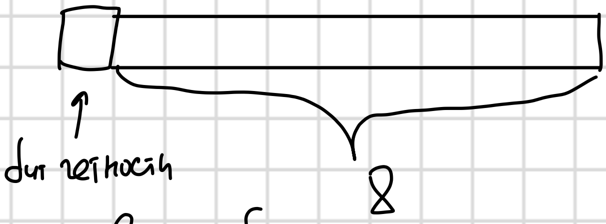
Избыточное кодирование

Бит четности



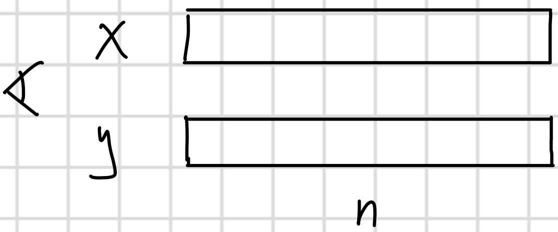
① вес байта

$c: \mathbb{B}^8 \to \mathbb{B}^9$

расстояние Хэмминга

$H(x,y)$ — кол-во позиций $i: x[i] \neq y[i]$

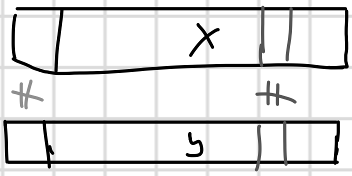
$H(001101, 101000) = 3$



расстояние:

1) $d(x,y) \geq 0$
2) $d(x,y) = 0 \Leftrightarrow x = y$
3) $d(x,y) + d(y,z) \geq d(x,z)$

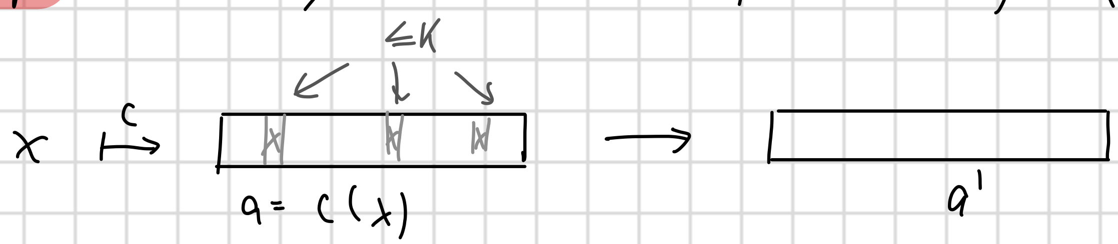
$\exists\, d(c) = 2$



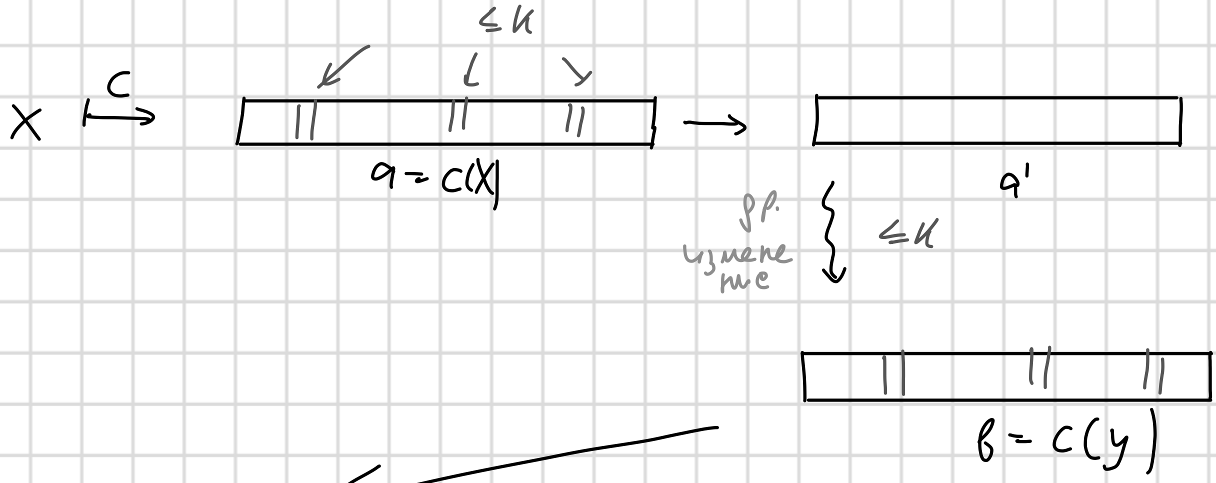
$\forall\ c: \Sigma \to \mathbb{B}^n$

$$\min_{x,y \in \Sigma} H(c(x), c(y)) = d(c)$$

Опр: c обнаруживает k ошибок, если $d(c) > k$



Опр.: C исправляет K ошибок если $d(C) > 2K$



$$\left.\begin{array}{l} H(a,a') \le K \\ H(a',b) \le K \end{array}\right\} H(a,b) \le 2K$$ противоречие

Утв 1: если код C испр K ошибок то C обн. 2K ошибок

Утв 2: если код C обнр. K ошибок то C испр $\left\lfloor \frac{K}{2} \right\rfloor$ ошибок

Утв 3: $\forall K$ $\exists$ код, обнар. K ошибок

Т Σ $|\Sigma| \le 2^n$

$\Sigma = \{c_1, c_2 \dots c_s\}$ $s \le 2^n$

c_1 00...0

c_2 00...1

c_3 00..10

c_s . . . . .

c_1 |0...0|0...0| ... |0...0| (1ый c_1, 2ой c_1, ..., s-ый c_1; блоки по K+1) → кодовое слово для c_1

c_2 |0...0|0...0| ... |1...1| (блоки по K+1)

(2K+1) → $C: \Sigma \to \mathbb{B}^{(2K+1)n}$

неэффективно, но $C: \Sigma \to \mathbb{B}^{(K+1)n}$ можно обнаружить K ошибок (испр)

Опр.: $\mathbb{B}^n$ дискретный шар $x \in \mathbb{B}^n$, $r \in \mathbb{Z}^+$

$S(x,r) = \{ y \mid H(x,y) \leq r \}$

$S(0000,1) = \{ 0000, 0001, 0010, 0100, 1000 \}$ – шар

Опр.: $V(n,r)$ – объем шара в $\mathbb{B}^n$, радиус r

Замечание: $V(n,r) = |S(x,r)| \quad \forall x \in \mathbb{B}^n$

$S(x,r) = \{ z \mid z = t \oplus x \oplus y, t \in S(y,r) \}$

$H(x,z) = |\{ i \mid x[i] \neq z[i] \}|$

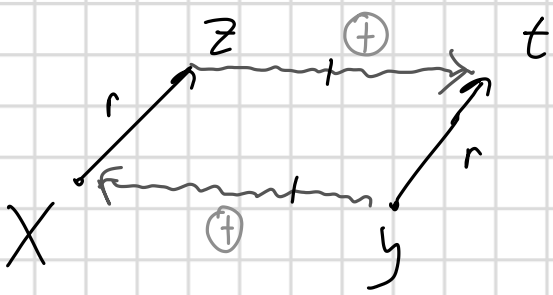
$y = x \oplus (x \oplus y)$

$t = z \oplus (x \oplus y)$

$H(y,t) = |\{ i \mid y[i] \neq t[i] \}| = |\{ i : x_i \oplus (x_i \oplus y_i) \neq z_i \oplus (x_i \oplus y_i) \}| = |\{ i \mid x_i \neq z_i \}| =$

$= H(x,z)$

если сделать хог то получим



Лемма: $x \neq y \in \Sigma$

C – код исп K ошибок

то $S(c(x), K) \cap S(c(y), K) = \varnothing$

$\exists\, z \in S(c(x), K) \cap S(c(y), K)$

$H(c(x), z) \leq K$

$H(c(y), z) \leq K$

$\Big\} \; H(c(x), c(y)) \leq 2K$ противоречие

Теорема (Граница Хемминга)

C – код для m – симв алфв. исправ. K ошибок и

$C: \Sigma \to \mathbb{B}^n$, то $m \cdot V(n, K) \leq 2^n$

Пр.: 3 символа, исп 1 ош., $m = 3$, $K = 1$,

$n = 3$?

$3 \cdot V(3, 1) \leq 2^3$

$3 \cdot 4 \leq 2^3$ неверно $\Rightarrow$ кода нет

$\log_2 m + \log_2 V(n, K) \leq n$

$\frac{\log_2 m}{n} \leq 1 - \frac{\log_2 V(n, K)}{n}$

↑ плотность информации в коде

$\forall\ B^n \qquad x_1 = c(1)$

$S(x_1; 2k)$ – нельзя брать

$x_2 \in B^n \setminus S(x_1; 2k)$

$x_2 = c(2)$

$S(x_2; 2k)$ – нельзя

$x_3 \in B^n \setminus \left(\bigcup_{i=1}^{2} S(x_i; 2k) \right)$

$\vdots$

$\exists\ m = 3,\ k = 1,\ n = 3$

$x_1 = 000$ тогда $x_2 = 111 \Rightarrow x_3 = \emptyset$

Теорема (Граница Гильберта)

т. $V(n; 2k) \le 2^n$, то $\exists\ C: \Sigma \to B^n$, исправляющий k ошибок, $|\Sigma| = m$

$$V(n, r) = 1 + n + \frac{n(n-1)}{2} + \ldots + C_n^r$$

$r = 1$

$V(n, 1) = 1 + n$

$m(n+1) \le 2^n \iff m \le \frac{2^n}{n+1}$

Код Хемминга

$K = l$ (примерно) $\Leftrightarrow$ $m \cdot V(n,1) \le 2^n$

$K > 1$ сложно и непонятно

4 контрольных 2^i поз

7 – информационных

информационные и контрольные биты

$\exists\ |\Sigma| \le 128$

Код постоянной длины $\rightarrow$ B^7

Контрольный бит 2^i соот позиции $P_i = \{ j \mid j \,\&\, 2^i = 2^i \}$

позиция

$\{1,3,5,7,9,11\} = P_0$

$\{2,3,6,7,10,11\} = P_1$

$\{4,5,6,7\} = P_2$

$\{8,9,10,11\} = P_3$

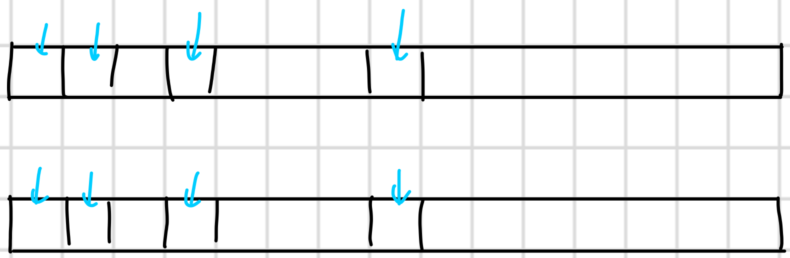
Контрольный бит i исх. так, чтобы $\bigoplus_{j \in P_i} a_j = 0$

$1\,00\,1111 \rightarrow 00110011111$

7 11

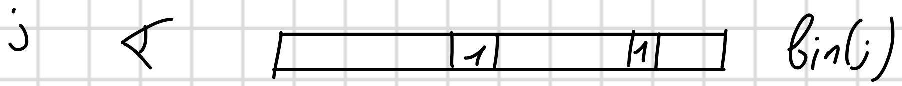
Теорема Код Хемминга исп 1 ошибку

$H(x,y) \geq 3$



Разл 3 инф бита → ОК

Разл 1 инф бит



≥2 контр битов

Разл 2 инф бита

=> хотя бы 1-ин контрольный бит различ.