

**Циклдік кодтар. Циклдік
кодтарды декодтау.**

Циклдік кодтар - хабарламадағы (сөздегі) циклдік жылжыту код шекарасынан шығып кетпейтін кодтар. Циклдық кодтар бөгеуілге орнықты кодтардың ішінен қатені табу жағынан ең тиімді код болып саналады

L O O O O O O O O O	↔ 9
O L O O O O O O O O	↔ 8
O O L O O O O O O O	↔ 7
O O O L O O O O O O	↔ 6
O O O O L O O O O O	↔ 5
O O O O O L O O O O	↔ 4
O O O O O O L O O O	↔ 3
O O O O O O O L O O	↔ 2
O O O O O O O O L O	↔ 1
O O O O O O O O O L	↔ 0

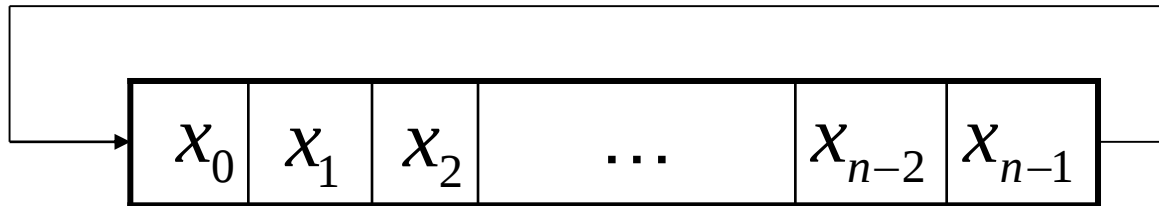
Сызықты циклдік кодтар

(n,k) -коды сызықты циклдік деп аталады, егер циклдік жылжыту осы топқа жатса:

$$\chi = \begin{bmatrix} x_0 \\ x_1 \\ \dots \\ x_{n-2} \\ x_{n-1} \end{bmatrix} \Rightarrow \chi^{(1)} = \begin{bmatrix} x_{n-1} \\ x_0 \\ \dots \\ x_{n-3} \\ x_{n-2} \end{bmatrix}$$

Циклдік жылжыту

Циклдік жылжыту ұзындығы n жылжыту регистрінің көмегімен жүзеге асады (кері байланыс).

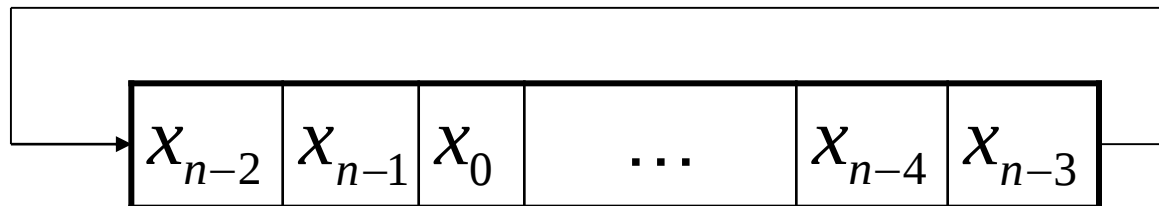


Циклдік жылжытуды жүзеге асыру

1 тактідегі жылжыту регистрі



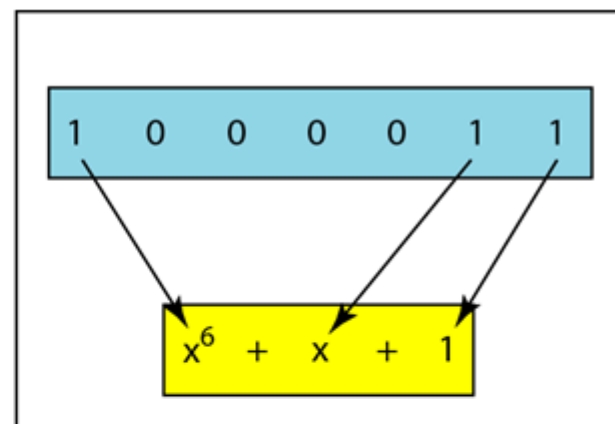
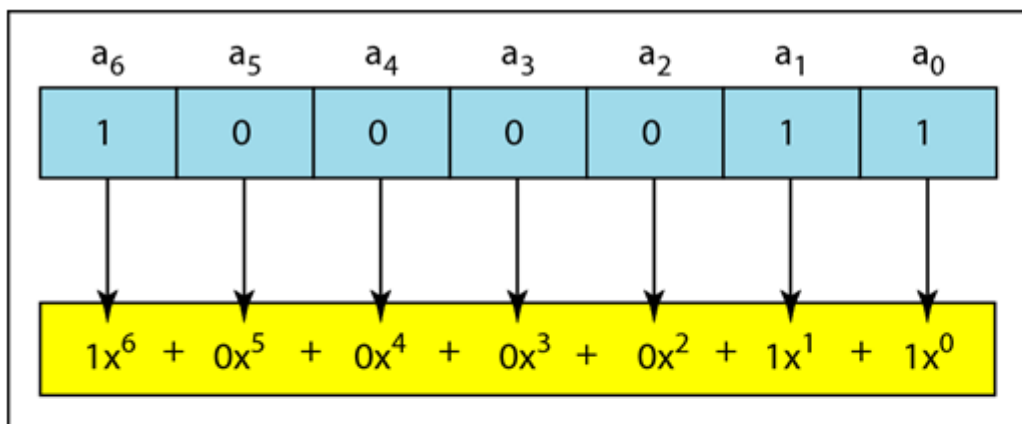
2 тактідегі жылжыту регистрі



Кодтық сөздерді кодтық көпмүшелік арқылы беру

$$\alpha = \begin{bmatrix} a_0 \\ a_1 \\ \dots \\ a_{n-2} \\ a_{n-1} \end{bmatrix} \Rightarrow a(x) = a_0 \oplus a_1 x \oplus \dots \oplus a_{n-1} x^{n-1}$$

Кодтық сөздерді көпмүшелік түрінде беру



Көпмүшелікті циклдік жылжыту

$$a(x) = a_0 \oplus a_1 x \oplus \dots \oplus a_{n-1} x^{n-1}$$

$$a^{(1)}(x) = a_{n-1} \oplus a_0 x \oplus \dots \oplus a_{n-3} x^{n-2} \oplus a_{n-2} x^{n-1} =$$

$$= a_0 x \oplus \dots \oplus a_{n-3} x^{n-2} \oplus a_{n-2} x^{n-1} \oplus a_{n-1} x^n \pmod{x^n \oplus 1} =$$

$$= x \cdot a(x) \pmod{x^n \oplus 1}$$

Көпмүшеліктің циклдік жылжытуы

$$\alpha^{(i)} = \begin{bmatrix} a_{n-i} \\ a_{n-i+1} \\ \dots \\ a_{n-i-2} \\ a_{n-i-1} \end{bmatrix} \Rightarrow x^i \cdot a(x) \pmod{x^n \oplus 1}$$

Кодтау

- Циклдік кодты кодтау – ақпараттық көпмүшелікті туынды көпмүшелікке көбейту.

(7,4)-циклдік код

- *мысалы.* $g(x) = 1 \oplus x \oplus x^3$
- *жіктеу* $x^7 \oplus 1 = (x \oplus 1)(1 \oplus x \oplus x^3)(1 \oplus x^2 \oplus x^3)$

ақпарат	Кодтық сөз	Көпмүшелік
0000	0000000	$0 \cdot g(x)$
1000	1101000	$1 \cdot g(x)$
0100	0110100	$x \cdot g(x)$
1100	1011100	$(1 \oplus x) \cdot g(x)$
0010	0011010	$x^2 \cdot g(x)$
1010	1110010	$(1 \oplus x^2) \cdot g(x)$
0110	0101110	$(x \oplus x^2) \cdot g(x)$
1110	1000110	$(1 \oplus x \oplus x^2) \cdot g(x)$
0001	0001101	$x^3 \cdot g(x)$
1001		
0101		
1101		Өздеріңіз толтырыңыздар
0011		
1011		
0111		
1111		

Циклдік кодтың туынды матрицасы

$$G_{k \times n}^T = \begin{pmatrix} 1 & g_1 & g_2 & \dots & g_{n-k-1} & 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & g_1 & \dots & g_{n-k-2} & g_{n-k-1} & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & \dots & \dots & g_{n-k-1} & 1 & \dots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & 1 & g_1 & g_2 & \dots & g_{n-k-1} & 1 \end{pmatrix}$$

Циклдік кодтың тексеру көпмүшелігі

- Циклдік кодтың туынды көпмүшелігі

$$x^n \oplus 1 = h(x) \cdot g(x)$$

- $h(x)$ – тексеру көпмүшелігі

Циклдік кодтың тексеру матрицасы

- Барлық кодтық сөзді мына түрде жазуға болады:

$$c(x) = a(x) \cdot g(x), \quad \deg a(x) \leq k - 1$$

- Онда
$$\begin{aligned} c(x) \cdot h(x) &= a(x) \cdot g(x) \cdot h(x) = \\ &= a(x) \cdot (1 \oplus x^n) = \\ &= a(x) \oplus a(x) \cdot x^n \end{aligned}$$

- Сондықтан

$$\deg c(x) \cdot h(x) \leq k - 1$$

Циклдік кодтың тексеру матрицасы

- Сонда

$$c_0 \cdot h_k \oplus c_1 \cdot h_{k-1} \oplus \dots \oplus c_k \cdot h_0 = 0$$

$$c_1 \cdot h_k \oplus c_2 \cdot h_{k-1} \oplus \dots \oplus c_{k+1} \cdot h_0 = 0$$

$$c_2 \cdot h_k \oplus c_3 \cdot h_{k-1} \oplus \dots \oplus c_{k+2} \cdot h_0 = 0$$

...

$$c_{n-k-1} \cdot h_k \oplus c_{n-k} \cdot h_{k-1} \oplus \dots \oplus c_{n-1} \cdot h_0 = 0$$

Циклдік кодтың тексеру матрицасы

$$H_{(n-k) \times n} = \begin{pmatrix} h_k & h_{k-1} & h_{k-2} & \dots & h_1 & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & \dots & h_2 & h_1 & h_0 & 0 & \dots & 0 \\ 0 & 0 & h_k & \dots & \dots & \dots & h_1 & h_0 & \dots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & h_k & h_{k-1} & h_{k-2} & \dots & h_1 & h_0 \end{pmatrix}$$

Есеп. Циклдік кодтың кодтық комбинациясын жазу керек, егер туынды полином $P(x) = x^3 + x^2 + 1$

Ақпарат көзінен түскен кодтық комбинация – парольдің соңғы екі цифры.

шешімі:

$N = 23;$

$$23_{10} = 10111_2$$

Бұл санды полином ретінде жазсақ:

$$A(x) = 1 * x^4 + 0 * x^3 + 1 * x^2 + 1 * x^1 + 1 * x^0 = x^4 + x^2 + x + 1$$

1) $r=3$ болсын, онда:

- Екілік кодта:

$$A(x) * x^3 = (x^4 + x^2 + x + 1) * x^3 = x^7 + x^5 + x^4 + x^3 = x^7 + x^5 + x^4 + x^3$$

$$A(x) = 10111000$$

2) Бөлу операциясы:

$$\begin{array}{r}
 x^7 + x^5 + x^4 + x^3 \mid x^3 + x^2 + 1 \\
 \underline{x^6 + x^5 + x^3} \\
 x^7 + x^6 + x^4 \\
 \underline{x^5 + x^4 + x^2} \\
 x^7 + x^6 + x^5 + x^2 \\
 \underline{x^3 + x^2 + 1} \\
 x^3 + x^2 + 1 \Rightarrow R(x) = x^7 + x^6 + x^5 + x^3 + 1 \\
 R(x) = 11101001
 \end{array}$$

3) Кодерден өткеннен кейін сигнал мынаған тең:

$$A(x) * x^r + R(x) = 1011111101001$$