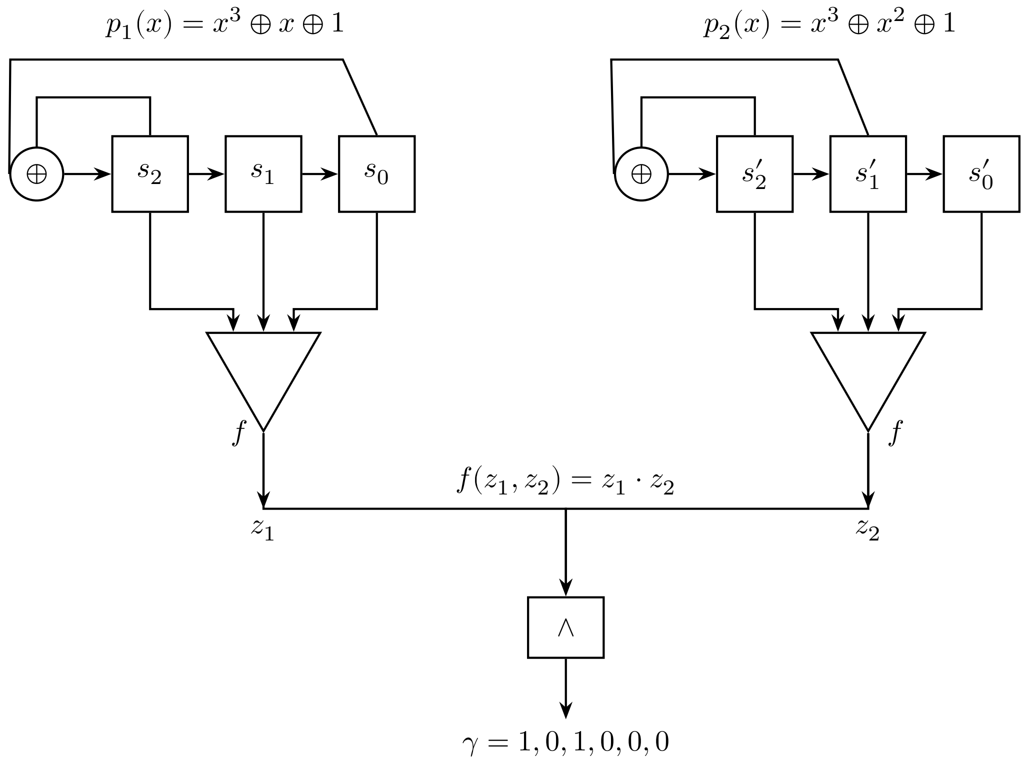
Тому для **LFSR 1:** $p_1(x) = x^3 \oplus x \oplus 1 = x^3 + 0 \cdot x^2 + 1 \cdot x + 1$ маємо:

$$\boxed{z_{n+3} = z_{n+1} \oplus z_n}$$

А для **LFSR 2:** $p_2(x) = x^3 \oplus x^2 \oplus 1 = x^3 + 1 \cdot x^2 + 0 \cdot x + 1$:

$$\boxed{z_{n+3} = z_{n+2} \oplus z_n}$$

На малюнку повна схема виглядатиме так (трохи кривенько, бо попросив ШІ по шаблону згенерувати, щоб я міг більше на розв'язку зосередитися):



Крок 2. Потактова робота LFSR

Нехай початковий стан для LFSR 1 це (a_0, a_1, a_2), а для LFSR 2: (b_0, b_1, b_2).

За умовою, генератор спочатку робить один крок переходу, тому перший біт гами відповідає z_1, а не z_0.

LFSR 1: $z_{n+3} = z_{n+1} \oplus z_n$			**LFSR 2**: $z_{n+3} = z_{n+2} \oplus z_n$		
n	z_n (вираз)	z_n	n	z_n (вираз)	z_n
0	a_0	—	0	b_0	—
1	a_1	$z_1^{(0)}$	1	b_1	$z_2^{(0)}$
2	a_2	$z_1^{(1)}$	2	b_2	$z_2^{(1)}$
3	$a_1 \oplus a_0$	$z_1^{(2)}$	3	$b_2 \oplus b_0$	$z_2^{(2)}$
4	$a_2 \oplus a_1$	$z_1^{(3)}$	4	$b_2 \oplus b_1 \oplus b_0$	$z_2^{(3)}$
5	$a_2 \oplus a_1 \oplus a_0$	$z_1^{(4)}$	5	$b_1 \oplus b_0$	$z_2^{(4)}$
6	$a_2 \oplus a_0$	$z_1^{(5)}$	6	$b_2 \oplus b_1$	$z_2^{(5)}$

Для LFSR 1:

$$
\begin{aligned}
z_3 &= z_1 \oplus z_0 = a_1 \oplus a_0 \\
z_4 &= z_2 \oplus z_1 = a_2 \oplus a_1 \\
z_5 &= z_3 \oplus z_2 = (a_1 \oplus a_0) \oplus a_2 = a_2 \oplus a_1 \oplus a_0 \\
z_6 &= z_4 \oplus z_3 = (a_2 \oplus a_1) \oplus (a_1 \oplus a_0) = a_2 \oplus a_0
\end{aligned}
$$

Для *LFSR 2:*

$$
\begin{aligned}
z_3 &= z_2 \oplus z_0 = b_2 \oplus b_0 \\
z_4 &= z_3 \oplus z_1 = (b_2 \oplus b_0) \oplus b_1 = b_2 \oplus b_1 \oplus b_0 \\
z_5 &= z_4 \oplus z_2 = (b_2 \oplus b_1 \oplus b_0) \oplus b_2 = b_1 \oplus b_0 \\
z_6 &= z_5 \oplus z_3 = (b_1 \oplus b_0) \oplus (b_2 \oplus b_0) = b_2 \oplus b_1
\end{aligned}
$$

Крок 3. Вихід (рівняння для гами)

Гама: $\gamma_i = z_1^{(i)} \cdot z_2^{(i)}$ (операція AND).

i	γ_i	$z_1^{(i)}$	$z_2^{(i)}$	Рівняння
0	1	a_1	b_1	$a_1 \cdot b_1 = 1$
1	0	a_2	b_2	$a_2 \cdot b_2 = 0$
2	1	$a_1 \oplus a_0$	$b_2 \oplus b_0$	$(a_1 \oplus a_0) \cdot (b_2 \oplus b_0) = 1$
3	0	$a_2 \oplus a_1$	$b_2 \oplus b_1 \oplus b_0$	$(a_2 \oplus a_1) \cdot (b_2 \oplus b_1 \oplus b_0) = 0$
4	0	$a_2 \oplus a_1 \oplus a_0$	$b_1 \oplus b_0$	$(a_2 \oplus a_1 \oplus a_0) \cdot (b_1 \oplus b_0) = 0$
5	0	$a_2 \oplus a_0$	$b_2 \oplus b_1$	$(a_2 \oplus a_0) \cdot (b_2 \oplus b_1) = 0$

Крок 4. Розв'язання системи

Якщо $\gamma_i = 1$, то **обов'язково** обидва множники дорівнюють 1.

З $\gamma_0 = 1$:

$$a_1 = 1, \quad b_1 = 1$$

З $\gamma_2 = 1$:

$$a_1 \oplus a_0 = 1, \quad b_2 \oplus b_0 = 1$$

Підставляємо $a_1 = 1$:

$$1 \oplus a_0 = 1 \quad \Rightarrow \quad a_0 = 0$$

Маємо:

$$\boxed{a_0 = 0, \quad a_1 = 1, \quad b_1 = 1, \quad b_2 \oplus b_0 = 1}$$

Якщо $\gamma_i = 0$, то **хоча б один** множник (під множенням насправді приховується $\wedge$) дорівнює 0. Підставляємо відомі значення:

При $\gamma_1 = 0$: $a_2 \cdot b_2 = 0$

$$a_2 = 0 \quad \text{або} \quad b_2 = 0$$

При $\gamma_3 = 0$: $(a_2 \oplus a_1) \cdot (b_2 \oplus b_1 \oplus b_0) = 0$

$$
\begin{aligned}
&(a_2 \oplus 1) \cdot (b_2 \oplus 1 \oplus b_0) = 0 \\
&a_2 = 1 \quad \text{або} \quad b_2 \oplus b_0 = 1 \text{ – це вже отримували вище}
\end{aligned}
$$

При $\gamma_4 = 0$: $(a_2 \oplus a_1 \oplus a_0) \cdot (b_1 \oplus b_0) = 0$

$$
\begin{aligned}
&(a_2 \oplus 1 \oplus 0) \cdot (1 \oplus b_0) = 0 \\
&(a_2 \oplus 1) \cdot (1 \oplus b_0) = 0 \\
&a_2 = 1 \quad \text{або} \quad b_0 = 1
\end{aligned}
$$

При $\gamma_5 = 0$: $(a_2 \oplus a_0) \cdot (b_2 \oplus b_1) = 0$

$$
\begin{aligned}
&(a_2 \oplus 0) \cdot (b_2 \oplus 1) = 0 \\
&a_2 = 0 \quad \text{або} \quad b_2 = 1
\end{aligned}
$$

При цьому всьому бачимо, що виникає три обмеження на наші диз'юнкти:

1. $a_2 = 0$ або $b_2 = 0$ (з γ_1)
2. $a_2 = 1$ або $b_0 = 1$ (з γ_4)
3. $a_2 = 0$ або $b_2 = 1$ (з γ_5)

Тобто треба розглянути два наступні випадки:
Випадок 1: $a_2 = 0$
З обмеження (2): $a_2 = 1$ або $b_0 = 1$. Оскільки $a_2 = 0 \neq 1$, маємо $b_0 = 1$.
З $b_2 \oplus b_0 = 1$: $b_2 \oplus 1 = 1$, тому $b_2 = 0$.
Тоді з обмеження (1): $a_2 = 0$ — виконано
А з обмеження (3): $a_2 = 0$ — виконано

$$\text{Розв'язком є: } (a_0, a_1, a_2) = (0, 1, 0), \quad (b_0, b_1, b_2) = (1, 1, 0)$$

Випадок 2: $a_2 = 1$
З обмеження (1): $a_2 = 0$ або $b_2 = 0$. Оскільки $a_2 = 1$, то $b_2 = 0$.
З $b_2 \oplus b_0 = 1$: $0 \oplus b_0 = 1$, тому $b_0 = 1$.
Перевіряємо обмеження (3): $a_2 = 0$ або $b_2 = 1$.
Маємо $a_2 = 1 \neq 0$ і $b_2 = 0 \neq 1$ – обмеження не виконується! Караул!
Тобто випадок 2 не можливий.

Крок 5. Це кінець (відповідь)

Отримали єдиний (на диво) початковий стан генератора:

$$\boxed{\begin{array}{ll} \text{LFSR 1:} & (s_0, s_1, s_2) = (0, 1, 0) \\ \text{LFSR 2:} & (s'_0, s'_1, s'_2) = (1, 1, 0) \end{array}}$$

P.S. Але після такої задачі хочеться вмерти

Крок 6. Ah shit, here we go again! (Перевірка)

В опів на дванадцяту ночі, то перевірку я лишив на ШІ, сподіваюся він правильно її зробив (ну, принаймні результат збігся). Все що тут необхідно було, це підставити $(a_0, a_1, a_2) = (0, 1, 0)$ і $(b_0, b_1, b_2) = (1, 1, 0)$ та отримати ланцюжок $\gamma = 1, 0, 1, 0, 0, 0$ з умови.
Виходи LFSR 1:

$$\begin{aligned} z_1^{(0)} &= a_1 = 1 \\ z_1^{(1)} &= a_2 = 0 \\ z_1^{(2)} &= a_1 \oplus a_0 = 1 \oplus 0 = 1 \\ z_1^{(3)} &= a_2 \oplus a_1 = 0 \oplus 1 = 1 \\ z_1^{(4)} &= a_2 \oplus a_1 \oplus a_0 = 0 \oplus 1 \oplus 0 = 1 \\ z_1^{(5)} &= a_2 \oplus a_0 = 0 \oplus 0 = 0 \end{aligned}$$

Виходи LFSR 2:

$$\begin{aligned}
z_2^{(0)} &= b_1 = 1 \\
z_2^{(1)} &= b_2 = 0 \\
z_2^{(2)} &= b_2 \oplus b_0 = 0 \oplus 1 = 1 \\
z_2^{(3)} &= b_2 \oplus b_1 \oplus b_0 = 0 \oplus 1 \oplus 1 = 0 \\
z_2^{(4)} &= b_1 \oplus b_0 = 1 \oplus 1 = 0 \\
z_2^{(5)} &= b_2 \oplus b_1 = 0 \oplus 1 = 1
\end{aligned}$$

Обчислення гами:

i	$z_1^{(i)}$	$z_2^{(i)}$	$\gamma_i = z_1^{(i)} \cdot z_2^{(i)}$	Очікуване
0	1	1	$1 \cdot 1 = 1$	1
1	0	0	$0 \cdot 0 = 0$	0
2	1	1	$1 \cdot 1 = 1$	1
3	1	0	$1 \cdot 0 = 0$	0
4	1	0	$1 \cdot 0 = 0$	0
5	0	1	$0 \cdot 1 = 0$	0

Результат: $\gamma = 1, 0, 1, 0, 0, 0$, такий як і мав бути!