ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Теорема Шеннона для дискретного канала с шумом

Методика построения помехоустойчивых кодов

Линейные блочные коды

Код Хэмминга

Расширенный код Хэмминга

Циклические коды

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Задача согласования дискретного источника с дискретным каналом с шумом

X – ансамбль сигналов на входе, Y – ансамбль сигналов на выходе. При наличии шума канал описывается выражением:

$$I(X,Y) = H(X) - H(X|Y)$$

Переходя к характеристикам в единицу времени:

$$I'(X,Y) = H'(X) - H'(X|Y)$$

Пусть C – пропускная способность канала (максимальная скорость передачи информации) без шума. Имеется некоторый дискретный источник информации с производительностью $[H'(U)=I'(X,Y)]<C$. Тогда

$$H'(U) = H'(X) - H'(X|Y)$$

откуда: $H'(X) = [\ H'(U) + H'(X|Y)\ ] > H'(U)$

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Теорема Шеннона для дискретного канала с шумом

Если производительность источника сообщений $H'(U)$ меньше пропускной способности канала C, т.е. $H'(U)<C$, то существует такая система кодирования, которая обеспечивает возможность передачи сообщений источника со сколь угодно малой вероятностью ошибки (или со сколь угодно малой ненадежностью).

Если $H'(U)>C$, то можно закодировать сообщение таким образом, что потери информации в единицу времени не будут превышать величину $H'(U)-C+\varepsilon$, где ε - сколь угодно мало.

Не существует способа кодирования, обеспечивающего потери в канале, меньшие, чем $H'(U)-C$.

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Алгебраическое основы операций кодирования и декодирования

Функции кодирования и декодирования включают арифметические операции суммирования и умножения, выполняемые над кодовыми словами. Эти арифметические операции выполняются в соответствии с правилами для алгебраического поля, которое имеет своими элементами символы, содержащиеся в алфавите кода (обычно 0 и 1, т.е. $q=2$).

Такие поля с ограниченным числом элементом q называются полями Галуа, например GF(q). Операции суммирования и умножения над элементами их GF(q) осуществляются по модулю q и обозначаются как (mod q).

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Методика построения помехоустойчивых кодов. Модели ошибок

В каждом разряде вектора ошибки единица появляется с вероятностью *P* независимо от того, какие значения получили остальные разряды вектора ошибки.

Этой гипотезе наиболее соответствует биномиальный закон распределения кратности ошибки, в соответствии с которым вероятностью того, что при передаче по дискретному каналу в кодовой комбинации бинарного кода длины *n* возникнет ошибка кратности *q* равна:

$$P_{n,k} = C_n^q P^q (1-P)^{n-q}$$

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Методика построения помехоустойчивых кодов. Характеристики кодов

Коэффициент повышения верности $K_{пв}$ при использовании помехоустойчивого кода определяется как отношение вероятности появления ошибочных кодовых комбинаций на выходе дискретного канала к вероятности появления необнаруженных ошибок.

Блочные коды образуются в результате отождествления каждого состояния источника в процессе кодирования с определенным кодовым словом (блоком, кодовой комбинацией).

Непрерывные коды представляют собой последовательность кодовых символов, не разделяемую на последовательность кодовых блоков.

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Методика построения помехоустойчивых кодов. Характеристики кодов

Избыточные блочные коды (длины $n = k+r$):

- разделимые (систематические) - в каждой кодовой комбинации можно отделить информационные (k) и проверочные (r) разряды;

- неразделимые (несистематические) - все разряды равноправные и в кодовой комбинации нельзя отделить информационные и проверочные разряды.

Расстояние между двумя векторами кодового пространства по Хэммингу равно весу разности векторов. Минимальное расстояние между любыми двумя векторами кодового пространства называется кодовым расстоянием набора кодовых векторов (d_{min}). Корректирующий код обозначается либо как (n,k), либо как (n,k,$d_{\min}$).

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Методика построения помехоустойчивых кодов. Характеристики кодов

Для *обнаружения* всех ошибок кратности, не превышающей q_{max}, кодовое расстояние должно быть не менее

$$d_{min} = q_{max} + 1.$$

Для обеспечения возможности *исправления* ошибок кратности не более q_{max}, кодовое расстояние должно быть не менее

$$d_{min} = 2q_{max} + 1.$$

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Методика построения помехоустойчивых кодов. Оптимальные помехоустойчивые коды

Верхняя граница кодового расстояния d_{min} при заданных основании кода m, числе элементов кода n и числе информационных символов k (граница Плоткина, для m=2):

$$d_{\min} \le \frac{n * 2^{k-1}}{2^k - 1}$$

Граница Варшамова-Гилберта дает нижнюю границу для числа избыточных символов r, необходимых для обеспечения кодового расстояния d_{min} (для m=2):

$$2^r \ge 1 + \sum_{i=1}^{d_{\min}-2} C_{n-1}^{i}$$

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Линейные блочные коды. Порождающая и проверочная матрицы

Пусть x_1, x_2, ..., x_k означают слово из k информационных битов на входе кодера, кодируемое в кодовое слово C размерности n битов:

вход кодера: $X=[x1, x2, ..., xk]$

выход кодера: $C=[c1, c2, ..., cn]$

Пусть задана специальная порождающая матрица $G_{n,k}$, задающая блочный код (n,k).

Строки матрицы $G_{n,k}$ должны быть линейно независимы.

$$G_{n,k} = \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{bmatrix} = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{bmatrix}$$

Тогда разрешенная кодовая комбинация C, соответствующая кодируемому слову X:

$$C=x_1g_1 + x_2g_2 + ... + x_kg_k.$$

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Линейные блочные коды. Порождающая и проверочная матрицы

Систематическая (каноническая) форма порождающей матрицы *G* размером *k*x*n* :

$$G_{n,k} = [I_k \; P] = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & p_{11} & p_{12} & \cdots & p_{1r} \\ 0 & 1 & 0 & \cdots & 0 & p_{21} & p_{22} & \cdots & p_{2r} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & p_{k1} & p_{k2} & \cdots & p_{kr} \end{bmatrix}$$

Порождающая матрица систематического кода создает линейный блочный код, в котором первые *k* битов любого кодового слова идентичны информационным битам, а остальные *r=n-k* битов любого кодового слова являются линейными комбинациями *k* информационных битов.

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Линейные блочные коды. Синдром ошибки

Проверочная матрица $H_{n,k}$ имеет rxn элементов, причем справедливо:

$$C \times H^T = 0.$$

Это выражение используется для проверки полученной кодовой комбинации. Если равенство нулю не выполняется, то получаем матрицу-строку $||c_1, c_2, ..., c_r||$, называемую синдромом ошибки.

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Линейные блочные коды. Порождающая и проверочная матрицы

Матрицу $H_{n,k}$ можно определить как:

$$H_{n,k} = \left[-P^T \; I_{n-k} \right]$$

Отрицательный знак можно опустить, поскольку при работе с двоичными кодами вычитание по модулю 2 идентично сложению по модулю 2:

$$H_{n,k} = \left[P^T \; I_{n-k} \right] = \begin{bmatrix} p_{11} & p_{21} & \cdots & p_{k1} & 1 & 0 & \cdots & 0 \\ p_{12} & p_{22} & \cdots & p_{k2} & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ p_{1r} & p_{2r} & \cdots & p_{kr} & 0 & 0 & \cdots & 1 \end{bmatrix}$$

На практике обычно используются три типа линейных блочных кодов: код Хэмминга, код Адамара и код Голея.

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Код Хэмминга (для $d_{min}=3$)

Число разрешенных кодовых комбинаций для n-разрядных ($n=k+r$) кодовых слов:

$$2^n/(n+1)$$

Число информационных разрядов k и размер кодового слова n

$$k = \log_2(2^n/(n+1)] = n - \log_2(n+1)$$

Целочисленные решения (n,k): (3,1); (7,4); (15,11)....

Два взаимоисключающих режима работы:

- режим обнаружения ошибок кратности q<=2;
- режим исправления ошибок кратности q=1

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Код Хэмминга. Проверочная и порождающая матрицы

Особенность проверочной матрицы кода Хэмминга:

для двоичного (n,k)-кода $n=2^w-1$ столбцов состоят из всех возможных двоичных векторов с r=n-k элементами, исключая вектор со всеми нулевыми элементами.

$$H_{7,4} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Порождающая матрица:

$$G_{7,4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Расширенный код Хэмминга

Кодовые вектора дополняются двоичным разрядом так, чтобы число единиц, содержащихся в каждом кодовом слове, было четным.

Преимущества:

- длины кодов = 2^w;

- d_{min}=4 (обнаружение ошибок кратности q=3, коррекция ошибок кратности q=1);

- гибридный режим работы декодера: обнаружение (q=2) и коррекция (q=1) ошибок.

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Расширенный код Хэмминга

Проверочная матрица H $(2^w,k)$-кода получается из проверочной матрицы $(2^w-1,k)$-кода:

- к матрице $(2^w-1,k)$-кода дописывается нулевой столбец;
- полученная матрица дополняется строкой, полностью состоящей из одних единиц.

Синдром ошибки (в гибридном режиме):

При одиночной ошибке s'(r) = 1. По значению синдрома (младшие (r-1) битов) находим и исправляем ошибочный бит.

При двойной ошибке компонента s'(r) = 0, а синдром отличен от нуля. Ситуация обнаруживается, но не исправляется.

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Циклические коды

Циклические коды являются подмножеством линейных кодов и обладают свойствами, упрощающими процессы их кодирования и декодирования.

Разрешенные кодовые комбинации формируются из других разрешенных слов циклическим сдвигом символов.

Процедуры кодирования и декодирования сводятся к операциям умножения и деления степенных полиномов, легко реализуемых технически.

Представление кодовых слов в виде многочлена идентично линейному векторному пространству кодовых векторов. Степени используются только для обозначения места компоненты в регистре сдвига

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Циклические коды

Кодовое слово ***v***, состоящее из n битов, определяется полиномом

$$v(X) = v_0 + v_1x + v_2x^2 + \ldots + v_{n-1}x^{n-1} = v_{n-1}x^{n-1} + v_2x^2 + v_1x + v_0.$$

В полиномиальном представлении циклический сдвиг на один разряд влево (обозначается как $v^1(X)$) соответствует умножению на x по модулю (x^n+1) и обозначается как:

$$v^1(X) = x \cdot v(X) \bmod (x^n+1).$$

Многочлен, соответствующий i-кратному циклическому сдвигу вектора ***v***, можно получить как остаток от деления многочлена $x^i \cdot v(X)$ на (x^n+1). Это свойство циклического кода используется для обнаружения ошибок при декодировании.

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Циклические коды. Порождающий многочлен

Порождающий многочлен – неприводимый ненулевой многочлен (или произведение неприводимых многочленов) степени $r=n-k$, у которого свободный член обязательно равен единице :

$$g(X) = x^{n-k} + g_{n-k-1}x^{n-k-1} + g_1 x + 1.$$

Порождающий многочлен циклического кода является множителем (x^n+1), т.е.

$$(x^n+1) = g(X)\cdot h(X)$$

Для формирования кодового слова каждое информационное слово (многочлен степени не выше k) умножается на порождающий многочлен степени r (в результате получается многочлен степени не выше $n = k+r$):

$$v(X) = a(X)\cdot g(X)$$

или

$$v(X) = a_{k-1}x^{k-1}g(X) + \ldots + a_2x^2g(X) + a_1xg(X) + a_0g(X).$$

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Циклические коды. Проверочный многочлен

Проверочный многочлен циклического кода является множителем (x^n+1), т.е.

$$h(X) = (x^n+1) / g(X).$$

Кодовые комбинации циклического кода удовлетворяют условиям:

- без остатка делятся на порождающий многочлен $g(X)$;
- при умножении на проверочный полином $h(X)$ дают 0 по модулю (x^n+1).

Старшая степень порождающего многочлена определяет число контрольных символов в кодовом слове.

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Циклические коды. Пример

Пример циклического кода (7,4) с порождающим многочленом $g(X) = (x^3 + x + 1)$ (код не является систематическим!):

Информ. слово (4 бита)	**Многочлен**	**Кодовое слово (7 битов)**
0000	$0 \cdot g(X)$	0000000 (0)
0001	$1 \cdot g(X) = x^3 + x + 1$	0001011 (3)
0010	$x \cdot g(X) = x^4 + x^2 + x$	0010110 (3)
0011	$[x + 1] \cdot g(X) = x^4 + x^3 + x^2 + 1$	0011101 (4)
0100	$x^2 \cdot g(X) = x^5 + x^3 + x^2$	0101100 (3)
0101	$[x^2 + 1] \cdot g(X) = x^5 + x^2 + x + 1$	0100111 (4)
0110	$[x^2 + x] \cdot g(X) = x^5 + x^4 + x^3 + 1$	0111010 (4)
0111	$[x^2 + x + 1] \cdot g(X) = x^5 + x^4 + 1$	0110001 (3)
1000	$x^3 \cdot g(X) = x^6 + x^4 + x^3$	1011000 (3)
1001	$[x^3 + 1] \cdot g(X) = x^6 + x^4 + x + 1$	1010011 (4)
1010	$[x^3 + x] \cdot g(X) = x^6 + x^3 + x^2 + x$	1001110 (4)
1011	$[x^3 + x + 1] \cdot g(X) = x^6 + x^2 + 1$	1000101 (3)
1100	$[x^3 + x^2] \cdot g(X) = x^6 + x^5 + x^4 + x^2$	1110100 (4)
1101	$[x^3 + x^2 + 1] \cdot g(X) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$	1111111 (7)
1110	$[x^3 + x^2 + x] \cdot g(X) = x^6 + x^5 + x$	1100010 (3)
1111	$[x^3 + x^2 + x + 1] \cdot g(X) = x^6 + x^5 + x^3 + 1$	1101001 (4)

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Циклические коды. Порождающая матрица

Каждое кодовое слово может быть представлен в виде произведения $v(X) = a(X) \cdot g(X)$:

$$v(X) = a_{k-1}x^{k-1}g(X) + \ldots + a_2x^2g(X) + a_1xg(X) + a_0g(X),$$

где каждое слагаемое представляет собой сдвиг порождающего многочлена $g(X)$, которому соответствует вектор $\boldsymbol{g} = (1, g_{r-1}, \ldots, g_1, 1)$.

Кодовый вектор $\boldsymbol{v}$, соответствующий многочлену $v(X)$, может быть представлен в виде произведения информационного вектора $\boldsymbol{a}$ на порождающую матрицу $\boldsymbol{G}$ вида:

$$G_{kxn} = \begin{pmatrix} 1 & g_{r-1} & g_{r-2} & \cdots & g_1 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & g_{r-1} & \cdots & g_2 & g_1 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & g_{r-1} & \cdots & g_2 & g_1 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & g_{r-1} & g_{r-2} & \cdots & g_1 & 1 \end{pmatrix} = \begin{pmatrix} a_{k-1}x^{k-1}g(X) \\ \cdots \\ \cdots \\ \cdots \\ a_0g(X) \end{pmatrix}$$

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Циклические коды. Проверочная матрица

Для получения проверочной матрицы используется утверждение, что порождающий многочлен $g(X)$ делит (x^n+1) без остатка:

$$x^n + 1 = g(X) \cdot h(X).$$

Многочлен $h(X)$ степени $k=n-r$ называется *проверочным многочленом*.

Уравнение синдромного декодирования: $v \cdot H^T = 0$,

где

$$H_{n,k} = \begin{pmatrix} h_0 & h_1 & h_2 & \cdots & h_{k-1} & h_k & 0 & 0 & 0 & 0 \\ 0 & h_0 & h_1 & h_2 & \cdots & h_{k-1} & h_k & 0 & 0 & 0 \\ 0 & 0 & h_0 & h_1 & \cdots & h_{k-2} & h_{k-1} & h_k & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & 0 & \cdots & h_0 & h_1 & h_2 & \cdots & h_{k-1} & h_k \end{pmatrix}$$

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Систематические циклические коды.

Рассмотрим информационный многочлен степени k-1:

$$a(X) = a_{k-1}x^{k-1} + \ldots + a_1x + a_0$$

и его $r=n-k$ кратный сдвиг:

$$x^r \cdot a(X) = a_{k-1}x^{n-1} + \ldots + a_1x^{r+1} + a_0x^r.$$

Представим многочлен $x^r \cdot a(X)$ в виде:

$$x^r \cdot a(X) = a(X) \cdot g(X) + b(X),$$

где $b(X)$ – остаток от деления $x^r \cdot a(X)$ на $g(X)$. Отсюда следует:

$$x^r \cdot a(X) + b(X) = a(X) \cdot g(X)$$

Алгоритм кодирования систематического цикл. (n,k)-кода:

1) информационный многочлен $a(X)$ степени k-1 умножается на x^r, где $r=n-k$;

2) находится остаток $b(X)$ от деления $x^r \cdot a(X)$ на $g(X)$;

3) многочлен $b(X)$ степени r заносится в r младших разрядов кодового слова. Получаем: $v(X) = x^r \cdot a(X) + [x^r \cdot a(X) \bmod g(X)]$

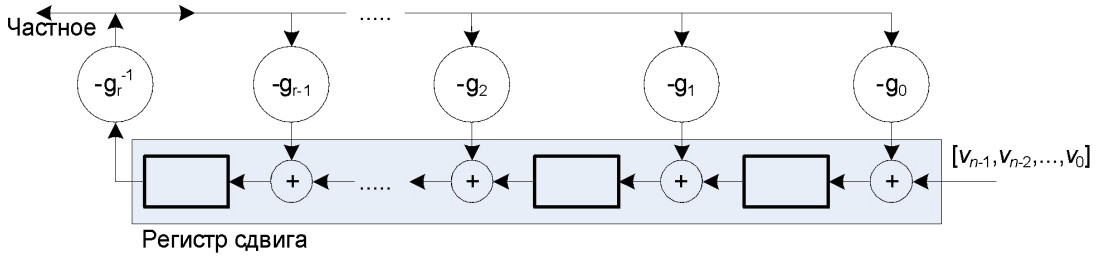
ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Деление многочленов с использованием регистра сдвига

При кодировании систематическим кодом *операция деления* выполняется для вычисления остатка при делении на порождающий многочлен в процессе формирования кодового слова.

При декодировании *операция деления* полученного кодового слова на порождающий многочлен позволяет получить остаток, являющийся синдромом ошибки (если он не равен нулю, то имела место ошибка при передаче).

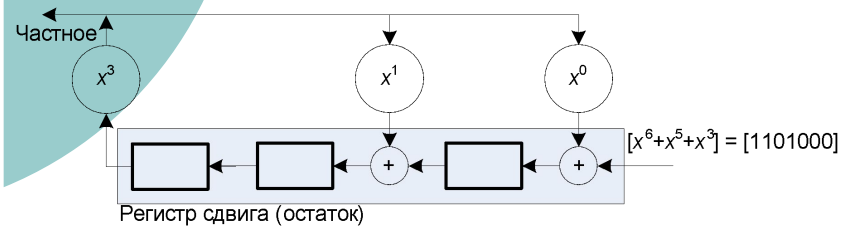
В общем виде схем реализации деления (по алгоритму Евклида) имеет вид:



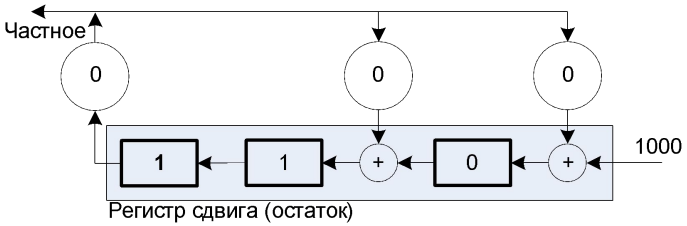
ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Деление многочленов с использованием регистра сдвига. Пример

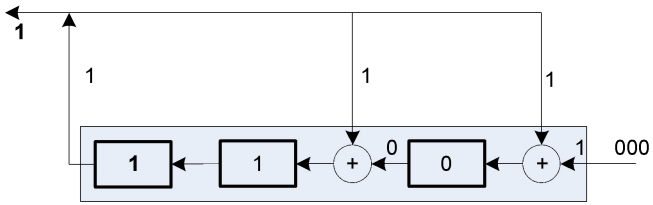
Разделить многочлен $x^6 + x^5 + x^3$ (степень равна n=6) на $x^3 + x + 1$ (степень многочлена равна r=3)

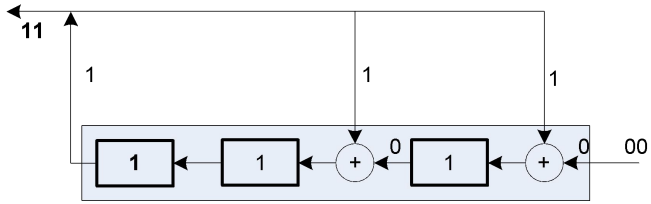


Структура связей

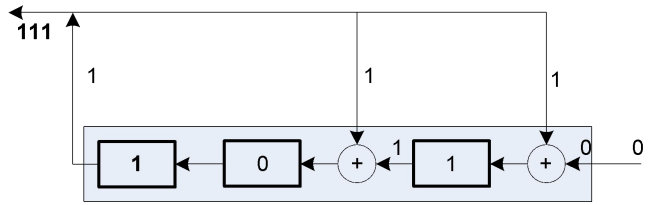


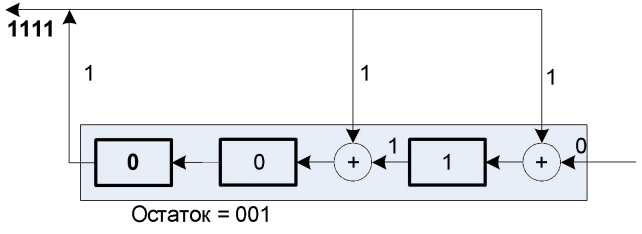
Начальное состояние





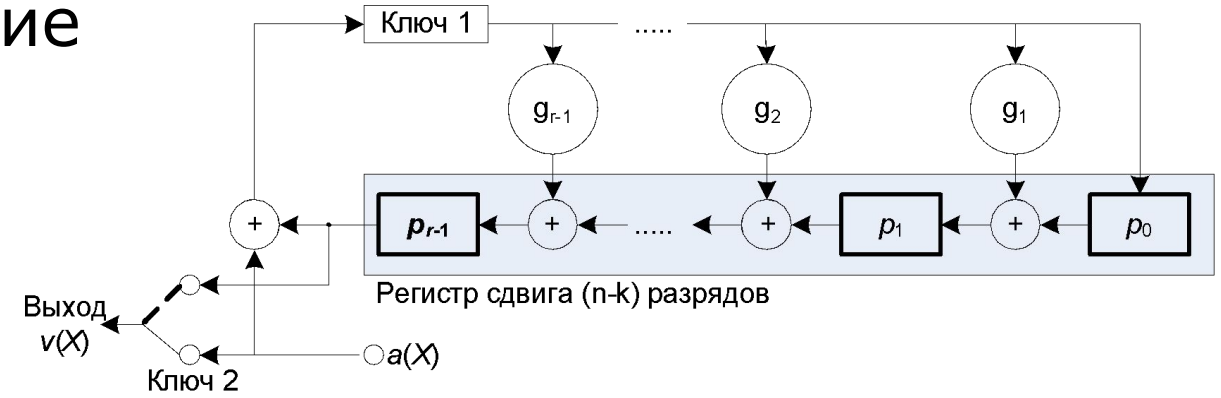
Ответ:
частное: x^3+x^2+x+1
остаток: 1





ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Систематические циклические коды. Кодирование



Для систематического кодирования необходимо реализовать деление смещенного влево (вверх) полиномиального сообщения $x^r \cdot a(X)$ на порождающий многочлен $g(X)$.

1) При первых k сдвигах ключ № 1 открыт для передачи битов сообщения в n-k разрядный регистр сдвига. Ключ № 2 установлен в нижнее положение: идет вывод в кодовое слово k информационных символов;

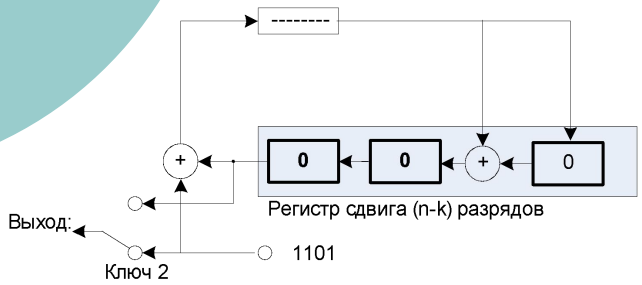
2) После передачи k-го бита сообщения ключ № 1 открывается, а ключ № 2 переходит в верхнее положение;

3) При остальных $r=n-k$ сдвигах происходит работа с регистров сдвига: проверочные биты поочередно выдвигаются в выходной регистр (кодовое слово).

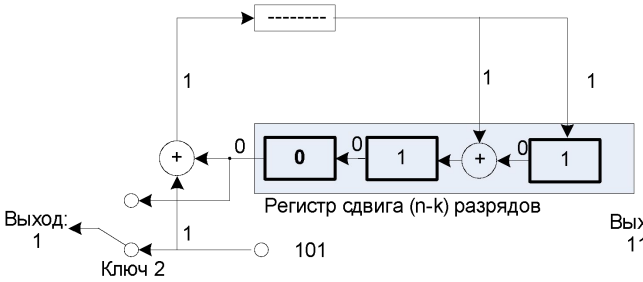
ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

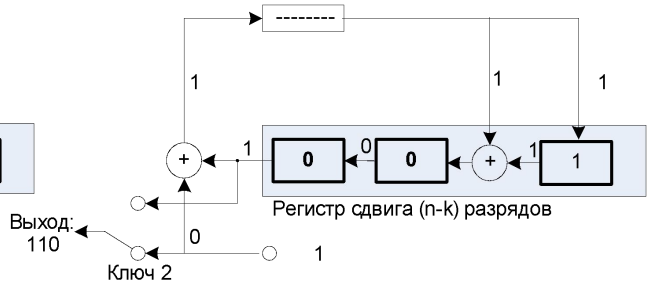
Систематические циклические коды. Кодирование. Пример

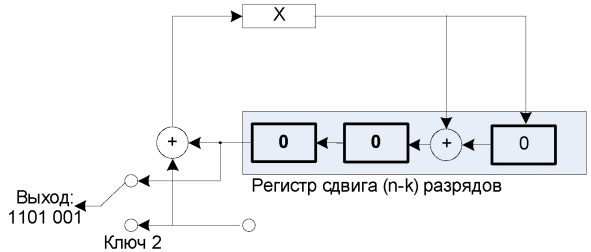
Вычислить кодовое слово систематического циклического (7,4)-кода для информационного многочлена $a(X) = x^3 + x^2 + 1 = 1101$ (порождающий многочлен $g(X) = (x^3 + x + 1)$).



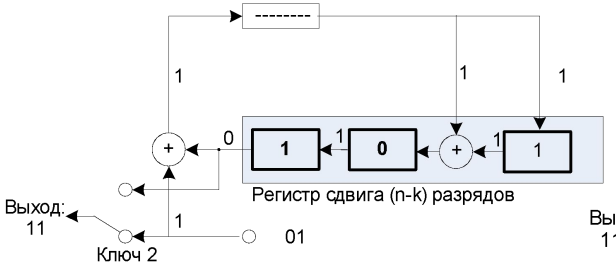
Начальное состояние

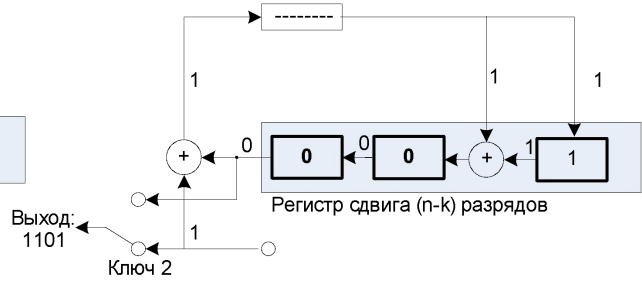






Смена состояния ключей. После $n=7$ сдвигов





Первые $k=4$ сдвигов

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Систематические циклические коды. Декодирование. Синдром ошибки

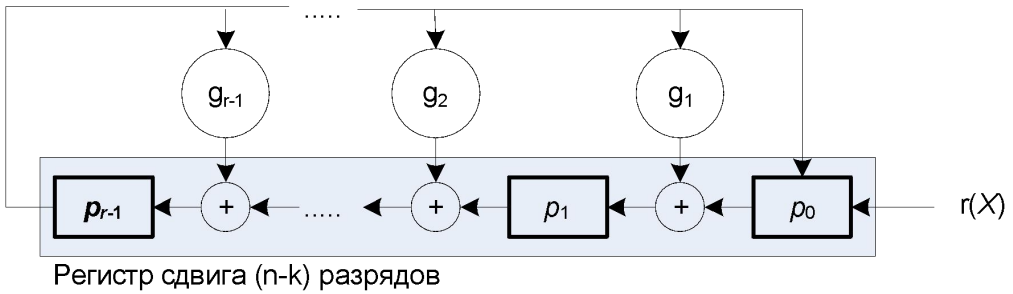
При передачи данных по каналу связи с шумом к кодовому слову v(X) добавляется многочлен ошибок e(X). В результате многочлен принятого кодового слова имеет вид:

$$r(X) = v(X) + e(X) \quad \text{или} \quad r(X) = a(X) \cdot g(X) + s(X),$$

где $s(X)$ – синдром ошибки (полином степени $r=n-k$).

Если $r(X)$ – кодовый многочлен, то $s(X)$ – нулевой многочлен (отсутствие ошибки или необнаруживаемая ошибка).

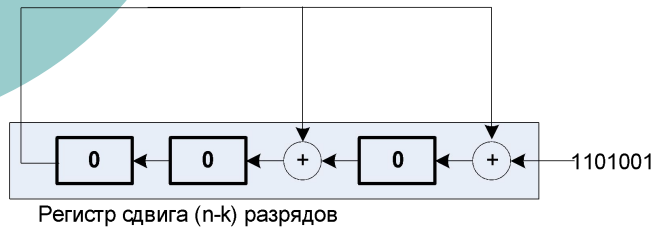
Синдром $s(X)$ есть остаток от деления принятого кодового слова $r(X)$ на порождающий многочлен $g(X)$.



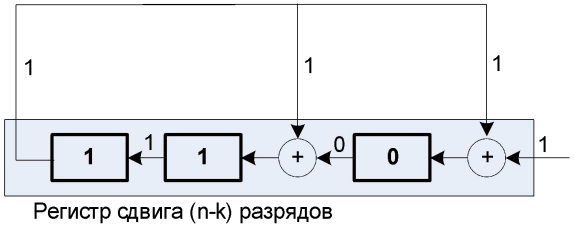
ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Систематические циклические коды. Декодирование. Пример-1

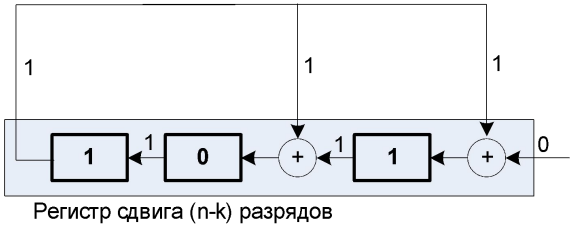
Вычислить синдром для полученного кодового слова v(X) = 1101001, соответствующего информационному слову 1101 для циклического (7,4)-кода с порождающим многочленом $g(X) = (x^3 + x + 1)$.



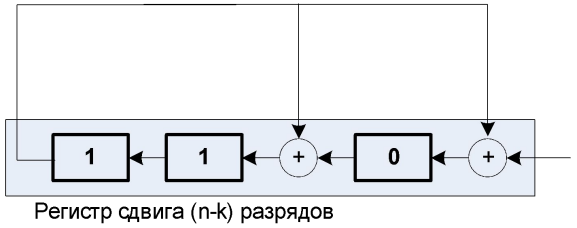
1101001



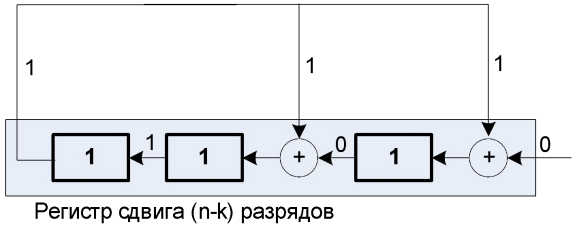
001



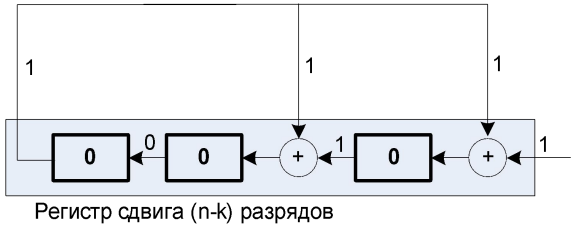
Начальное состояние



1001



01



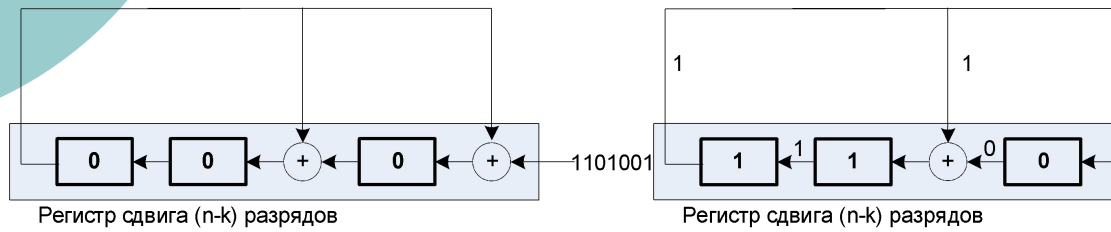
После первых r=3 сдвигов (заполнения регистра сдвига)

Синдром после n сдвигов (=0)

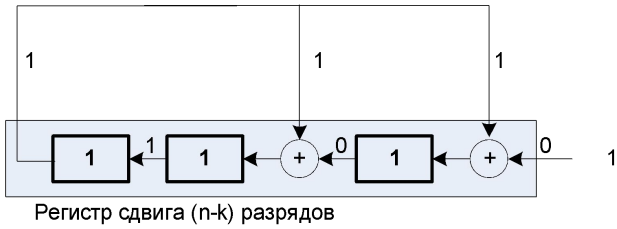
ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

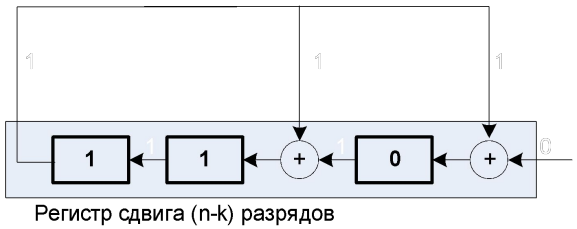
Систематические циклические коды. Декодирование. Пример-2

Вычислить синдром для полученного кодового слова v(X) = 1101**1**01, соответствующего информационному слову 1101 для циклического (7,4)-кода с порождающим многочленом $g(X) = (x^3 + x + 1)$.

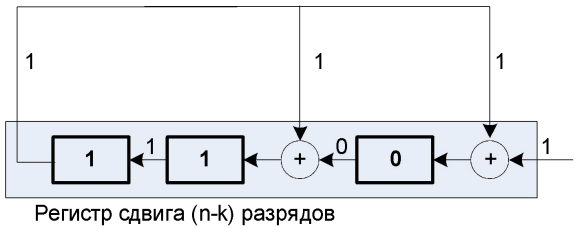


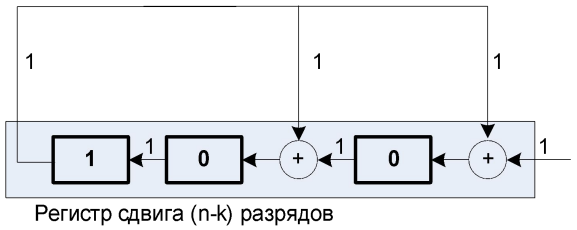
Начальное состояние





После первых r=3 сдвигов (заполнения регистра сдвига)





Синдром после n сдвигов (=100)

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Систематические циклические коды. Декодирование. Исправление ошибки

Возьмем в качестве отправной точки синдром ошибки для какого-либо известного бита (по приведенному выше примеру синдром для ошибки в бите № 2 равен 100) и отключим входной регистр в приведенной выше схеме. Продолжая выполнять циклические сдвиги регистра, будем последовательно получать синдромы для ошибок в бите № 3, 4, ..., 6, 0, 1.

Номер бита	**Синдром**
2	**100**
3	011
4	110
5	111
6	101
0	001
1	010

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Дополнительные возможности циклических кодов

Особенность циклических кодов - способность к распознаванию пакетов ошибок (группы последовательных ошибок), в том числе концевых (зацикленных).

Пакет ошибок длины равной, или меньшей r всегда распознается (обнаруживается). (Если длина пакета ошибок не превосходит $r=n-k$, то степень многочлена ошибок меньше k. В этом случае $e(X)$ не делится на $g(X)$ без остатка и синдром принятого слова всегда отличен от нуля).

Варианты циклических кодов для систем связи: код Боуза-Чоудхури-Хоквенгема, код Рида-Соломона и др.

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Выполнение лабораторной работы № 3. Вариант моделирования шума в канале связи

Для генерации битов ошибки можно использовать СВ, имеющую смысл «Интервал между искаженными битами».

Для генерации нормальной СВ *y* (М-матожидание, σ - СКО) на основе равномерно распределенной СВ с выборкой R_i размером n отсчетов можно использовать алгоритм:

$$y = M + \frac{\sigma}{\sqrt{n/12}}\left[\sum_{i=1}^{n} R_i - \frac{n}{2}\right]$$

M соответствует среднему интервалу между искажаемыми битами, σ – разбросу интервала относительно среднего значения (максимальный разброс не превышает 3*σ).

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ СООБЩЕНИЙ

Выполнение лабораторной работы № 3. Пример анализа работы помехоустойчивого кодека

Код: XXXXX (n,k, d_{min})

Параметры шума (интервал между искаженными битами): M, σ

Режим: обнаружение ошибок

Кодер		**Канал связи**		**Декодер**				
Размер информ. сообщения (байтов)	Количество кодовых слов	Кратность ошибки	Число кодовых слов с ошибкой	Результаты декодирования кодовых слов				Количество информ. байтов сообщения, передача которых не состоялась из-за обнаруженной ошибки
				Число кодовых слов с обнаруженными ошибками всего	Число кодовых слов с верно обнаруженными ошибками	Число кодовых слов с неверно обнаруженными ошибками	Число кодовых слов с необнаруженными ошибками при их наличии	
??	??	0 1 2 …	xx xx xx …	xx xx xx …	?? ?? ?? ..	?? ?? ?? ..	?? ?? ?? ..	??