Kody Liniowe.

- Niech K - skończone ciało. Kod liniowy C to podprzestrzeń liniowe K^n.

$$C \leq K^n$$

- $\Delta(C) = \min\{d_H(s,t) \; s,t \in C \wedge s \neq t\} =$

$$[\text{kody } C \text{ liniowy}] = \min\{d_H(s,0) : s \in C \wedge s \neq 0\}$$

- Waga Hamminga słowa $s \in K^n$ nazywamy liczbę

$$w_H(s) = d_H(s,0) = |\{i : s_i \neq 0\}|$$

Np: $w_H(\underline{1}0\underline{1}0) = 2$

PARAMETRY KODU

Def • Kod liniowy C nazywamy $[n,k,d]_q$ kodem, gdy:

$$C \leq F_q^n, \; \dim(C) = k, \; \Delta(C) = d,$$

gdzie F_q ciało q-elementowe

- Kod liniowy C jest $[n,k]_q$ kodem gdy

$$C \leq F_q^n, \; d_-(C) = k$$

ozn $[n,k] = [n,k]_2$

$(n, M, d)_q$ — n: dł., M: moc C, d: Δ, q: |A|

Macierz kodu liniowego

UWAGA Kod liniowy jest podprzestrzenią, więc ma bazę: $b_1, b_2, \dots, b_n \in F_q^n$.

Def Niech $C \leq F_q^n$ kod liniowy. Macierzą kodu C nazywamy macierz: $M_C = \begin{bmatrix} -b_1- \\ -b_2- \\ \vdots \\ -b_k- \end{bmatrix} \in F_q^{k \times n}$

gdzie, $b_1, b_2, \dots b_k$ - baza C, $(\dim(C) = k)$

Np. $\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$ macierz kodu C

Jest to $[4, 2, 2]_2$ - kod.

- Def Niech $M \in F_q^{k \times n}$ macierz kodu C.

Kodowaniem nazywamy funkcję:

$$K_C( ) = v \cdot M : F_q^k \to F_q^n.$$

Przykład: $M = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$

$$k_C(a,b) = (a,b) \cdot \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix} = [b, a+b, 0, a]$$

UWAGA. Niech $M = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{bmatrix}$ macierz kodu C. Skoro $b_1 \dots b_k$ są liniowo niezależne, to za pomocą operacji elementarnych M możemy przekształcić do postaci:

$M \to \cdots M' = [I|A] \leftarrow$ Macierz standardowa kodu C.

Przykład. Ciało $F_2 = \{0,1\}$

$$M = \left[\begin{array}{cc|cc} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{array}\right] \xrightarrow{I \leftrightarrow II} \left[\begin{array}{cc|cc} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{array}\right] \xrightarrow{I \to I+II} \left[\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{array}\right] = [I|A]$$

(I | A)

Kodowanie

$$k_C(a,b) = (a,b) \cdot \left[\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{array}\right] = [a, b, 0, a+b]$$

Def Niech $M = [I:A]$ macierz standardowa kodu C.
Macierzą parzystości C nazywamy macierz:

$$N = \left[\begin{array}{c} -A \\ \hline I \end{array}\right]$$

(I | A)

Przykład. • Dla $M = \left[\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{array}\right]$ w $\mathbb{Z}_2$

$$N = \begin{bmatrix} -0 & -1 \\ -0 & -1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

• $M = \left[\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & 2 \end{array}\right]$, $N = \begin{bmatrix} -1 \\ -2 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix}$ w $\mathbb{Z}_3$

Tw. Niech N macierz kontroli poprzystości kodu liniow. $C \leq K^n$
Wtedy:

$$(\forall v \in K^n) \quad v \in C \iff v \cdot N = 0$$

Lemat. Jeśli A, B, C, D są macierzami (odpow. wymiarów)

to $[A|B] \cdot \begin{bmatrix} C \\ D \end{bmatrix} = A \cdot C + B \cdot D$

D-d ćw.

D-d Twierdzenia.

Niech $M = [I : A]$ - macierz standardowa kodu C,

$N = \begin{bmatrix} -A \\ I \end{bmatrix}$.

Zauważmy, że $* \; M \cdot N = [I\,A] \begin{bmatrix} -A \\ I \end{bmatrix} \overset{\text{Lem}}{=} I \cdot (-A) + A \cdot I = 0$

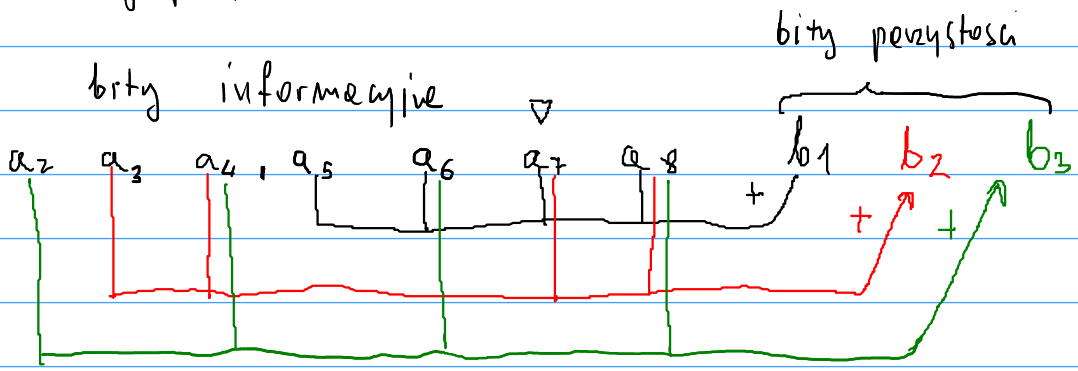
Niech $v \in C$ zatem istnieje w takie, że $v = w \cdot M$

Wtedy:

$$v \cdot N = (w \cdot M) \cdot N = w \cdot (M \cdot N) \overset{*}{=} w \cdot 0 = 0 \; \square$$

Kody Hamminga. (binarne kody liniowe).

IDEA: bity parzystości



Np.

1	0	1	1	0	0	1		b_1	b_2	b_3			
								0	0	1			

Rozważmy kod $C \leq \mathbb{Z}_2^{10}$, $v \in C$, gdy zostało utworzone wyżej opisany sposób $|C| = 2^7$.

UWAGA C koryguje jeden błąd.

KODY HAMMINGA

- $[2^m - 1, 2^m - m - 1, 3]_2$, $m > 2$.
- Kod Hamminga jest kodem doskonałym.
- Konstrukcja
  - bity parzystości są na pozycjach $1, 2, 4, 8, 16 \ldots$ (b_i)
  - bity informacyjne to pozostałe. (a_i)

Oznaczmy bity parzyst $b_1, b_2, b_4, b_8, b_{16}, \ldots$
Słowo: $b_1 b_2 a_3 b_4 a_5 a_6 a_7 b_8 a_9 a_{10} a_{11} \ldots$
gdzie:

$b_1 = a_3 + a_5 + a_7 + a_9 + a_{11} + \ldots$

$b_2 = a_3 + a_6 + a_7 + a_{10} + a_{11}$

$b_4 = a_5 + a_6 + a_7 + a_{12} + a_{13} + a_{14} + a_{15}$