Teoria Kodowania.

- Kodowanie to przypisywanie obiektom słów zbudowanych z liter ustalonego alfabetu.

Kod ASCII Litery alfabetu $\rightarrow$ ciągi 0 1

- Kodowanie $\neq$ Szyfrowanie.

- Ustalmy niepusty skończony zbiór A, nazywany alfabetem, elementy A nazyw. literami.

- słowo to skończony ciąg liter

Np $A = \{0,1\}$, $s_1 = 001$, $s_2 = 0$.

- długość słowa to liczba jego liter.

- Słowo puste to słowo długości 0, oznaczane ε.

- Konkatenacja słów s i z to $s \| z$
  Przykład $s = 00$, $z = 11$ to $s \| z = 0011$.

- Zbiór wszystkich słów nad alfabetem A ozn: A^*
- Zbiór słów długości n nad A oznaczamy A^n

- Odległość Hamminga na A^n.

Dla $s \in A^n$ niech s_i - ita litera słowa s

Np $s = 11\underline{0}$ to $s_3 = 0$.

Odległość Hamminga słów $s, z \in A^n$

$$d_H(s,z) = |\{i : s_i \neq z_i\}|$$

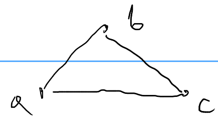
Np: $d_H(12\underline{3}, 12\underline{4}) = |\{3\}| = 1$.

<u>TW</u> (A^n, d_H) jest przestrzenią metryczną.

D-d: 1. $\forall z,s \in A^n \quad d_H(z,s) = d_H(s,z)$ ok.

2. $\forall z,s \in A^n \quad d_H(z,s) \geq 0$

$d_H(z,s) = 0 \iff z = s$ ok.



3. Nierówność trójkąta:

$\forall a,b,c \in A^n \quad d_H(a,b) + d_H(b,c) \geq d_H(a,c)$

$|A| + |B| \geq |A \cup B|$

$$d_H(a,b) + d_H(b,c) = |\{i : a_i \neq b_i\}| + |\{i : b_i \neq c_i\}| \geq$$
$$|\{i : a_i \neq b_i \lor b_i \neq c_i\}| \geq |\{i : a_i \neq c_i\}| = d_H(a,c)$$

$\square$

- Kula o środku w $s \in A^n$ i promieniu r nazywamy zbiór:

$$B(s,r) = \{w \in A^n : d_H(s,w) \leq r\}$$

Przykład: $B(00\ldots0, 1) =$ $A = \{0,1\}$
„słowa z nie więcej niż jedną literą różną od zera"

Fakt Niech $|A| = q$. Wtedy dla każdego $s \in A^n$, $r \in \mathbb{N}$

$$|B(s,r)| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i .$$

D-d ćw.

Kody.

- Kodem nad alfabetem A nazywamy skończony niepusty podzbiór A^*

- Kodem blokowym długości $n \in \mathbb{N}$ nad A nazywamy skończony niepusty podzbiór A^n.

Przykład $\{1, 01, 001\}$ – kod nad $A = \{0,1\}$
$\{111, 000, 101\}$ – kod blokowy dług. 3 nad $A = \{0,1\}$

- Rozstęp kodu blokowego $K \in A^n$ to liczba

$$\Delta(K) = \min \{ d_H(s,z) : s \neq z \wedge s,z \in K \}$$

Przykład $\Delta(\{\underset{\sim}{111}, 000, \underset{\sim}{101}\}) = d_H(111, 101) = 1$

- Parametry kodu blokowego.

$K \subseteq A^n$ jest $(n, M, d)_q$ – kodem gdy
- słowa K są długości n.
- $M = |K|$
- $d = \Delta(K)$
- $q = |A|$.

Przykład $K = \{111, 222, 333\}$

K jest $(3,3,3)_3$ - kodem.

Tw Ograniczenie Hamminga.
Jeśli istnieje $(n, M, d)_q$ kod to

$$M \cdot \sum_{i=0}^{k} \binom{n}{i} (q-1)^i \leq q^n \quad , \text{gdzie} \quad k = \left\lfloor \frac{d-1}{2} \right\rfloor$$

D-d. Kule o promieniu k o środkach w słowach $s \in K$ są rozłączne i każda z nich ma

$$\sum_{i=0}^{k} \binom{n}{i} (q-1)^i \quad \text{punktów.}$$

Takich kul jest M sztuk. Zatem wszystkich punktów leżących w sumie tych kul jest

$$M \cdot \sum_{i=0}^{k} \binom{n}{i} (q-1)^i$$

i nie może być ich więcej niż punktów całej przestrzeni

zatem $M \cdot \sum_{i=0}^{k} \binom{n}{i} (q-1)^i \leq q^n$ $\square$

Kanał Komunikacyjny.

Rozważmy sytuację gdy osoby A i B przesyłają sobie słowa kodu $K \subseteq A^n$

• Pojedynczy błąd to zamiana pojedynczej litery słowa kodowego.

• Kod K wykrywa b błędów gdy:
jeśli A przesyła słowo kodowe $w \in K$, kanał nie więcej niż b błędów to otrzymane słowo $w' \notin K$.

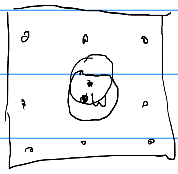
• Def Niech $K \subseteq A^n$. Powiemy, że K wykrywa $b \in \mathbb{N}^+$ błędów gdy

$$\forall w \in K \quad B(w, b) \cap K = \{w\}$$

• Def Niech $K \subseteq A^n$. Powiemy, że K koryguje $b \in \mathbb{N}^+$ błędów gdy

$$\forall w \in K \quad \forall v \in A^n \quad d_H(w, v) \leq b \rightarrow B(v, b) \cap K = \{w\}$$

Rys A^n:



Fakt. Niech $K \subseteq A^n$ kod blokowy. Wtedy

1. Kod wykrywa $\Delta(K) - 1$ błędów
2. Kod koryguje $\left\lfloor \frac{\Delta(K) - 1}{2} \right\rfloor$ błędy.

D-d. ćw. (2) Nierówność Δ.

Def. $(n, M, d)_q$ kod $K \subseteq A^n$ nazywamy kodem doskonałym, gdy zbiór A^n jest sumą rozłącznych kul

$$A^n = \dot{\bigcup_{s \in K}} B\left(s, \left\lfloor \frac{d-1}{2} \right\rfloor\right)$$

Kody Liniowe.

- Niech alfabetem będzie ciało skończone K (np $\mathbb{Z}_2 = \{0,1\}$).
Wtedy K^n jest przestrzenią liniową nad K.
$K_n = \{(k_1, k_2, \dots, k_n) : k_i \in K\}$.

- Kodem Liniowym nazywamy podprzestrzeń liniową K^n

- Parametry kodu Liniowego.
$C \leq K^n$ nazywamy $[n,k]_q$ kodem gdy $|K| = q$, $\dim C = k$

Fakt. Niech $C \leq K^n$ kod liniowy to zachodzi:

$$\Delta(C) = \min\{d_H(s, 0) : s \in C, s \neq 0\}.$$

Lemat. Odległość d_H jest niezmiennicza na przesunięcie:
$\forall s, z \in K^n, v \in K^n \quad d_H(z,s) = d_H(z+v, s+v)$.

D-d $d_H(z,s) = |\{i : z_i \neq s_i\}| = |\{i : z_i + v_i \neq s_i + v_i\}| =$
$d_H(z+v, s+v)$ $\square$

D-d. Faktu.
$\Delta(C) = \min\{d_H(z,s) : z, s \in C \wedge z \neq s\} =$

$\min\{d_H(z-s, s-s) : z, s \in C \wedge z \neq s\} =$
$\min\{d_H(z-s, 0) \quad z, s \in C \wedge z \neq s\} =$
$\min\{d_H(s, 0) : s \in C \wedge s \neq 0\}.$ $\square$