Обработка и интерпретация сигналов
Конспект лекции 2

Александр Клыков

1 Эффективность кода

Определение 1. ***Код*** *— это множество (набор)* ***кодовых слов****.*

Интуитивно **эффективный** код должен сочетать:

- достаточно большую длину кодового слова n (что обычно позволяет увеличить минимальное расстояние);
- приемлемую сложность кодера и декодера.

В дальнейшем рассматриваем в основном линейные коды над GF(2).

2 Линейные коды и порождающая матрица

Пусть задан линейный (n, k)-код C над GF(2).

Определение 2. ***Порождающая матрица*** G *линейного* (n, k)*-кода — это матрица размера* $k \times n$*, строки которой образуют базис данного линейного подпространства. Любое кодовое слово является линейной комбинацией строк матрицы* G*.*

Пусть

$$m = (m_1, \ldots, m_k) \in \mathrm{GF}(2)^k$$

— **информационное слово**. Тогда соответствующее **кодовое слово**

$$c = (c_1, \ldots, c_n) \in \mathrm{GF}(2)^n$$

вычисляется по формуле

$$c = mG.$$

3 Проверки и проверочная матрица

Пусть $h = (h_1, \ldots, h_n)$ — вектор длины n над GF(2).

Определение 3. *Вектор* h *называется* ***проверкой*** *(ортогональным вектором кода), если для любого* $c \in C$ *выполняется*

$$(c, h) = c_1 h_1 + c_2 h_2 + \cdots + c_n h_n = 0.$$

Так как любое c является линейной комбинацией строк G, условие ортогональности всех кодовых слов эквивалентно

$$Gh^T = 0.$$

3.1 Сколько существует проверок

Матрица G имеет ранг k (строки линейно независимы). Значит пространство решений системы

$$Gh^T = 0$$

имеет размерность $n - k$. То есть существует 2^{n-k} различных проверок h (в двоичном случае).

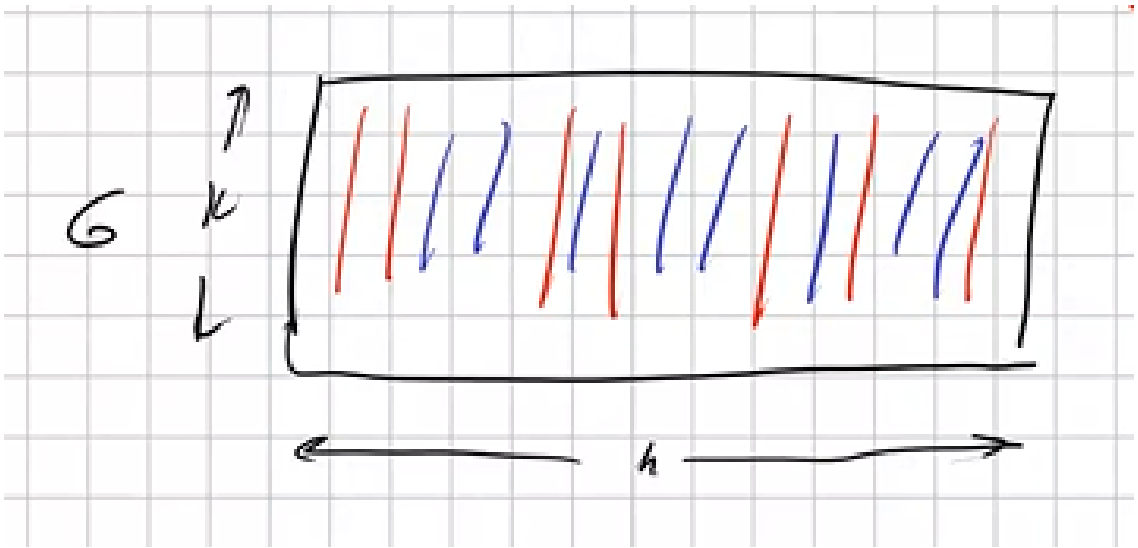
Определение 4. ***Проверочная матрица*** *(parity-check matrix) H — это матрица размера $(n - k) \times n$, строки которой образуют базис пространства проверок. Тогда выполняются соотношения:*

$$GH^T = 0, \qquad cH^T = 0 \quad \textit{для любого } c \in C.$$

4 Информационная и проверочная совокупности столбцов

Так как $\mathrm{rank}(G) = k$, в матрице G существует набор из k линейно независимых столбцов. Индексы этих столбцов образуют **информационную совокупность**. Оставшиеся индексы образуют **проверочную совокупность**.

Часто для удобства перестановкой столбцов добиваются, чтобы первые k позиций были информационными.



5 Систематический вид и связь G и H

С помощью элементарных преобразований строк (метод Гаусса) и перестановок столбцов порождающую матрицу можно привести к систематическому виду:

$$G = \begin{bmatrix} I_k & P \end{bmatrix},$$

где I_k — единичная матрица размера $k \times k$, а P — матрица размера $k \times (n - k)$.

Определение 5. *Код называется* ***систематическим****, если его порождающая матрица имеет вид $G = [I_k \ P]$. Тогда*

$$c = mG = (m, \ mP),$$

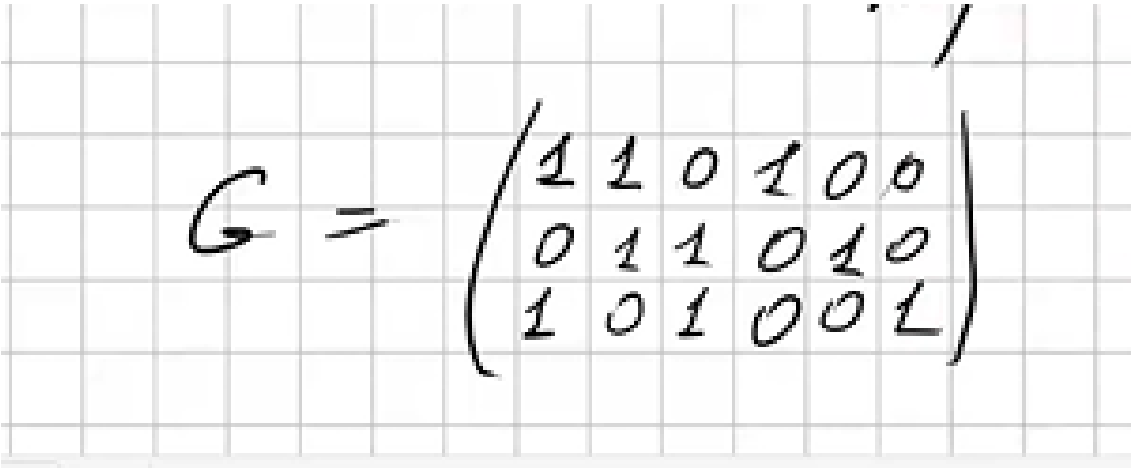
то есть первые k символов кодового слова совпадают с информационными.

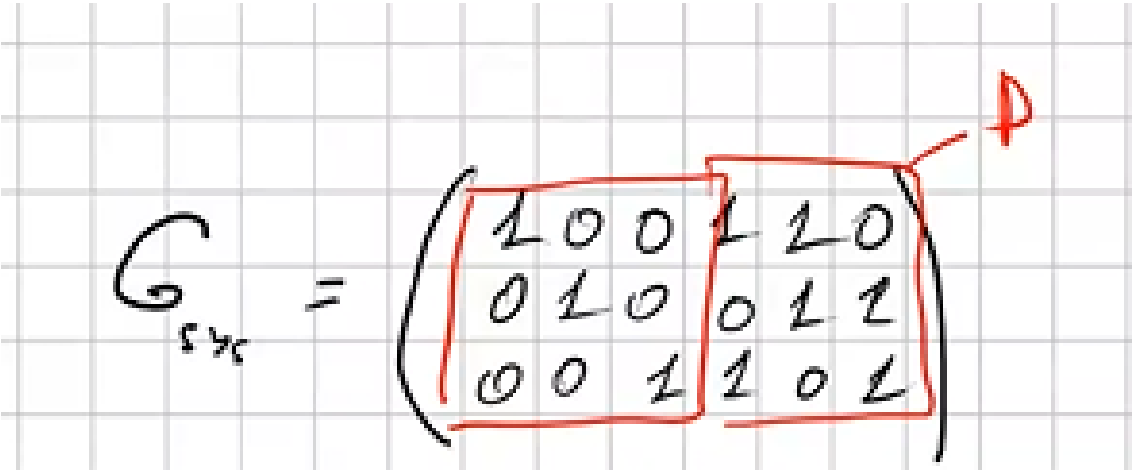
Утверждение 1. *Для систематического кода $G = [I_k \; P]$ можно взять проверочную матрицу в виде*

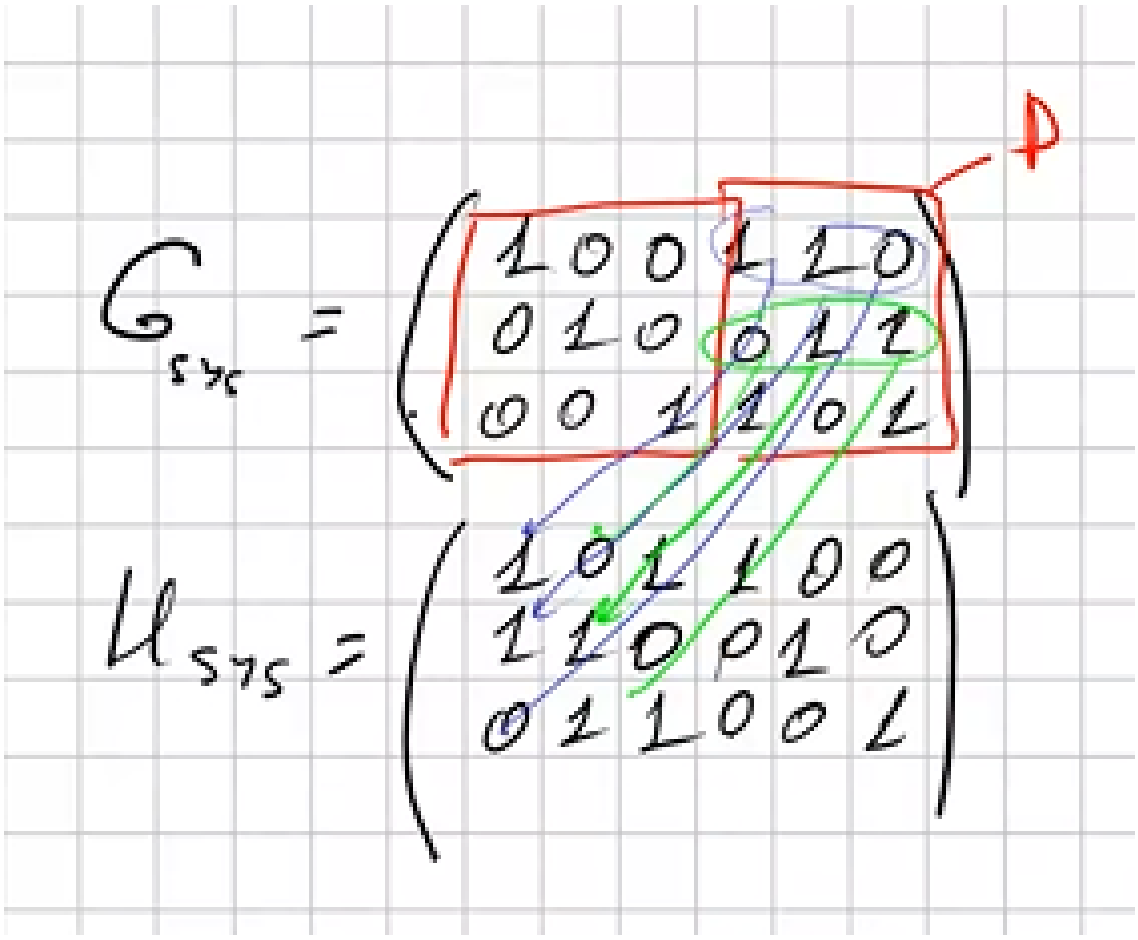
$$H = \begin{bmatrix} P^T & I_r \end{bmatrix}, \qquad r = n - k.$$

(Все операции выполняются в GF(2)*.)*

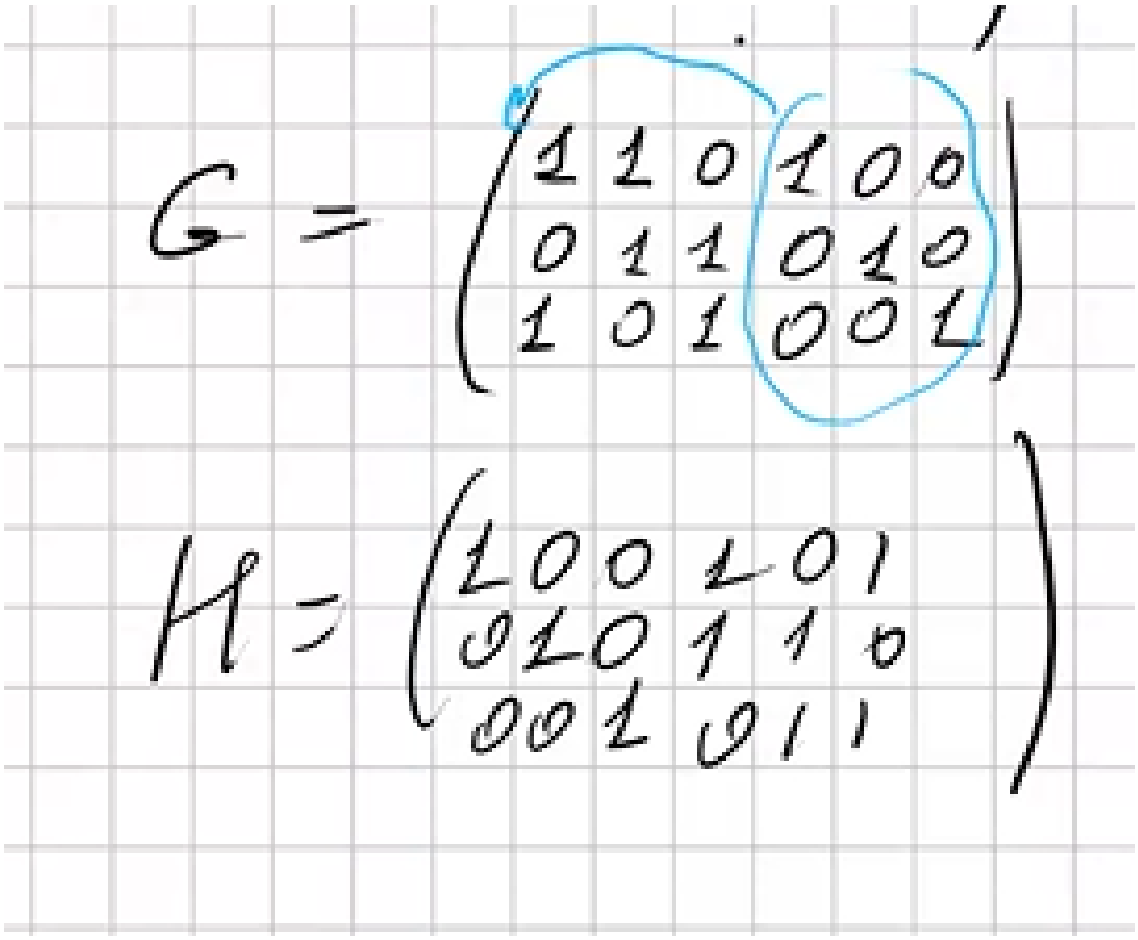
5.1 Пример с матрицами G и H







Если требуется получить проверочную матрицу для *исходной* матрицы G, нужно «откатить» преобразования (обратное преобразование).



6 Минимальное расстояние и вычисление через G

Одной из ключевых характеристик кода является **минимальное расстояние** $d_{\min}$. Для линейного кода:

$$d_{\min} = \min_{m \neq 0} \omega(mG),$$

где $\omega(\cdot)$ — вес Хемминга, а минимум берётся по всем ненулевым информационным словам $m \in \mathrm{GF}(2)^k$.

Чтобы вычислить $d_{\min}$ прямым перебором через G, нужно рассмотреть $2^k - 1$ ненулевых вариантов m.

7 Минимальное расстояние и проверочная матрица

Из условия проверок:

$$cH^T = 0.$$

Пусть кодовое слово c имеет вес $\omega(c) = t$ и единицы стоят в позициях $i_1, \ldots, i_t$. Тогда

$$cH^T = h_{i_1} + h_{i_2} + \cdots + h_{i_t} = 0,$$

где h_j — j-й столбец матрицы H. Следовательно, столбцы $h_{i_1}, \ldots, h_{i_t}$ линейно зависимы.

Отсюда важный критерий.

Теорема 1. *Минимальное расстояние линейного (n, k)-кода равно d тогда и только тогда, когда:*

- *любые $d-1$ столбцов проверочной матрицы H линейно независимы;*
- *существует набор из d столбцов H, который линейно зависим.*

Так как $\mathrm{rank}(H) = n-k$, то в H существует $n-k$ линейно независимых столбцов (и не может быть больше).

7.1 Граница Синглтона

Теорема 2 (Граница Синглтона)**.** *Минимальное расстояние линейного (n,k)-кода удовлетворяет неравенству*

$$d_{\min} \le n - k + 1.$$

8 Дуальный код

Определение 6. ***Дуальный код*** *$C^{\perp}$ к коду C — это код, порождающая матрица которого является проверочной матрицей кода C. То есть если для C заданы G и H и выполнено $GH^T = 0$, то для дуального кода можно взять*

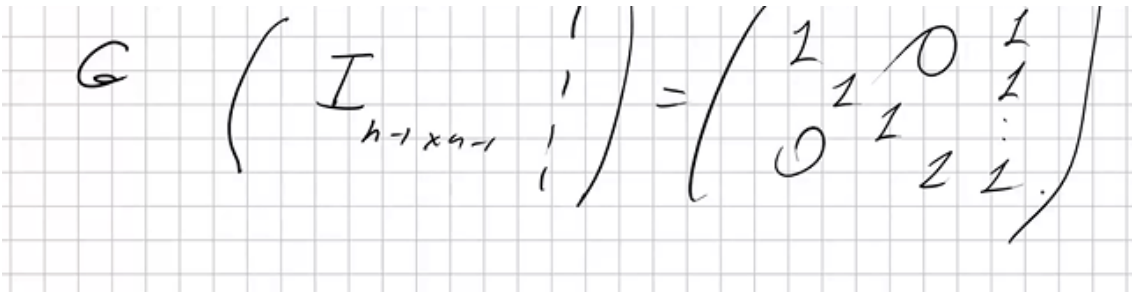
$$G^{\perp} = H, \qquad H^{\perp} = G.$$

9 Код чётности: пример $(n, n-1)$

Рассмотрим код с параметрами $(n, n-1)$. Тогда размер проверочной матрицы равен $1 \times n$, и можно взять

$$H = (1\ 1\ \cdots\ 1).$$

Такой код называется **кодом с проверкой на чётность**: любое кодовое слово имеет чётный вес.



Для этого кода $d_{\min} = 2$: он **не исправляет** ошибки, но **обнаруживает** любые ошибки нечётной кратности.

10 Исправление одиночной ошибки и коды Хэмминга

Пусть передано $c = mG$, а в канале возникла ошибка e веса $\omega(e) = 1$. Тогда принято слово $c + e$. Рассмотрим синдром:

$$(c+e)H^T = cH^T + eH^T = eH^T.$$

Если e имеет единственную единицу в позиции j, то

$$eH^T = h_j,$$

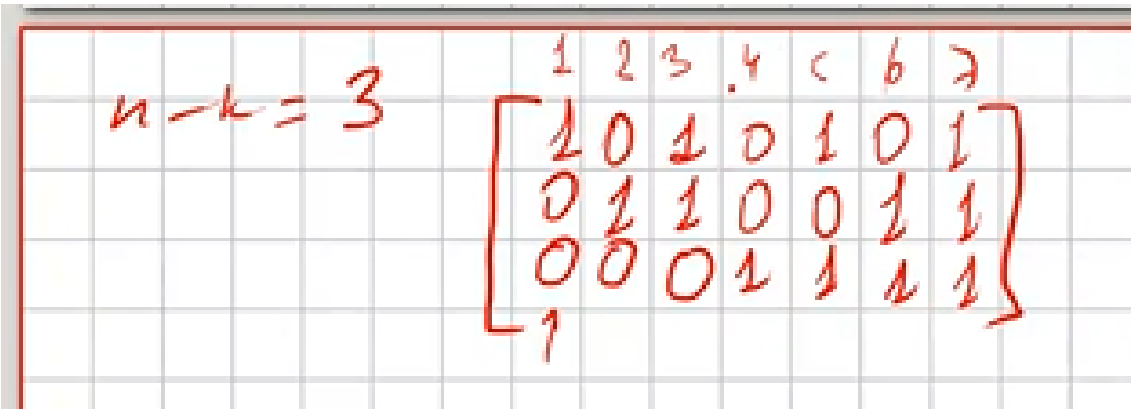
то есть синдром равен j-му столбцу H. Значит, по синдрому можно определить позицию ошибки и исправить её.

Идея кода Хэмминга: построить H так, чтобы **все столбцы были различны и ненулевые**. Тогда каждый возможный синдром соответствует ровно одной позиции ошибки.

Пусть $r = n - k$. Если выбрать r так, что все ненулевые двоичные столбцы длины r использованы ровно по одному разу, то

$$n = 2^r - 1, \qquad k = n - r = 2^r - 1 - r.$$

Это семейство называется **двоичными кодами Хэмминга**. Для них $d_{\min} = 3$ и они исправляют одну ошибку.



Замечание 1. *В матрице H Хэмминга при заданном r число столбцов равно $2^r - 1$ (все ненулевые столбцы длины r).*

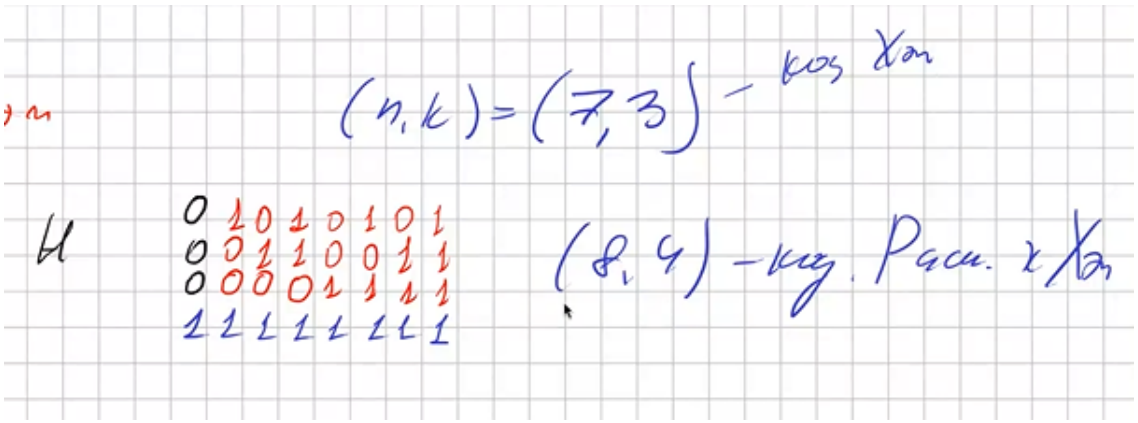
10.1 Дуальный коду Хэмминга и симплексный код

Дуальный код коду Хэмминга (то есть код, порождённый матрицей $H_{\text{Хэм}}$) называется **симплексным кодом**. Для симплексного кода характерно, что все ненулевые кодовые слова имеют одинаковый вес, а расстояния между различными кодовыми словами одинаковы. (В лекции отмечалось, что параметры расстояния зависят от r; обычно для двоичного симплексного кода длины $n = 2^r - 1$ минимальное расстояние равно 2^{r-1}.)

11 Расширенный код Хэмминга

Расширенный код Хэмминга получается из кода Хэмминга добавлением общей проверки на чётность. На уровне проверочной матрицы: к матрице H Хэмминга добавляют нулевой столбец, а затем добавляют строку из всех единиц (как было показано в лекции).

Для примера: код Хэмминга имеет параметры $(n, k) = (7, 4)$, а расширенный код Хэмминга — $(8, 4)$.



Также в лекции упоминалось, что дуальный код к расширенному коду Хэмминга связан с **кодами Рида–Маллера первого порядка**.