Код – набор кодовых слов.

Эффективный код:

- длинные (n) -> большое минимальное расстояние

- сложность кодера и декодера

Линейные кода – > G, mG = C

Порождающие матрицы линейного (n, k) кода – матрица размера k на n, строки – базисные вектора лин. пространства.

Кодовые слова – линейные комбинации базисных векторов.

$M = (m_1, \dots m_k), c = mG, c = (c_1, .. c_n)$

$h = (h_1, .. h_n), c \in C, \left(\underset{c}{\rightarrow}, \underset{h}{\rightarrow}\right) = 0$

Какова размерность линейного пространства проверок $GH^T = 0$

G: k на n – k линейно-независимых строк – ранг = k => в матрице G существует k линейно независимых столбцов.

Индексы ЛН столбцов образуют информационную совокупность, остальные – проверочную совокупность.

$$Gh^T = \begin{pmatrix} g_{1,1} \cdot\cdot g_{1,k} \, g_{1,k+1} \cdot\cdot g_{1,n} \\ \cdot\cdot \; \cdot\cdot \; \cdot\cdot \quad \cdot\cdot \quad \cdot\cdot \; \cdot\cdot \\ g_{k,1} \cdot\cdot g_{k,k} \, g_{k,k+1} \cdot\cdot g_{k,n} \end{pmatrix} \begin{pmatrix} x_! \\ \cdot\cdot \\ x_k \\ h_{k+1} \\ \cdot\cdot \\ h_n \end{pmatrix}$$

Зафиксируем $h_{k+1}, .. h_n$

Найти $x_1, .. k_k$

$$\underset{g_i}{\rightarrow} = \begin{pmatrix} g_{1,i} \\ \cdot\cdot \\ g_{k,i} \end{pmatrix}$$

$$\underset{g_1}{\rightarrow} x_1 + .. + \underset{g_k}{\rightarrow} x_k + .. \underset{g_n}{\rightarrow} x_n = 0$$

$$\begin{pmatrix} g_{1,1} \cdot\cdot g_{1,k} \\ \cdot\cdot \; \cdot\cdot \; \cdot\cdot \\ g_{k,1} \cdot\cdot g_{k,k} \end{pmatrix} \begin{pmatrix} x_! \\ \cdot\cdot \\ x_K \end{pmatrix} = -(\underset{g_{k+1}}{\longrightarrow} h_{k+1} + .. + \underset{g_n}{\rightarrow} h_n)$$

det левой части не равен 0.

Для GF(2) $(h_{k+1}, .. h_n) - 2^{n-k}$ способов представить

H = (n-k) * n

H = (n-k) * n, r = n - k – избыточность кода

$G_{k*n} = [I_{k*k} \; P]$ – систематический вид

$H = (P^T I_k)$

Пример

$$G = \begin{pmatrix} 110100 \\ 011010 \\ 101001 \end{pmatrix}$$

$$G_{sys} = \begin{pmatrix} 100110 \\ 010011 \\ 001101 \end{pmatrix}$$

$$H_{sys} = \begin{pmatrix} 101100 \\ 110010 \\ 011001 \end{pmatrix}$$

$$H = \begin{pmatrix} 100101 \\ 010110 \\ 001011 \end{pmatrix}$$

$d_{min} = \min\big((\omega) mG\big)$ *по m не равным 0*

Чтобы найти d_{min} достаточно найти минимальный набор линейно независимых столбцов H.

Теорема. Минимальное расстояние линейного (n, k) - кода равно d в том и только в том случае, когда любые d-1 столбец проверочной матрицы линейно независимы и существует набор из d линейно зависимых столбцов.

Сколько в матрице H линейно независимых столбцов.(n-k)

Теорема. Граница символов.

Минимальное расстояние линейного (n,k) – кода удовлетворяет неравенству:

$$d \leq n - k + 1$$

Дуальный код к данному код — это код, порождающая матрица которого является проверочной матрицей данного.

Примеры кодов

(n, n-1) – код, H=(1..1)

$$G = \begin{pmatrix} I_{n-1*n-1} \begin{matrix} 1 \\ 1 \\ 1 \\ 1 \end{matrix} \end{pmatrix}$$

Код с проверкой на чётность

Может обнаружить любые ошибки нечетного веса

Коды Хэмминга

Двоичные кода Хэмминга оптимальны в том смысле, что не существует кодов (даже линейных) с большим числом кодовых слов с расстоянием d=3 при такой же длине.

Для дуальных кодов кодам Хэмминга $d = 2^{n-1}$ – симметричный код

Синдрон

ное декодирование