# Билет 1.1:
# Система передачи информации. Двоичный симметричный канал

*Система передачи информации* включает передатчик, который передает последовательности длины $n$ из 0 и 1: $u = (u_1, u_2, ..., u_n)$, где $u_i \in \{0, 1\}$. В канале действует случайная помеха: каждый символ передаваемой последовательности независимо от других может быть искажен с вероятностью $\tau < \frac{1}{2}$.

*Двоичный симметричный канал* описывается следующим образом:

$$p(0|0) = p(1|1) = 1 - \tau, \quad p(0|1) = p(1|0) = \tau$$


Рис. 1: Простейшая модель передачи данных

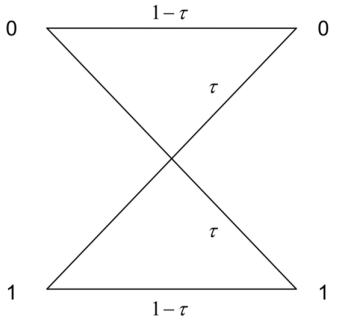


Рис. 2: Двоичный симметричный канал

# Билет 1.2:
# Кодовое расстояние. Связь между кодовым расстоянием и корректирующей способностью кода

Кодовое расстояние $d$ между двумя кодовыми словами - это число позиций, в которых эти слова отличаются.

Кодовое расстояние кода - это минимальное расстояние между любыми двумя кодовыми словами этого кода. Корректирующая способность кода тесно связана с кодовым расстоянием. Если кодовое расстояние кода равно $d$, то этот код может исправить любые $\frac{d-1}{2}$ ошибок.

# Билет 1.3:
# Скорость передачи данных и кодовое расстояние (граница Гилберта)

*Скорость кода* $R$ определяется как $R = \frac{k}{n}$ или $R = \frac{\log_2 M}{n}$, где $k$ - длина информационного вектора, $n$ - длина кода, $M$ - мощность кода.

*Граница Гилберта* устанавливает связь между скоростью кода, кодовым расстоянием и вероятностью ошибки.

*Теорема*

Если $R < 1 - \frac{1}{n} \log_2 \sum_{i=1}^{d-1} \binom{n}{i}$, то код с параметрами $(n, M, d)$ существует.

# Билет 1.4:
# Код как линейное векторное подпространство. Порождающая и проверочная матрицы кода

• *Определение:* Линейным векторным пространством над полем F называется множество V векторов, которые удовлетворяют условиям:

1. Множество V является аддитивной абелевой группой.
2. $\forall c \in F, v \in V \rightarrow cv \in V$
3. Выполняются дистрибутивные законы, то есть если:

$$\forall c \in F, v \in V \rightarrow c \cdot (u + v) = c \cdot u + c \cdot v, \quad \forall c, d \in F, v \in V \rightarrow v \cdot (c + d) = v \cdot d + c \cdot v$$

4. Умножение ассоциативно, то есть $(c \cdot d) \cdot v = c \cdot (d \cdot v)$

• *Определение:* Подмножество векторов A пространства V называется подпространством, если в нём выполняются условия определения пространства.

*Порождающая матрица линейного кода:*

1. Размерность $V$ : $\dim V = n$, а значит его базис состоит из $n$ векторов, например $e_1, e_2, ..., e_n$, где $e_i$ — единичные орты
2. Размерность $A$ : $\dim V = k$, а значит его базис состоит из $k$ векторов $a_1, a_2, ..., a_k$ длины $n$. Это значит, что любой вектор $c \in A$ имеет вид: $c = \alpha_1 a_1 + \alpha_2 a_2 + ... + \alpha_k a_k$, где $\alpha_i \in GF(q)$.
3. Составим $k \times n$ матрицу $G$, называемую порождающей матрицей кода $A$:

$$G = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & a_{k3} & \dots & a_{kn} \end{pmatrix}$$

*Проверочная матрица линейного кода:*

Ортогональное подпространство состоит из $q^{n-k}$ векторов, а значит его базис состоит из $n - k$ векторов длины n: Причём $\forall v \in A : (v, h_i) = 0$. По аналогии с G построим порождающую матрицу подпространства $A'$:

$$H = \begin{pmatrix} h_1 \\ h_2 \\ \vdots \\ h_{n-k} \end{pmatrix} = \begin{pmatrix} h_{11} & h_{12} & h_{13} & \dots & h_{1n} \\ h_{21} & h_{22} & h_{23} & \dots & h_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_{n-k,1} & h_{n-k2} & h_{n-k3} & \dots & h_{n-k,n} \end{pmatrix}$$

Данную матрицу называют проверочной матрицей линейного кода, так как:

$$\forall v \in A : H \cdot v^t = \begin{pmatrix} (v, h_1) \\ (v, h_2) \\ \vdots \\ (v, h_{n-k}) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = 0$$

# Билет 1.5:
# Каноническая форма проверочной и порождающей матриц. Их связь друг с другом.

*Каноническая форма базисных матриц*

*Идея: выделить в матрице $G$ единичную подматрицу.*

1. В $i$-й строке ($i = 1, 2, ..., k$) матрицы $G$ найдется по крайней мере одна ненулевая компонента. Пусть первая отличная от нуля компонента этой строки находится в $j$-м столбце. Разделим каждую компоненту строки на $a_{ij}$. В результате получится новая компонента $a'_{ij}$ матрицы, равная единице.
2. К каждой $z$-й строке ($z \neq i$) прибавим $i$-ю строку, умноженную на $a_{zj}$. В результате в $j$-м столбце $i$-я строка будет содержать единицу, а все остальные строки — нули.
3. Применим шаги (1)-(2) к каждой строке матрицы $G$.
4. Столбцы с одной единицей переставим на первые $k$ позиций.

*Связь между проверочной и порождающей матрицами*

$$\forall v \in A : H \cdot v^t = \begin{pmatrix} (v, h_1) \\ (v, h_2) \\ \vdots \\ (v, h_{n-k}) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = 0$$

# Билет 1.6:
# Проверочная матрица и минимальное расстояние кода. Связь метрических свойств кода со столбцами проверочной матрицы.

Теория про проверочную матрицу находится в билете 4.

- *Определение:* Весом $w(v)$ вектора $v$ называется число отличных от нуля его компонент.

## *Основная теорема о минимальном расстоянии линейного кода*

Любому значению расстояния $d(v_1, v_2)$ между векторами $v_1$ и $v_2$ линейного $(n, k)$ – кода отвечает кодовый вектор $v_1 v_2 = v$, для веса $w(v)$ которого выполняется равенство $w(v) = d(v_1, v_2)$. И, наоборот, каждому значению $w(v)$ веса кодового вектора v отвечает пара кодовых векторов v1 и v2 с расстоянием $d(v_1, v_2) = w(v)$, причём таких пар имеется в точности $q^k$.

## *Доказательство*

В силу того, что код – всегда группа с операцией поразрядного сложения векторов, разность двух кодовых векторов есть снова кодовый вектор: $v_1 - v_2 = v$, и вес $w(v)$ вектора $v$, то есть число отличных от нуля его компонент в точности равно расстоянию $d(v_1, v_2)$. Наоборот, пусть вектор v имеет вес $w(v)$. Сложив вектор v с произвольным кодовым вектором $v_i$, получим, что $d(v + v_i, v_i) = w(v)$, чем и завершается доказательство. Остаётся вспомнить, что кодовых векторов $v_i$ имеется в точности $q^k$

## *Метрические свойства проверочной матрицы*

Пусть $v = (a_1, a_2, \ldots, a_n)$ – кодовый вектор. Представим проверочную матрицу в виде: $H = [h_1 h_2 \ldots h_n]$, где $h_i$ есть i-вектор-столбец проверочной матрицы. Тогда выражение $v \cdot H^T = 0$ можно переписать в виде $a_1 h_1 + a_2 h_2 + \cdots + a_n h_n = 0$.

Иначе говоря, каждый отличный от нуля кодовый вектор $v$ задаёт нетривиальное соотношение линейной зависимости векторов-столбцов проверочной матрицы. Пусть $a_{i1}, a_{i2}, \ldots, a_{iw}$ все отличные от нуля компоненты вектора $v$. Тогда равенство превратится в $a_{i1} h_{i1} + a_{i2} h_{i2} + \ldots + a_{iw} h_{iw} = 0$.

Если $w \leq d - 1$, то это означает, что имеется такой кодовый вектор, вес которого не превосходит $d1$, а значит, найдутся такие пары векторов, расстояния между которыми не превосходит $d - 1$. Тем более, минимальное расстояние оказывается меньше чем $d$. С другой стороны, если любые $d - 1$ столбцов проверочной матрицы линейно независимы, то минимальный вес, а значит минимальное расстояние кода, не менее $d$.

## *Основная теорема о проверочной матрице*

Для того, чтобы минимальное расстояние линейного кода было не менее, чем $d$, необходимо и достаточно, чтобы любые $d - 1$ и менее столбцов проверочной матрицы были линейно независимы.

## *Следствие*

Граница Сигнлтона: $d - 1 \leq n - k$

# Билет 1.7:
# Границы Синглтона и Варшамова-Гилберта.

*Граница Сигнлтона*

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

*Граница Варшамова-Гилберта*

Будем строить проверочную матрицу $H$ размера $(n-k) \cdot n$ следующим образом. В качестве первого столбца $h_1$ можно выбрать любой ненулевой столбец длины $n-k$. Вторым столбцом $h_2$ может стать любой из оставшихся $q^{n-k} - q$ столбцов, кроме ненулевого и $q-1$ столбцов, кратных столбцу $h_1$. Предположим, что выбрано уже $j$ столбцов и имеется не более

$$(q-1) \cdot \binom{1}{j} + (q-1)^2 \cdot \binom{2}{j} + \cdots + (q-1)^{d-2} \cdot \binom{d-2}{j}$$

их различных линейных комбинаций, содержащих $d-2$ и менее столбцов. Если эта величина меньше, чем $q^{n-k} - 1$, то можно добавить ещё один ненулевой столбец, который отличен от всех этих линейных комбинаций. Тогда никакие $d-1$ столбцов из выбранных $j+1$ столбцов не буду линейно зависимы.

Если выполняется соотношение:

$$(q-1) \cdot \binom{1}{n-1} + (q-1)^2 \cdot \binom{2}{n-1} + \cdots + (q-1)^{d-2} \cdot \binom{d-2}{n-1} < q^{n-k} - 1$$

то можно добавить ещё один ненулевой $n$-й столбец и любые $d-1$ и менее из этих $n$ столбцов будут линейно независимы. Проверочная матрица построена, у данной границы есть предельная форма:

$$R \leq 1 - h(\delta)$$

где $R = \frac{k}{n}, \delta = \frac{d}{n}$, $h(x)$ - функции энтропии.

График для данного билета есть в 3 лекции на последнем слайде.

# Билет 1.8: Декодирование линейного кода. Синдромное декодирование. Стандартное расположение.

*Основные теоремы синдромного декодирования*

1. Линейный код $A$ исправляет все независимые ошибки кратности $t$ и менее тогда и только тогда, когда все векторы веса $t$ и менее принадлежат различным смежным классам.
2. Минимальное расстояние линейного кода равно $d = 2t + 1$ тогда и только тогда, когда все векторы веса $1, 2, \ldots, t$ принадлежат различным смежным классам.

*Алгоритм синдромного декодирования*

- Вход: принятый вектор $v$, проверочная матрица $H$.
- Выход: кодовое слово $u$ или отказ от декодирования.

1. Вычисляем $S = v \cdot H^T$
2. По вычисленному $S$ находим смежный класс $A_i$ кода $A$
3. Ищем вектор минимального веса в $A_i$: если их несколько, то возвращаем отказ от декодирования, если вектор $e$ единственный, то переходим к следующему шагу
4. Возвращаем $u = v - e$

*Алгоритм через стандартное расположение*

1. Выпишем все векторы кодового подпространства слева направо, начиная с нулевого вектора.
2. Расположим произвольный смежный класс под кодовым подпространством, начиная с вектора $e$ минимального веса (лидер смежного класса), так чтобы под кодовым вектором $u$ находился вектор $v = u + e$ смежного класса.
3. Приняв вектор $v$, и вычислив его синдром $S$, определяем отвечающий ему смежный класс, а в нём находим вектор $v$.
4. Непосредственно над ним в первой строке таблицы находится перелвшийся вектор $u$.