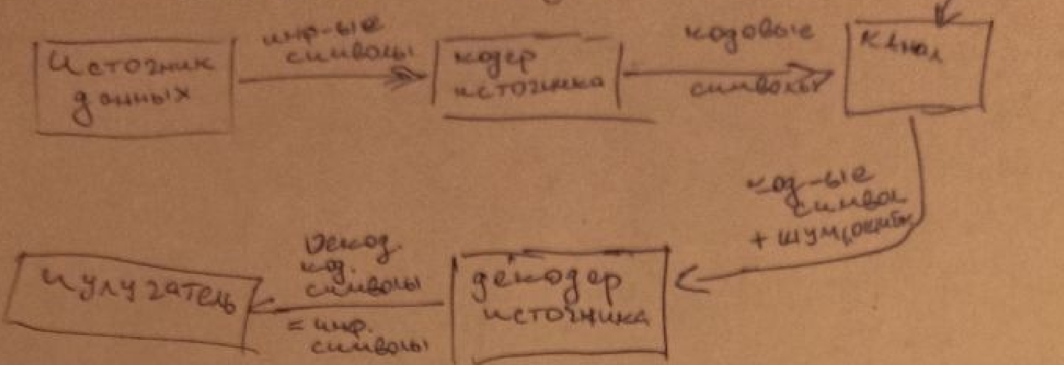
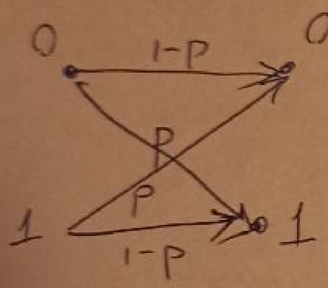
Лекция 1.

Упрощенная модель цифровой системы связи.



Дискретные последовательности символы $\in GF(2) = \{0,1\}$

Двоично симметричный канал



p – переходная вероятность (вероятность ошибки) одного символа

$\exists\, p=10^{-3}$ как уменьшить вероятность ошибки? очевидный вариант продублировать ещё два раза. и восстановить исходные символы по мажоритарному признаку

$0 \to 000$

$1 \to 111$

инф. символы — кодовое слово

вероятность ошибки – P_e

при $0\to0$, $1\to1$ $P_e = p$

при $0\to000$, $1\to111$

000→000
001
010
011
100
101
110
111

$$P_e = 3p^2(1-p) + p^3 \approx 10^{-6}$$

есть вариант лучше

00 → 00000
01 → 10110
10 → 01011
$\underset{k}{11} \to \underbrace{11101}_{n}$

тут лучше, слово всё ещё можно востановить ~~(порой, даже если ошибка в передачи двух символов~~

выгода в том что код "компактнее" было из 1 символа 3, а сейчас из одного символа 2,5.

$$\boxed{R = \frac{k}{n} \text{ — скорость кода}}$$

~~•→•••~~ • → ••• $R = \frac{1}{3}$ •• → ••••• $R = \frac{2}{5}$

Для ДСК с переходн. вер-ю p вводитс понятие пропускная способность $C = 1 - h(p)$

$$h(p) = -p\log_2(p) - (1-p)\log_2(1-p)$$

(энтропия двоичного ансамбля

> при R меньшей C можно обеспечить сколь угодно малую P_e за счёт увеличения длины кодовых слов из чего следует увеличение скорости кодирования и декодирования. если $R > C$ то надёжная передача невозможна

Вес Хемминга

если x - кодовое слово, то $w(x)$ - вес Хемминга и определяется как число ненулевых эл-тов в x (В двоичном случае - число единиц)

Расстояние Хеминга между двумя кодовыми словами x и y → $d(x, y)$ = количество символов слова, которые отличаются друг от друга

		w
x	001101	3
y	101001	3

$d(x, y) = 2$

$d(x,y) = w(x \oplus y)$ ~~А1~~ $\quad d(x,y) = w(x \oplus y)$

↑
побитово mod 2

$d(x,0) = w(x)$

$d(x,y)$ – матрица (удовл. аксиомам)

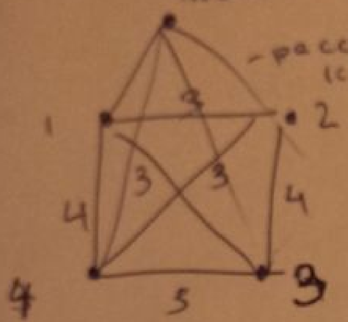
$t=1$ – сколько ошибок исправляет

00 → 00000 (1)
01 → 10110 (2)
10 → 01011 (3)
11 → 11101 (4)

$d(x,y)$	1	2	3	4
1	0	3	3	4
2	3	0	4	3
3	3	4	0	3
4	4	3	3	0

← $d_{min} = 3$

новое слово



– расстояния (самое минимал. и есть решение)

$$d_{min} = \min_{x \neq y} d(x,y)$$

~~тред~~

$$t \leq \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor$$

↑
кол-во исправл. ошибок

~~ИЯЛ~~-така

Iᵇ Линейный код – код, в котором сумма двух любых кодовых слов тоже явл-ся кодовым словом. C – мн.во кодовых слов

$$\forall x, y \in C \Rightarrow (x \oplus y) \in C$$

$$d(x,y) = w(x \oplus y) = w(z) = w(z \oplus 0) = d(z,0)$$

$$d_{min} = \min_{x,y \in C, x \neq y} d(x,y) = \min_{z \in C, z \neq 0} w(z)$$

__Опр__ линейный q-ичный код (над $GF(q)$)

($[n, k]$ код – C) – называют $\forall$ k-мерное подпр-во F_q^n всевозможных векторов длины n

$\uparrow$ код. $\uparrow$ инф.

пример:

$q=3$ $k=2$ $n=5$

$$F_3^2 \left\{ \begin{array}{lcl} 00 & — & 00000 \\ 01 & & \\ 02 & & \\ 10 & & \\ 11 & & \\ 12 & & \\ 20 & & \\ 21 & & \\ 22 & — & 22222 \\ \underleftrightarrow{\ \ }_{2} & & \underleftrightarrow{\qquad}_{5} \end{array} \right.$$

$q^n = 3^5 =$