

ЛЕКЦИЯ №14.

5. Каналы связи.

5.1. Дискретный канал связи (ДКС).

5.1.1. Информационные характеристики ДКС.



Как было показано ранее, среднее значение взаимной информации определяется по формуле:

$$I(X, Y) = \sum_{k=1}^L \sum_{l=1}^M p(a_k, b_l) I(a_k, b_l) = \sum_{k=1}^L \sum_{l=1}^M p(a_k, b_l) \log_2 \left(\frac{p(a_k, b_l)}{p(a_k) p(b_l)} \right) = I(Y, X).$$

Свойства средней взаимной информации.

1. $I(X, Y) \geq 0$, т.е. средняя взаимная информация – величина неотрицательная.
 $I(X, Y) = 0$, если X и Y не зависят друг от друга. Это наблюдается при больших шумах в канале связи.
2. $I(X, Y) = H(X)$, когда сообщения X и Y равны.
3. Среднюю взаимную информацию можно найти через энтропию и условную энтропию следующим образом:

$$I(X, Y) = H(X) - H(X / Y) = H(Y) - H(Y / X) \quad (5.1)$$

Скорость передачи взаимной информации – количество взаимной информации, переданной по каналу связи в единицу времени

$$R_{КС} = \frac{I(X, Y)}{T_H} \text{ (бит/с) }, \quad (5.2)$$

где T_H – время передачи.

Пропускная способность канала связи – максимально достижимая скорость передачи взаимной информации по каналу

$$C = \max_{\{p\}} R_{КС} \text{ (бит/с) }, \quad (5.3)$$

где максимум ищется по распределению вероятностей $\{p_k\}$.

Информационная эффективность (коэффициент использования канала связи) определяется как

$$\eta = \frac{R_{КС}}{C} \quad (5.4)$$

$0 \leq \eta < 1$, η тем больше, чем ближе R_{RC} к C .

5.1.2. Модель дискретного канала без памяти (ДКБП).

Пусть $X \in A = \{a_1, \dots, a_n\}$, $Y \in B = \{b_1, \dots, b_m\}$ с вероятностями появления $p(a_k)$, $p(b_j)$. Вход-выход канала описывается условными вероятностями $p(b_j / a_k) = P\{Y = b_j / X = a_k\}$, $j = 1, 2, \dots, m$, $k = 1, 2, \dots, n$. Граф такого канала связи имеет вид, изображенный на рисунке 5.1.

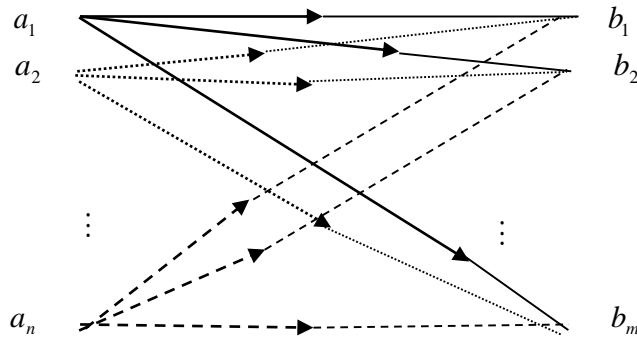


Рисунок 5.1. Граф ДКС без памяти.

Например, переход от a_1 к b_2 описывается вероятностью $p(b_2 / a_1)$ и т.д.

Двоичный симметричный канал (ДСКС) является частным случаем ДКБП. У ДСКС $X \in \{0, 1\}$, $Y \in \{0, 1\}$, где X - набор возможных значений входа, Y - набор возможных значений выхода. Если канальный шум и другие нарушения вызывают статистически независимые ошибки при передаче двоичной последовательности со средней вероятностью $p_{ош}$, то

$$P\{Y = 0 / X = 1\} = P\{Y = 1 / X = 0\} = p_{ош}, \quad P\{Y = 1 / X = 1\} = P\{Y = 0 / X = 0\} = 1 - p_{ош}.$$

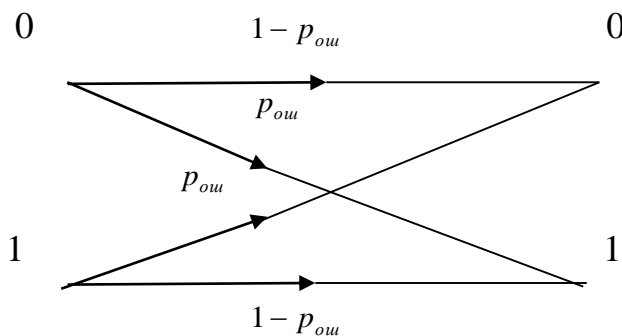


Рисунок 5.2. Граф ДСКС.

Пропускная способность ДСКС.

$I(X, Y) = I_{\max}(X, Y)$, если $p(0) = p(1) = 0.5$. Тогда по формулам (5.1), (5.2), (5.3) запишем:

$$C = \frac{1}{T_H} (H_{\max}(Y) - H_{\max}(Y / X)). \quad (5.5)$$

Далее, используя формулу полной вероятности ТВ, получим:

$$P\{Y = 0\} = p(0)P\{Y = 0 / X = 0\} + p(1)P\{Y = 0 / X = 1\} = 0.5(1 - p_{ош}) + 0.5p_{ош} = 0.5.$$

Аналогично определяем, что $P\{Y = 1\} = 0.5$. Т.е. выход канала равновероятен, тогда $H(Y) = H_{\max}(Y) = \log_2 n = \log_2 2 = 1$ бит/символ.

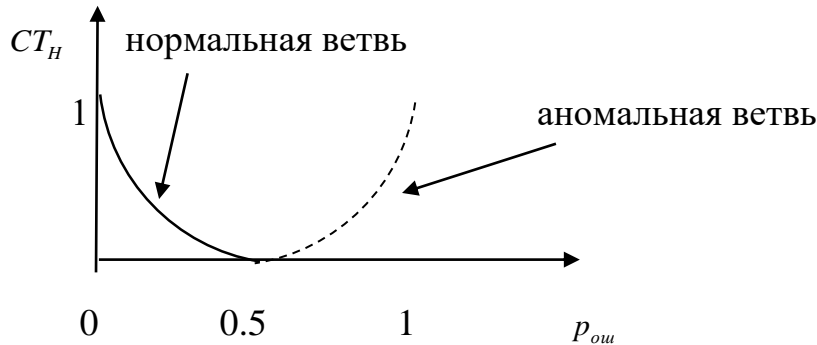
Затем по формуле условной энтропии найдем энтропию $H_{\max}(Y / X)$.

$$\begin{aligned} H_{\max}(Y / X) &= -\sum_{j=1}^2 \sum_{k=1}^2 p(b_j, a_k) \log_2(p(b_j / a_k)) = -\sum_{j=1}^2 \sum_{k=1}^2 p(a_k) p(b_j / a_k) \log_2(p(b_j / a_k)) = \\ &= -(p(0)p(1/0)\log_2 p(1/0) + p(1)p(1/1)\log_2 p(1/1) + p(0)p(0/0)\log_2 p(0/0) + p(1)p(0/1)\log_2 p(0/1)) = \\ &= -0.5(2p_{ош} \log_2 p_{ош} + 2(1 - p_{ош}) \log_2 (1 - p_{ош})) = -(p_{ош} \log_2 p_{ош} + (1 - p_{ош}) \log_2 (1 - p_{ош})). \end{aligned}$$

Подставляя выражения для $H_{\max}(Y)$ и $H_{\max}(Y / X)$ в формулу (5.5), окончательно получим пропускную способность ДСКС:

$$C = \frac{1}{T_H} (1 + p_{ош} \log_2 p_{ош} + (1 - p_{ош}) \log_2 (1 - p_{ош})) \quad (5.6)$$

Выводы. Пропускная способность ДСКС зависит только от вероятности ошибки $p_{ош}$, она увеличивается, если $p_{ош}$ уменьшается.



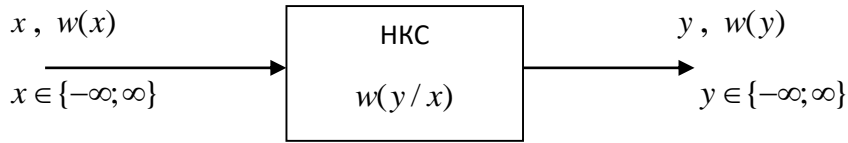
При увеличении отношения сигнал/шум вероятность ошибки $p_{ош}$ уменьшается, а пропускная способность увеличивается.

Теорема Шеннона для кодирования канала с шумами. Существуют кодеры и декодеры, которые позволяют создавать надежную связь со столь малой, насколько угодно вероятностью ошибки, если скорость передачи информации меньше пропускной способности канала связи:

$$R_{КС} < C \quad (5.7)$$

5.2. Непрерывный канал связи.

5.2.1. Информационные характеристики НКС.



Наиболее важный случай - канал с аддитивным белым гауссовским шумом (АБГШ), для которого

$$y = x + \mu, \quad (5.8)$$

где μ - стационарный гауссовский процесс с нулевым математическим ожиданием и дисперсией σ_μ^2 .

Среднее значение взаимной информации определяется по формуле

$$I(x, y) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} w(x, y) \log_2 \left(\frac{w(x, y)}{w(x)w(y)} \right) dx dy \quad (5.9)$$

Скорость передачи взаимной информации R_{KC} определяется по (5.2).

Пропускная способность НКС (см. ф-лу (5.3)) :

$$C = \max_{\{w(\bullet)\}} R_{KC} \text{ (бит/отсчет с)}$$

Пропускная способность гауссовского канала связи (ГКС).

Пусть ширина полосы рабочих частот канала $F_\epsilon: 0 \leq f \leq F_\epsilon$. Пропускная способность ищется следующим образом:

$$C = \frac{1}{T_H} (H_d(y) - H(y/x))_{\max},$$

где T_H - длительность реализации случайных процессов $x(t), y(t)$. Вместо одного отсчета рассмотрим выборку $\vec{y}_n = (y_1, \dots, y_n), \vec{x}_n = (x_1, \dots, x_n)$, объем выборки $n = 2F_\epsilon T_H$, т.к. $n = \frac{T_H}{\Delta t}, \Delta t = \frac{1}{2F_\epsilon} \Rightarrow n = 2F_\epsilon T_H$. Тогда

$$H_d(\vec{y}_n) = \sum_{k=1}^n H_d(y_k) = \sum_{k=1}^n \frac{1}{2} \log_2(2\pi e \sigma_y^2) = \frac{n}{2} \log_2(2\pi e \sigma_y^2) = \frac{2F_\epsilon T_H}{2} \log_2(2\pi e \sigma_y^2) = F_\epsilon T_H \log_2(2\pi e \sigma_y^2) = H_{d \max}(\vec{y}_n)$$

Причем, $\sigma_y^2 = \sigma_x^2 + \sigma_\mu^2$. В результате имеем $H_{\max}(\vec{y}_n) = F_\epsilon T_H \log_2(2\pi e(\sigma_x^2 + \sigma_\mu^2))$.

Далее с учетом формулы (5.8) запишем:

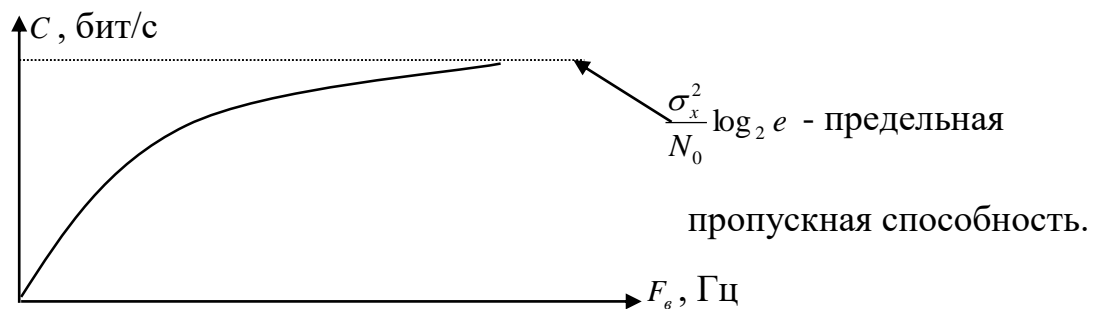
$$H(\vec{y}_n / \vec{x}_n) = H_d(\vec{y}_n - \vec{x}_n) = H_d(\vec{\mu}_n) = \sum_{k=1}^n H_d(\mu_k) = \sum_{k=1}^n \frac{1}{2} \log_2(2\pi e \sigma_\mu^2) = \frac{n}{2} \log_2(2\pi e \sigma_\mu^2) = F_\epsilon T_H \log_2(2\pi e \sigma_\mu^2)$$

Тогда пропускная способность гауссовского канала связи равна

$$C = \frac{F_{\epsilon} T_H}{T_H} (\log_2(2\pi e(\sigma_x^2 + \sigma_{\mu}^2)) - \log_2(2\pi e\sigma_{\mu}^2)) = F_{\epsilon} \log_2\left(\frac{\sigma_x^2 + \sigma_{\mu}^2}{\sigma_{\mu}^2}\right) = F_{\epsilon} \log_2(1 + q),$$

где $q = \frac{\sigma_x^2}{\sigma_{\mu}^2} = \frac{\sigma_x^2}{F_{\epsilon} N_0}$ - отношение сигнал/шум, N_0 - односторонняя СПМ белого гауссовского шума.

$$C = F_{\epsilon} \log_2\left(1 + \frac{\sigma_x^2}{F_{\epsilon} N_0}\right) \quad (5.10)$$



Таким образом, пропускная способность ГКС растет с увеличением ширины полосы канала и стремится к предельному значению $\frac{\sigma_x^2}{N_0} \log_2 e$.

6. Помехоустойчивое кодирование.

Для увеличения помехоустойчивости приема (уменьшения вероятности ошибки) применяют канальное (помехоустойчивое) кодирование. Оно позволяет обнаружить и исправить ошибки в приемнике, тем самым уменьшая вероятность ошибки приема символа.

6.1. Линейные блочные коды.

Блочный код состоит из набора векторов фиксированной длины, которые называются **кодовыми словами**. Длина кодового слова – число элементов в векторах, обозначим ее буквой n . Элементы кодового слова выбираются из алфавита с q элементами. Если $q = 2$, тогда код называют двоичным. Если $q > 2$, то код недвоичный. Если же $q = 2^b$, где b - целое положительное число, то каждый элемент имеет эквивалентное двоичное представление, состоящее из b битов. Т.е. недвоичный код длины N можно представить двоичным кодом длиной $n = bN$.

Кодовое слово длины n содержит $k < n$ информационных символов. Код обозначается как (n, k) - код, а отношение

$$R_c = \frac{k}{n} \quad (6.1)$$

называется **скоростью кода**. Величина $1 - R_c$ - **избыточность**.

Блок из k информационных бит отображается в кодовое слово длины n , выбираемое из набора $M = 2^k$ кодовых слов. Каждое кодовое слово состоит из k информационных бит и $n - k$ проверочных.

Вес кода $w_i (i = 1, 2, \dots, M)$ – число ненулевых элементов слова, является одной из важных характеристик кода. Для двоичных кодов вес - это количество единиц в кодовом слове. Каждое кодовое слово имеет свой вес. Набор всех весов кода $\{w_i\}$ образует **распределение весов кода**. Если все M кодовых слов имеют одинаковый вес, тогда код называется кодом с **постоянным весом**.

Функции кодирования и декодирования включают арифметические операции сложения и умножения, выполненные над кодовыми словами. Эти операции соответствуют соотношениям и правилам для алгебраического поля с q элементами. Если $q = 2$, то имеем символы $\{0, 1\}$. В общем поле F состоит из q элементов $\{0, 1, \dots, q-1\}$. Операции сложения и умножения удовлетворяют следующим аксиомам.

Сложение.

1. Поле F замкнуто относительно сложения: если $a, b \in F$, то $a + b \in F$.
2. Ассоциативность: если $a, b, c \in F$, то $a + (b + c) = (a + b) + c$.
3. Коммутативность: $a, b \in F \Rightarrow a + b = b + a$.
4. Поле F содержит **нулевой элемент** 0 такой, что $a + 0 = a$.
5. Каждый элемент поля F имеет свой **отрицательный элемент**, т.е., если $b \in F \Rightarrow -b \in F$ его отрицательный элемент. Вычитание $a - b$ определено как $a + (-b)$.

Умножение.

1. Поле F замкнуто относительно умножения: если $a, b \in F$, то $ab \in F$.
2. Ассоциативность: если $a, b, c \in F$, то $a(bc) = (ab)c$.
3. Коммутативность: $a, b \in F \Rightarrow ab = ba$.
4. Поле F содержит **единичный элемент** 1 такой, что $a \cdot 1 = a$.
5. Каждый элемент поля F , исключая нулевой элемент, имеет **обратный**. Если $b \in F, b \neq 0 \Rightarrow b^{-1}$ его обратный элемент и $b \cdot b^{-1} = 1$. Деление $\frac{a}{b}$ определено как ab^{-1} .

Из курса «Математики» хорошо известны поля вещественных и комплексных чисел. Эти поля имеют бесконечное число элементов. Поля, из которых строятся коды, имеют ограниченное число элементов.

Ограниченное поле с q элементами называют полем Галуа и обозначают $GF(q)$. Операции сложения и умножения осуществляются по модулю q

$(\text{mod } q)$.

Пример 1. $GF(2)$

+	0	1
0	0	1
1	1	0
•	0	1
0	0	0
1	0	1

Пример 2. $GF(5)$.

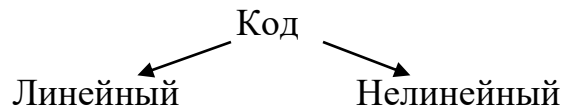
+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

•	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Если $q = p^m$, где p, m - целые положительные числа, то поле $GF(p)$ можно расширить до $GF(p^m)$. Операции сложения и умножения проводятся по модулю $p, (\text{mod } p)$.

Пусть C_i и C_j - два кодовых слова в (n, k) кодовом блоке. Мера разницы между C_i, C_j - число позиций, в которых они различаются. Эта мера называется **расстоянием Хемминга** и обозначается $d_{i,j}$, причем $0 < d_{i,j} \leq n, i \neq j$. Минимальное кодовое расстояние определяется следующим образом:

$$d_{\min} = \min_{i,j=1,2,\dots,M} \{d_{i,j}\} \quad (6.2)$$



Рассмотрим два кодовых слова C_i, C_j и скалярные величины α_1, α_2 . Код называется линейным, если $\alpha_1 C_i + \alpha_2 C_j$ тоже является кодовым словом из (n, k) блока. Значит, линейный код должен содержать кодовое слово, состоящее из одних нулей. Поэтому код с постоянным весом – нелинейный. Пусть C_i – линейный двоичный блочный код, $i = 1, 2, \dots, M$. $C_1 = (0 \dots 0)_{1 \times n}$ – кодовое слово из нулей, w_i – вес i -го кодового слова. Тогда w_i – расстояние Хемминга между C_i и C_1 . В результате имеем:

$$d_{\min} = \min_{i \neq 1} \{w_i\}, \quad (6.3)$$

так как $d_{i,j}$ равно весу разности $C_i - C_j$, а разность эквивалентна сумме по модулю 2, но $C_i - C_j$ – тоже кодовое слово с весом, включенным в набор $\{w_i\}$.

6.1.1. Порождающая и проверочная матрица.

Пусть $X_i = (x_{i1}, x_{i2}, \dots, x_{ik})_{1 \times k}$ – вектор из k информационных бит, $C_i = (c_{i1}, c_{i2}, \dots, c_{in})_{1 \times n}$ – вектор помехоустойчивого кода. Тогда

$$C_i = X_i G \quad (6.4)$$

$G_{k \times n}$ – порождающая матрица кода.

$$G = \begin{pmatrix} g_{11} & g_{12} & \dots & g_{1n} \\ \vdots & \vdots & \vdots & \vdots \\ g_{k1} & g_{k2} & \dots & g_{kn} \end{pmatrix} = \begin{pmatrix} \vec{g}_1 \\ \vdots \\ \vec{g}_k \end{pmatrix}. \text{ Если выражение (6.4) раскрыть, то}$$

$$C_i = (x_{i1} \quad \dots \quad x_{ik}) \begin{pmatrix} \vec{g}_1 \\ \vdots \\ \vec{g}_k \end{pmatrix} = x_{i1} \vec{g}_1 + \dots + x_{ik} \vec{g}_k, \text{ т.е. произвольное кодовое слово –}$$

линейная комбинация векторов $\{\vec{g}_l\}, l = 1, 2, \dots, k$ из порождающей матрицы G . Вектора $\{\vec{g}_l\}$ должны быть **линейно независимыми**.

Система векторов $\{\vec{g}_l\}$ называется линейно зависимой, если хотя бы один из этих векторов является линейной комбинацией остальных векторов и линейно независимой в противном случае.

Любую порождающую матрицу $G(n, k)$ - кода путем проведения операций над строками и столбцами можно свести к **систематической** форме:

$$G = \begin{pmatrix} I_{k \times k} & P_{k \times (n-k)} \end{pmatrix}, \quad (6.5)$$

где $I_{k \times k}$ - единичная матрица размерностью $k \times k$, $P_{k \times (n-k)}$ - матрица дополнение, которая определяет $n - k$ избыточных (проверочных) символов. Тогда по формуле (6.4) получим **систематический код**, у которого первые k бит информационные, остальные $n - k$ проверочные.

Для декодирования используется проверочная матрица $H_{(n-k) \times n}$, причем,

$$\begin{aligned} C_i H^T &= 0_{1 \times (n-k)}, \\ GH^T &= 0_{k \times (n-k)}. \end{aligned} \quad (6.6)$$

Если линейный двоичный (n, k) код систематический, то проверочная матрица имеет вид:

$$H = \begin{pmatrix} P^T & I_{(n-k) \times (n-k)} \end{pmatrix} \quad (6.7)$$

Коды Хемминга.

Двоичные коды Хемминга: $(n, k) = (2^m - 1, 2^m - 1 - m)$, где m - целое положительное число. Если $m = 3$, то получим $(7, 4)$ код. $n = 2^m - 1$ столбцов матрицы H состоят из всех возможных двоичных векторов с $n - k = m$ элементами, исключая нулевой вектор.

Пример. Рассмотрим систематический $(7, 4)$ код Хемминга с проверочной

матрицей $H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}_{3 \times 7}$. Здесь $P^T = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}_{3 \times 4}$ -

транспонированная матрица дополнение. Тогда порождающая матрица имеет

вид: $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}_{4 \times 7}$. Пусть $X_i = (x_{i1}, x_{i2}, x_{i3}, x_{i4})$ информационное

словое, которое поступает на вход кодера. Далее по формуле (6.4) получим помехоустойчивое словое:

$$C_i = (x_{i1}, x_{i2}, x_{i3}, x_{i4}) \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (c_{i1}, c_{i2}, c_{i3}, c_{i4}, c_{i5}, c_{i6}, c_{i7}),$$

ГДЕ $c_{i1} = x_{i1}, c_{i2} = x_{i2}, c_{i3} = x_{i3}, c_{i4} = x_{i4}, c_{i5} = x_{i1} \oplus x_{i2} \oplus x_{i3}, c_{i6} = x_{i2} \oplus x_{i3} \oplus x_{i4}, c_{i7} = x_{i1} \oplus x_{i2} \oplus x_{i4}.$

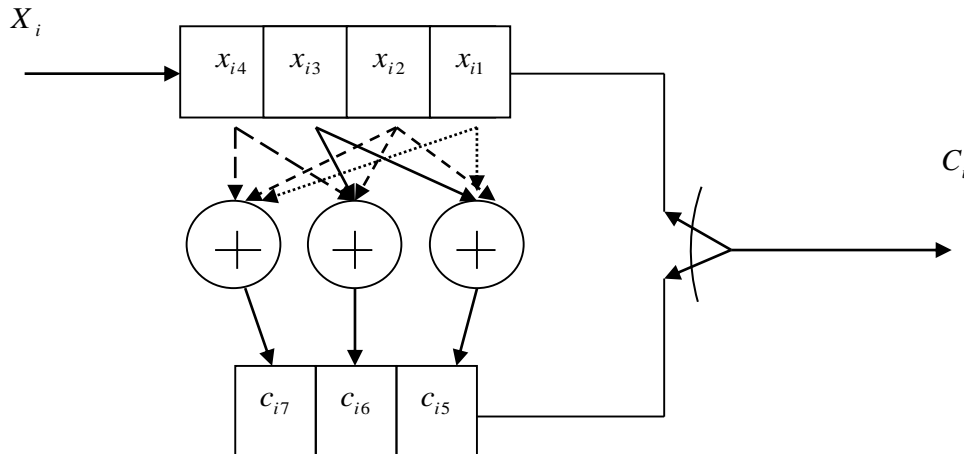


Рисунок 6.1. Кодер систематического кода (7,4).

Кодер использует 4 –х битовый и 3-х битовый регистр сдвига, а также 3 сумматора по модулю 2.

Замечание. При $m > 1$ для (n, k) кода Хемминга $d_{\min} = 3$.

6.1.2. Оптимальное декодирование линейных блочных кодов.

Блочный (n, k) код способен обнаружить $d_{\min} - 1$ ошибку и исправить $\left\lfloor \frac{1}{2}(d_{\min} - 1) \right\rfloor$ ошибок, где $\lfloor \bullet \rfloor$ - наибольшее целое, содержащееся в аргументе.

Пусть C_i - переданное кодовое слово, $Y = C_i + e$ - принятое кодовое слово, где e - вектор ошибок. Тогда

$$YH^T = (C_i + e)H^T = C_iH^T + eH^T = eH^T = S, \text{ т.к. } C_iH^T = 0_{1 \times (n-k)}.$$

Произведение

$$YH^T = eH^T = S \quad (6.8)$$

называется **синдромом**. S - характеристика образцов ошибок. Существует 2^n возможных образцов ошибок, но только 2^{n-k} синдромных. Следовательно, разные образцы ошибок приводят к одинаковым синдромам.

Для декодирования составляется таблица размером $2^k \times 2^{n-k}$ которая называется стандартным расположением для заданного кода.

C_1	C_2	C_3	\dots	C_{2^k}
e_2	$C_2 + e_2$	$C_3 + e_2$	\dots	$C_{2^k} + e_2$
e_3	$C_2 + e_3$	$C_3 + e_3$	\dots	$C_{2^k} + e_3$
\vdots	\vdots	\vdots	\vdots	\vdots
$e_{2^{n-k}}$	$C_2 + e_{2^{n-k}}$	$C_3 + e_{2^{n-k}}$	\dots	$C_{2^k} + e_{2^{n-k}}$

Первый столбец – образцы ошибок, первая строка – все возможные кодовые слова, начиная с кодового слова, состоящего из одних нулей. Каждую строку называют **смежным классом**, а первый столбец – **лидеры смежных классов**. Таким образом, смежный класс состоит из всевозможных принимаемых кодовых слов, получающегося от частного образца ошибки (лидера смежного класса).

Пример. Задан код (5,2) с порождающей матрицей $G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$.

Тогда $2^k = 2^2 = 4$, $2^{n-k} = 2^{5-2} = 8$, проверочная матрица $H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$.

Стандартное расположение (таблица декодирования):

Таблица 1.

$X_1 = (00)$	$X_2 = (01)$	$X_3 = (10)$	$X_4 = (11)$
00000	01011	10101	11110
00001	01010	10100	11111
00010	01001	10111	11100
00100	01111	10001	11010
01000	00011	11101	10110
10000	11011	00101	01110
11000	10011	01101	00110
10010	11001	00111	01100

Образцы ошибок с весом 2 были выбраны так, чтобы соответствующие ей синдромы отличались от тех, которые соответствуют одиночным ошибкам.

Для заданного кода минимальное кодовое расстояние $d_{\min} = 3$. Его можно определить по формуле (6.3) для разрешенных кодовых комбинаций (первая строка таблицы 1), исключая из рассмотрения нулевое кодовое слово.

Таблица 2.

e_i	S_i
00000	000
00001	001
00010	010
00100	100
01000	011
10000	101
11000	110
10010	111

Пусть принято кодовое слово Y . Находим синдром $S = YH^T$, далее выбираем соответствующий этому синдрому наиболее правдоподобный вектор ошибки \hat{e} (по таблице 2). Тогда оценка передаваемого кодового слова

$$\hat{C} = Y \oplus \hat{e} \quad (6.9)$$

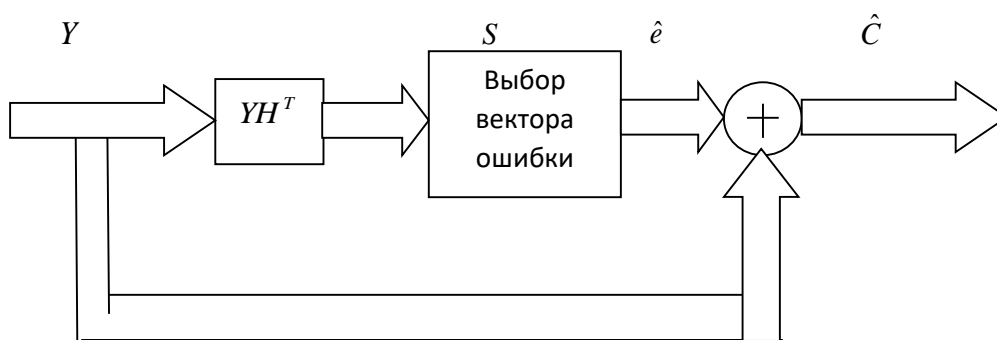


Рисунок 6.2. Структурная схема декодера.

Данный код может обнаружить 2 ($d_{\min} - 1 = 3 - 1 = 2$) ошибки, исправить все одиночные ошибки ($\left\lfloor \frac{1}{2}(d_{\min} - 1) \right\rfloor = 1$) и только 2 двойные, синдромы которых отличаются от синдромов одиночных ошибок. Подтвердим сказанное на примере.

Пусть принимаемое кодовое слово $Y = (11111)$, где $C_i = (01011) = C_2, e = (10100)$.

Тогда $S = (11111) \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (001)$. Полученному синдрому соответствует вектор

ошибки $\hat{e} = (00001) = e_1$. По (6.9) находим оценку переданного кодового слова $\hat{C} = (11111) \oplus (00001) = (11110) = C_4 \neq C_2$. Т.е. получаем ошибку декодирования.

Вывод. Алгоритм (6.9) работает по критерию максимального правдоподобия (МП) или по критерию минимального расстояния. Он

обеспечивает минимальную вероятность ошибки декодирования в двоичном симметричном канале связи.