ЛЕКЦИЯ 5. СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ С ПРИМЕНЕНИЕМ ПОМЕХОУСТОЙЧИВЫХ КОДОВ, ОБНАРУЖИВАЮЩИХ ОШИБКИ

3.1.3. Алгоритмы обнаружения ошибок двоичными (*n*,*k*)-кодами с CRC и ненулевыми состояниями ячеек регистров.

Как и в предыдущем случае, (*n*,*k*)-коды с ненулевыми начальными состояниями ячеек регистра сдвига могут быть как с "простой", так и с расширенной CRC. В приведенных ниже вариантах таких кодов во всех ячейках регистра деления в начальном состоянии установлены "1".

Рассмотрим алгоритмы кодирования и декодирования систематических (*n*,*k*)-кодов с расширенной CRC-m и ненулевыми (единичными) состояниями ячеек регистров деления кодера и декодера

Процедура кодирования:

Шаг 1). Процесс кодирования исходной информационной комбинации в виде многочлена φ(x) начинается с умножения этой исходной комбинации на x^{n-k}.

Шаг 2). Одновременно с началом процесса кодирования во все (n – k) = m ячеек регистра деления на многочлен G(x), как стартовые состояния, записываются ”1”, т. е. в регистре кодера будет установлен многочлен

$$L(x) = 1 + x + x^2 + x^3 + \ldots + x^{n-k-1}.$$

Таким образом, этим двум первым шагам будет соответствовать добавление к старшим разрядам информационной комбинации φ(x) единичной комбинации, соответствующей многочлену L(x), т. е.

Шаг 3). Далее последовательно с подачей на вход кодера информационной комбинации, начиная со старшего разряда, происходит потактовое деление суммы $\varphi(x)\cdot x^{n-k} + x^k L(x)$ на образующий многочлен $G(x)$, в результате чего, после окончания поступления на вход информационных элементов, в ячейках регистра будут получены проверочные элементы

$r(x) = r_0 + r_1 x + \ldots + r_{n-k-1} x^{n-k-1}$,

при этом будет справедливо следующее сравнение:

$$\varphi(x)\cdot x^{n-k} + x^k L(x) \equiv r(x) \pmod{G(x)}. \qquad (1.18)$$

При этом информационные элементы также последовательно поступали на выход кодера, что соответствует построению систематического (n,k)-кода.

Шаг 4). После окончания поступления на вход кодера информационных элементов с ячеек регистра деления последовательно через инвертор считывается остаток от деления $r(x)$, т.е. многочлен $\overline{r(x)}$.

Шаг 5). Проверочные элементы инвертированного остатка добавляются к информационным элементам со стороны младших разрядов и в канал отправляется кодовая комбинация

$$f(x) = \overline{r(x)} + \varphi(x)\cdot x^{n-k}. \qquad (1.19)$$

Процедура декодирования.

Рассмотрим в общем виде процедуру декодирования принятой комбинации $h(x) = f(x) + e(x)$ по шагам в предположении, что ошибки в ней отсутствуют, т.е. $e(x) = 0$ и $h(x) = f(x)$.

Шаг 1). Перед началом поступления на вход декодера принимаемой комбинации в ячейках регистра деления на образующий многочлен $G(x)$ устанавливается стартовая комбинация из всех «1», т.е. параллельным кодом записывается многочлен $L(x) = 1 + x + x^2 + x^3 + \ldots + x^{n-k-1}$. Относительно поступающей комбинации $h(x) = f(x)$ эти $(n - k)$ единиц займут k старших разрядов в n-элементной комбинации, т.е. это будет многочлен $x^k L(x)$.

Шаг 2). После этого начинает поступать комбинация $h(x) = f(x)$ на умножитель на x^{n-k}, суммируясь при этом с последовательными элементами, поступающими с выхода регистра деления, т.е. с многочленом $x^k L(x)$.

Таким образом, пока на вход декодера потактово поступает кодовая комбинация $f(x)$, начиная со старшего разряда при x^{n-1}, происходит деление суммы $x^{n-k}[f(x) + x^k L(x)]$ на образующий многочлен $G(x)$.

Шаг 3). После окончания поступления кодовой комбинации в ячейках регистра деления будет содержаться определённый ненулевой синдром $S_0(x)$.

В результате деления будут происходить следующие преобразования:

$$x^{n-k}[f(x)+x^k L(x)] = x^{n-k}[x^{n-k}\varphi(x)+\overline{r(x)}+x^k L(x)] = x^{n-k}[x^{n-k}\varphi(x)+r(x)+L(x)+x^k L(x)].$$

Подставив в последнее выражение вместо *r*(*x*) выражение (1.18), получим:

$$x^{n-k}L(x) \equiv S_{\text{o}}(x) \pmod{G(x)}. \qquad (1.20)$$

ПРИМЕР 1. (Из черновиков к лекции)
«Простая» CRC-3. $P(x)= 1+x^2+x^3$.

$$\varphi(x) = x + x^2. \qquad \overline{r(x)} = 1. \qquad f(x) = 1 + x^4 + x^5.$$

$$S_0(x) = 1.$$

Рассмотренные варианты кодов можно отнести к псевдоциклическим.
Приведем обоснования.

Во-первых, такой систематический код не удовлетворяет **свойству линейности**, т.е. сумма двух или большего четного числа разрешённых кодовых комбинаций не образует некоторую другую разрешённую кодовую комбинацию. Рассмотрим это на примере двух разрешённых комбинаций $f_1(x)$ и $f_2(x)$, которые, в соответствии с (1.19), имеют вид:

$f_1(x) = \overline{r_1(x)} + \varphi_1(x) \cdot xn - k$; $\quad f_2(x) = \overline{r_2(x)} + \varphi_2(x) \cdot xn - k$.

$$\overline{r_1(x)} = r_1(x) + L(x) \quad \text{и} \quad \overline{r_2(x)} = r_2(x) + L(x),$$

$$\text{где} \quad r_1(x) \equiv x^{n-k}\varphi_1(x) + x^k L(x) \quad \text{и} \quad r_2(x) \equiv x^{n-k}\varphi_2(x) + x^k L(x).$$

Подставив $\overline{r_1(x)}, r_1(x), \overline{r_2(x)}, r_2(x)$ в выражения для разрешённых кодовых комбинаций $f_1(x)$ и $f_2(x)$, получим следующую сумму:

$$h(x) = f_1(x) + f_2(x) = x^{n-k}\varphi_1(x) + r_1(x) + \cancel{L(x)} + x^{n-k}\varphi_2(x) + r_2(x) + \cancel{L(x)} =$$

$$= \cancel{x^{n-k}\varphi_1(x)} + \cancel{x^{n-k}\varphi_1(x)} + \cancel{x^k L(x)} + \cancel{x^{n-k}\varphi_2(x)} + \cancel{x^{n-k}\varphi_2(x)} + \cancel{x^k L(x)} = 0.$$

Таким образом, сумма двух разрешённых комбинаций не является также разрешённой комбинацией, так как среди множества разрешённых комбинаций нулевая отсутствует. Значит, код не удовлетворяет свойству линейности, которое характерно для классических циклических кодов.

Во-вторых, покажем, что также **не работает свойство циклического сдвига**, порождающего новую разрешённую комбинацию для классического циклического кода.

Пусть имеется разрешённая кодовая комбинация $f(x)$, при декодировании которой получен заранее известный синдром $S_o(x)$ в соответствии с (1.20). Произведем теперь циклический сдвиг комбинации $f(x)$ на один шаг, в результате получим произведение x f(x), которое подвергнем декодированию по рассмотренному выше алгоритму:

$$x^{n-k}\left\{x\cdot f(x)+x^k L(x)\right\}=x^{n-k}\left\{x\left[x^{n-k}\cdot\varphi(x)+\overline{r(x)}\right]+x^k L(x)\right\}=x^{n-k}\left\{x\left[x^{n-k}\cdot\varphi(x)+r(x)+L(x)\right]+x^k L(x)\right\}=$$

$$=x^{n-k}\left\{x\left[\cancel{x^{n-k}\cdot\varphi(x)}+\cancel{x^{n-k}\cdot\varphi(x)}+x^k L(x)+L(x)\right]+x^k L(x)\right\}=x^{n-k}L(x)\left(x+x^k+x^{k+1}\right)\neq S_o(x)\quad\left[\mathrm{mod}\,G(x)\right].$$

Таким образом, циклический сдвиг разрешённой комбинации $f(x)$ на один шаг (умножение $f(x)$ на x) не порождает новую разрешённую комбинацию, т.е. при декодировании описанным выше алгоритмом синдром не равен $S_o(x)$.

Поэтому систематический (n,k)-код с расширенной CRC и ненулевыми начальными состояниями ячеек регистра деления не является в полном смысле циклическим и может быть назван как *псевдоциклический*.

Оценим вероятностные характеристики таких блочных систематических кодов с расширенной CRC и ненулевыми (единичными) начальными состояниями ячеек регистра деления на образующий многочлен *G(x)*.

Правильное декодирование будет происходить в случае отсутствия ошибок в принятой комбинации, состоящей из *n* элементов. Вероятность такого события в канале ДСК будет определяться выражением:

$$P_{\text{пп}} = (1 - p_{\text{о}})^n,$$

где $p_{\text{о}}$ – вероятность ошибочного приема сигнального элемента в двоичном симметричном канале.

Определим ситуации, при **которых ошибки обнаруживаться не будут**. Пусть принимаемая комбинация, будет: $h(x) = f(x) + e(x)$, где $e(x)$ – многочлен ошибок. Процедура декодирования в математических операциях будет следующей:

$$x^{n-k}\left\{h(x)+x^k L(x)\right\} = x^{n-k}\left\{f(x)+e(x)+x^k L(x)\right\} = x^{n-k}\left\{x^{n-k}\cdot\varphi(x)+\overline{r(x)}+e(x)+x^k L(x)\right\} =$$

$$= x^{n-k}\left\{x^{n-k}\cdot\varphi(x)+r(x)+L(x)+e(x)+x^k L(x)\right\} =$$

$$= x^{n-k}\left\{\cancel{x^{n-k}\cdot\varphi(x)} + \cancel{x^{n-k}\cdot\varphi(x)} + L(x)+e(x)+\cancel{x^k L(x)} + \cancel{x^k L(x)}\right\} =$$

$$x^{n-k}\left[L(x)+e(x)\right] = x^{n-k}L(x)+x^{n-k}e(x) = S_{\text{о}}(x)+x^{n-k}e(x) \quad \left[\operatorname{mod} G(x)\right].$$

Из полученного выражения следует, что необнаруживаемыми ошибками будут такие, многочлены которых $x^{n-k}\,e(x)$ делятся на *G(x)* без остатка, т.е. $\boldsymbol{x^{n-k}\,e(x) \equiv 0 \quad [\mathrm{mod} G(x)].}$

Как и в предыдущем случае, (*n*,*k*)-коды с ненулевыми начальными состояниями ячеек регистра сдвига могут быть как с "простой", так и с расширенной CRC. В приведенных ниже вариантах таких кодов во всех ячейках регистра деления в начальном состоянии установлены "1".

3.1.3.1. Варианты систематических кодов с "простой" CRC с d_{min} =3 и ненулевыми начальными состояниями ячеек регистров деления на образующий многочлен P(x).

1). Широко применяемым таким кодом является код CRC-5 для USB с образующим многочленом $P(x) = 1 + x + x^5$.

2). Другим примером является код CRC-6 для перспективной технологии CDMA – 2000-A с образующим многочленом $P(x) = 1 + x + + x^2 + x^5 + x^6$.

3). В этой же технологии CDMA – 2000 применяется код с CRC-16 с образующим многочленом $P(x) = 1+x + x^2 + x^5 + x^6 + x^{11} + x^{14} +x^{15} + x^{16}$.

4). Во многих современных системах применяется код с "простой" CRC-32 с единичными начальными состояниями ячеек регистра образующего многочлена $P(x)$, имеющего вид в шестнадцатеричной форме записи $(104C11DB7)_{16}$ со старшим разрядом слева. Одним из них является код с CRC-32 для MPEG-2.

3.1.3.2. Варианты систематических кодов с расширенной CRC с d_{min} =4 и ненулевыми начальными состояниями ячеек регистров деления на образующий многочлен G(x).

1) Одним из примеров является код **CRC-6 для перспективной технологии CDMA – 2000-B** с образующим многочленом

$$G(x) = 1 + x + x^2 + x^6 = (1 + x)(1 + x^2 + x^3 + x^4 + x^5)$$

2) Аналогичным примером является код **CRC-8 для технологии CDMA – 2000** с образующим многочленом $G(x) = 1 + x + x^3 + x^4 + x^7 + x^8$.

3) Во многих современных системах применяется код с расширенной **CRC-16** с единичными начальными состояниями ячеек регистра образующего многочлена $G(x) = (1 + x)\,P(x)$, $P(x)$ – примитивный многочлен 15-ой степени. Наиболее популярным является код с расширенной **CRC-16** и образующим многочленом

$$G(x) = 1 + x^5 + x^{12} + x^{16},$$

применяемый в таких протоколах как X.25, HDLC, V.42, XMODEM, Bluetooth

Тогда, в соответствии с (1.20), синдром безошибочной комбинации $S_o(x)$ для такого кода будет иметь вид:

$$S_0(x) = x^{16}L(x) = x^{16}(1 + x + x^2 + \ldots + x^{15}) \equiv x^{12} + x^{11} + x^{10} + x^8 + x^3 + x^2 + x + 1 \,(\mathrm{mod}\, G(x)),$$

что в двоичной и в 16-ричной форме записи будет

$So = (0001110100001111)_2 = (1D0F)_{16}$.

Вид CRC	Порожд. многочлен	d_{min}	Начальное состояние	Синдром $S_0(x)$
CRC-1 «простое»	$P(x)= 1+x$	2 Обн. ош.неч.	нули	$S_0(x) = 0$
CRC-m «простое»	$P(x)$ степени m; примитивный	3 Обн. ошибки 1 и 2 кратн.	нули	$S_0(x) = (0\ldots0)$
Расширен. CRC-(m+1)	G(x)= (1+x)P(x); degP(x)=m; P(x) – примит.	4 Обн. все ош. нечет. + 2-х кр	нули	$S_0(x) = (0\ldots0)$
CRC-m «просте»	P(x) – примит. Степени m	3 $t_{oo} = 1,2$	Все «1»	$S_0(x) \neq 0$
CRC-(m+1)	G(x)= (1+x)P(x); degP(x)=m; P(x) – примит.	4 Обн. все ош. нечет. + 2-х кр	Все «1»	$S_0(x) \neq 0$