Лекция 6

Тема: Циклические коды

1. Общие положения о циклических кодах (ЦК). Способы построения ЦК
2. Матричное представление ЦК
3. Выбор образующего полинома. Построение проверочной матрицы ЦК
4. Коррекция ошибок
5. Необнаруживаемые ошибки
6. Укороченный ЦК
7. Примитивные многочлены
8. Коды БЧХ
9. Код Файра

Общие положения о циклических кодах

- Циклические коды (ЦК) относятся к классу систематических блочных кодов.

Основное свойство ЦК

- Если известна одна разрешенная кодовая комбинация ЦК, то другие комбинации можно получить циклическим сдвигом исходной комбинации справа налево*.

Общие положения о циклических кодах

Пример

Если разрешенной является комбинация 1011000, то можно записать ряд других разрешенных комбинаций ЦК

1011000 → 0110001 → 1100010 → 1000101 →

→ 0001011 → 00101100 → 0101100

Общие положения о циклических кодах

- ЦК обычно рассматривают в виде полиномов некоторой степени с фиктивной переменной

$$F(x) = \sum_{i=0}^{n-1} a_i x^i \qquad (1)$$

где коэффициенты a_i могут принимать значения 0 или 1.

Общие положения о циклических кодах

Пример

Комбинацию 01001 можно представить в виде полинома

$$F(x) = \underline{0} \cdot x^4 + \underline{1} \cdot x^3 + \underline{0} \cdot x^2 + \underline{0} \cdot x^1 + \underline{1} \cdot x^0 = x^3 + 1 \qquad (2)$$

Общие положения о циклических кодах

- Представление кодовых комбинаций в форме (1) позволяет свести действия над комбинациями к действиям над многочленами. При этом сложение двоичных многочленов сводится к сложению по mod2 коэффициентов при равных степенях переменной x. Умножение и деление производится по обычным правилам перемножения и деления степенных функций, однако операции сложения и вычитания (в процессе выполнения умножения и деления) заменяются операцией сложения по mod2.

Пример

Разложение полинома на сомножители

$$x^7+1=(x+1)(x^3+x+1)(x^3+x^2+1) \qquad (3)$$

$$
\begin{array}{l|l}
x^7+1 & x+1 \\ \cline{2-2}
\underline{x^7+x^6} & x^6+x^5+x^4+x^3+x^2+x^1+1 \\
\quad x^6+1 & \\
\quad \underline{x^6+x^5} & \\
\qquad x^5+1 & \\
\qquad \ldots \quad \underline{} & \\
\qquad\qquad x+1 & \\
\qquad\qquad \underline{x+1} & \\
\qquad\qquad\ 0 &
\end{array}
$$

Пример

$$
\begin{array}{l|l}
x^6+x^5+x^4+x^3+x^2+x^1+1 & x^3+x+1 \\ \cline{2-2}
\underline{x^6+x^4+x^3} & x^3+x^2+1 \\
\quad x^5+x^2+x+1 & \\
\quad \underline{x^5+x^3+x^2} & \\
\qquad x^3+x+1 & \\
\qquad \underline{x^3+x+1} & \\
\qquad\qquad 0 &
\end{array}
$$

Пример

Проверка

$$
\begin{array}{r}
x^3+x+1 \\
\times \qquad x+1 \\
\hline
x^3+x+1 \\
\oplus \quad x^4+x^2+x \qquad \\
\hline
x^4+x^3+x^2+1
\end{array}
\qquad\qquad
\begin{array}{r}
x^4+x^3+x^2+1 \\
\times \qquad x^3+x^2+1 \\
\hline
x^4+x^3+x^2+1 \\
\oplus \quad x^6+x^5+x^4+x^2 \qquad \\
x^7+x^6+x^5+x^3 \qquad\qquad \\
\hline
x^7+1 \qquad\qquad\qquad\qquad
\end{array}
$$

Общие положения о циклических кодах

- Комбинации ЦК можно представлять как в виде многочленов с фиктивной переменной, так и в виде двоичных выражений.
- Для построения ЦК (в качестве образующих полиномов) используют **неприводимые многочлены**.

Определение

- Неприводимым называется многочлен, который не м.б. представлен в виде произведения многочленов низших степеней.
- Т.е. неприводимый многочлен делится только на самого себя или на единицу и не делится ни на какой другой многочлен.

Общие положения о циклических кодах

- На неприводимый многочлен делится без остатка двучлен x^n+1
- Степень образующих полиномов совпадает с количеством проверочных символов кода.
- Если код представлен в виде многочлена с фиктивной переменной, то циклический сдвиг влево равносилен умножению полинома на x с последующим приведением результата по модулю x^n+1.

Пример

$x^5 x^4 x^3 x^2 x^1 x^0 \quad x^5 x^4 x^3 x^2 x^1 x^0$

$1\ 0\ 1\ 1\ 0\ 1 \rightarrow 0\ 1\ 1\ 0\ 1\ 1$

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

$$\oplus\ x^6+1$$

$$x^4+x^3+x+1$$

Способы построения ЦК

1-й способ – построение систематического ЦК

- Обозначим комбинацию простого k-значного двоичного кода $Q(x)$, а соответствующую ей комбинацию систематического ЦК $F_1(x)$.

  Тогда, для получения $F_1(x)$, необходимо

1. $Q(x)$ умножить на одночлен x^r, где r – степень образующего полинома $P(x)$;
2. $Q(x)\cdot x^r$ разделить на образующий полином. Получаем частное $C(x)$, которое имеет такую же степень, что и кодовая комбинация простого кода $Q(x)$* и остаток $R(x)$.
3. Остаток $R(x)$ сложить с $Q(x)\cdot x^r$,

т.е. $$F_1(x)= Q(x)\cdot x^r + R(x)$$

Способы построения ЦК

Вывод

- Степень остатка ($r-1$) не м.б. больше степени образующего полинома, т.е. наибольшее число разрядов остатка равно r.

Способы построения ЦК

Пример 1

- Пусть $k=4$ – число информационных разрядов;
- $P(x)=x^3+x+1$ – образующий полином, т.е. комбинация ЦК должна иметь 3 проверочных разряда ($r=3$);
- $Q(x)= x^3+x^2+1$
- Необходимо записать кодовую комбинацию систематического ЦК

Пример 1

- 1-й шаг

  $Q(x) \cdot x^3 = (x^3+x^2+1) \cdot x^3 = x^6+x^5+x^3$; $(1101 \to 1101000)$
- 2-й шаг

  $Q(x) \cdot x^3 / P(x) = (x^6+x^5+x^3)/(x^3+x+1) = (x^3+x^2+x+1) + 1$;
- 3-й шаг

$$F_1(x) = x^6+x^5+x^3+1$$

В двоичном представлении

$$1101 \to \underbrace{1101}_{\text{информационные разряды}}\underbrace{001}_{\text{проверочные разряды}} \qquad (4)$$

Способы построения ЦК

2-й способ – построение несистематического ЦК

- Обозначим комбинацию простого k-значного двоичного кода $Q(x)$, а соответствующую ей комбинацию несистематического ЦК $F_2(x)$.

  Для получения $F_2(x)$ необходимо $Q(x)$ умножить на образующий полином $P(x)$

$$F_2(x) = Q(x) \cdot P(x)$$

Способы построения ЦК

Пример 2

- Пусть $k=4$ – число информационных разрядов;
- $P(x)=x^3+x+1$ – образующий полином, т.е. комбинация ЦК должна иметь 3 проверочных разряда ($r=3$);
- $Q(x)= x^3+x^2+1$
- Необходимо записать кодовую комбинацию несистематического ЦК

Пример 2

- Т.к. $F_2(x) = Q(x) \cdot P(x)$, то

$$F_2(x)=x^6+x^5+x^4+x^3+x^2+x^1+1^*$$

- или в двоичном представлении

$$1101 \rightarrow 1111111 \qquad (5)$$

Выводы

1. Результаты кодирования информационной последовательности зависят от применяемого способа кодирования (см. кодовые слова (4) и (5)).
2. Первый способ дает четкое разделение информационных и проверочных символов в блоке.
3. Применение второго способа приводит к перемешиванию информационных и проверочных символов. Поэтому чаще применяют первый способ.

2. Матричное представление ЦК

- ЦК, как любой систематический код однозначно определяется k определенным образом подобранными кодовыми комбинациями. Эти комбинации записываются в виде образующей матрицы (ОМ), состоящей из k строк и n столбцов.

Матричное представление ЦК

- ОМ разбивается на две подматрицы

$$G_{k,n}=|E_k^T, C_{k,r}|,$$

где E_k^T - единичная транспонированная матрица,

$C_{k,r}$ – контрольная подматрица с числом строк k и столбцов r.

Контрольная подматрица образована остатками от деления $Q_i(x)\cdot x^r/P(x)$ $(i=1,2,\ldots,k)$, которые равны $R_i(x)$, где $Q_i(x)$ — комбинации двоичного k-значного кода, содержащие единицу только в одном из разрядов.

Матричное представление ЦК

- ОМ дает возможность получить первые k комбинаций кода. Остальные 2^k-k-1 комбинаций получаются суммированием по mod2 строк ОМ во всех возможных сочетаниях. Последняя комбинация является нулевой.

Матричное представление ЦК

Пример

- Пусть $P(x)=x^3+x+1$ или $P(1,0)=1011$; $n=7$, $k=4$.
- Построить ОМ.
- Т.к. $k=4$, то $Q_1(x)=0001$; $Q_2(x)=0010$; $Q_3(x)=0100$; $Q_4(x)=1000$.
- Возьмем комбинацию с единицей в старшем разряде, припишем к ней три нуля справа (умножим $Q_4(x)$ на x^3) и разделим на образующий полином. В процессе деления получим все возможные остатки для ОМ.

Пример

```
1000000 | 1011
1011    |------
-----   | 1011
 01100
  1011
  -----
   1110
   1011
   ----
    101
```

Получили остатки
R_1=011; R_2=110;
R_3=111; R_4=101

Пример*

$$G_{4,7} = \left| \underbrace{\begin{matrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{matrix}}_{E_k^T} \;\vdots\; \underbrace{\begin{matrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{matrix}}_{C_{k,r}} \right|$$

3.Выбор образующего полинома (ОП)

1. Выбор ОП при наличии в таблице нескольких полиномов одной степени производится по количеству остатков, которые дает этот полином. Обычно выбирается полином, который дает максимальное число остатков.
2. ОП должен входить в разложение двучлена x^n+1 (n-длина блока).

Выбор образующего полинома (ОП)

3. Не всякий многочлен степени r, входящий в разложение двучлена x^n+1 м.б. использован в качестве ОП. Необходимо, чтобы для каждой из ошибок обеспечивался свой уникальный остаток (от деления принятой комбинации на ОП). Это будет иметь место, если выбранный неприводимый многочлен степени r, являясь делителем двучлена x^n+1, не входит в разложение никакого другого двучлена x^l+1, степень которого меньше n ($l<n$).

Пример

- Образующий полином $x+1$ — неприводимый полином наименьшей степени, входящий в разложение двучлена x^n+1.
- Если $k=4$, то

$$E_4^T = \begin{vmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{vmatrix}, \quad (1)$$

$$C_{4,1} = \begin{vmatrix} 1 \\ 1 \\ 1 \\ 1 \end{vmatrix} \quad (2)$$

Пример

- Контрольная подматрица (2) содержит остатки от деления 10000* на x+1

```
1 0 0 0 0 | 1 1
1 1       |------
---       | 1 1 1
  1 0
  1 1
  ---
    1 0
    1 1
    ---
      1 0
      1 1
      ---
        1
```

Выбор образующего полинома (ОП)

- Боуз и Чоудхури показали, что для любых целых положительных чисел m и $t_и$ существует ЦК значности

$$n=2^m-1 \qquad (1)$$

с кодовым расстоянием

$$d_{min} \geq 2t_и+1 \qquad (2)$$

При этом число проверочных символов $r=n-k$ не превышает величины $mt_и$, т.е.

$$r \leq mt_и. \qquad (3)$$

Такой код гарантированно исправляет ошибки кратности $t_и$ и менее. Кроме того, код обнаруживает все пакеты ошибок, длина которых равна или меньше r.

Выбор образующего полинома (ОП)

- Максимальные значения k и n для различных m

m*	1	2	3	4	5	6	7	8	9	10
n	1	3	7	15	31	63	127	255	511	1023
k	0	1	4	11	26	57	120	247	502	1013

Построение проверочной матрицы ЦК

- Для построения проверочной матрицы (ПМ) используют проверочный полином степени k

$$h(x)=\frac{x^n+1}{P^{-1}(x)}=b_0+b_1x+\ldots+b_kx^k, \qquad (4)$$

где $P^{-1}(x)$ — полином обратный образующему полиному.

- Если записать обратный и образующий полиномы, в двоичной форме, то можно увидеть, что нули и единицы обратного полинома записываются в обратном порядке по сравнению с образующим полиномом.

Построение проверочной матрицы ЦК

Пример

- $P(x) \to 1011$; $P^{-1}(x) \to 1101$

Определение

- Обратными называются полиномы, которые образуются путем подстановки $1/x$ вместо x в основной полином и умножения этого полинома на одночлен x^m, где m – степень основного полинома.

Построение проверочной матрицы ЦК

- Проверочный полином, дополненный (r-1) нулями, образует первую строку ПМ. Все остальные (r-1) строк получаются циклическим сдвигом слева направо, т.е. от младших разрядов к старшим.

$$H_{r,n}=\begin{array}{l}
\overbrace{\hphantom{b_0\quad b_1\quad b_2\quad \dots\quad b_k}}^{k+1}\;\overbrace{\hphantom{0\quad \dots\quad 0\quad 0}}^{r-1}\\
\left|\begin{matrix}
b_0 & b_1 & b_2 & \dots & b_k & 0 & \dots & 0 & 0\\
0 & b_0 & b_1 & \dots & b_{k-1} & b_k & 0 & \dots & 0\\
0 & & \dots & 0 & b_0 & b_1 & b_2 & \dots & b_k
\end{matrix}\right|\\
\underbrace{\hphantom{0\quad b_0\quad \dots\quad 0}}_{r-1}
\end{array}$$

Построение проверочной матрицы ЦК

Пример

- Построить проверочную матрицу ЦК, если $n=7$, $k=4$, $r=3$. В качестве образующего и обратного ему полиномов даны

$$P(x)=1011;\ P^{-1}(x)=1101$$

Пример

- Запишем проверочный полином

$$h(x)=\frac{x^7+1}{x^3+x^2+1}=x^4+x^3+x^2+1$$

$$\begin{array}{l|l}
x^7+0+0+0+0+0+0+1 & x^3+x^2+0+1 \\
\underline{x^7+x^6+0+x^4} & \overline{1\cdot x^4+1\cdot x^3+1\cdot x^2+0+1} \\
\quad x^6+0+x^4+0 & \quad b_4 \quad\; b_3 \quad\; b_2 \quad\; b_1 \;\; b_0 \\
\quad \underline{x^6+x^5+0+x^3} & \\
\qquad x^5+x^4+x^3+0 & \\
\qquad \underline{x^5+x^4+0+x^2} & \\
\qquad\quad x^3+x^2+0+1 & \\
\qquad\quad \underline{x^3+x^2+0+1} & \\
\qquad\qquad 0 &
\end{array}$$

Пример

Запишем проверочную матрицу

$$
H = \begin{array}{c}
\begin{vmatrix}
1 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 1
\end{vmatrix} \\
\begin{matrix} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \end{matrix}
\end{array}
$$

$$
\left\{
\begin{array}{l}
a_0 = a_2 \oplus a_3 \oplus a_4 \\
a_1 = a_3 \oplus a_4 \oplus a_5 \\
a_6 = a_2 \oplus a_4 \oplus a_5
\end{array}
\right\}
$$

Вывод

- Свойства проверочных матриц ЦК такие же, как у всех систематических (групповых) кодов.

4. Коррекция ошибок

- Обнаружение и исправление ошибок производится на основе следующего свойства ЦК:

|| разрешенная комбинация делится без остатка на образующий полином.

Коррекция ошибок

Алгоритм обнаружения и исправления ошибочного разряда

1. Принятую комбинацию делят на образующий полином (ОП).
2. Подсчитывают количество единиц в остатке (определяют вес остатка w). Если $w \leq t_и$*, то принятую комбинацию складывают по mod2 с полученным остатком. Сумма дает исправленную комбинацию.

Коррекция ошибок

3. Если $w>t_и$, то производят циклический сдвиг принятой комбинации влево на один разряд. Полученную комбинацию делят на ОП. Если вес остатка $w \le t_и$, то делимое суммируют по mod2 с остатком.
4. Исправленную комбинацию сдвигают вправо на один разряд.

Коррекция ошибок

5. Если после первого циклического сдвига и последующего деления вес остатка $w>t_и$, то повторяют п.3 до тех пор, пока не будет достигнуто значение веса остатка $w \leq t_и$*. Полученную в результате последнего циклического сдвига комбинацию суммируют с остатком от её деления на ОП.

Коррекция ошибок

6. Производят циклический сдвиг вправо ровно на столько разрядов, на сколько сдвинута исправленная на предыдущем шаге комбинация относительно исходной (принятой). В результате получим разрешенную комбинацию, соответствующую переданной по КС.

Коррекция ошибок

Пример

- Пусть была передана комбинация 1001110 ЦК ($t_и=1$, $P(x)=x^3+x+1$).
- Принятая комбинация имеет вид 1000110, т.е. произошла ошибка в четвертом разряде.
- Показать процесс исправления ошибки.

Пример

1. Делим принятую комбинацию на ОП и
2. Сравниваем вес полученного остатка с числом исправляемых ошибок $t_и=1$

$$
\begin{array}{l|l}
1000110 & 1011 \\
\underline{1011} & \\
\quad 1111 & \\
\quad \underline{1011} & \\
\quad\; 1000 & \\
\quad\; \underline{1011} & \\
\qquad\; 11 & (w=2>1)
\end{array}
$$

Пример

3. Производим циклический сдвиг принятой комбинации на один разряд влево и деление на ОП

номер сдвига $\rightarrow$ 1)

$$
\begin{array}{r|l}
0001101 & 1011 \\
\underline{1011} & \\
110 & \\
\end{array}
$$

(w=2>1)

4. Повторяем п.3 до тех пор, пока не будет получено $w \le t_и$.

Пример

номер сдвига → 2)

```
0011010   |1011
  1011    |----
  ----
   1100
   1011
   ----
    111     (w=3>1)
```

номер сдвига → 3)

```
0110100   |1011
 1011     |----
 ----
  1100
  1011
   ----
   1110
   1011
   ----
    101     (w=2>1)
```

Пример

```
номер сдвига → 4) 1101000      |1011
                  1011          |------
                   1100
                   1011
                    1110
                    1011
                     1010
                     1011
                      001   (w=1)
```

Пример

5. Складываем по mod2 последнее делимое с последним остатком

$$
\begin{array}{r}
1101000 \\
\oplus \quad \underline{\qquad\quad 1} \\
1101001
\end{array}
$$

Пример

6. Исправленную комбинацию сдвигаем на 4 разряда вправо

1) 1110100;

2) 0111010;

3) 0011101;

4) **1001110**.

Видно, что последняя комбинация соответствует переданной, т.е. не содержит ошибок.

5. Необнаруживаемые ошибки

- ЦК обнаруживает не все ошибки, а их часть.
- Для определения доли необнаруживаемых и неисправляемых ошибок строят специальную матрицу М.
- М состоит из трех подматриц, расположенных определенным образом.

Структура матрицы M

кратность ошибок

$$M^{1}_{n,\,(2n-k)} = \left| \begin{matrix} E_n^T & \begin{matrix} E_r^T \\ \\ C_{k,r} \end{matrix} \end{matrix} \right| \tag{1}$$

число строк

число столбцов

Построение матрицы M

1. Записывают n векторов ошибок* в виде квадратной единичной транспонированной матрицы E_n^T размером $n \times n$.
2. К матрице ошибок E_n^T справа приписывается матрица остатков от деления одночлена ошибок x^i на ОП P(x) степени r. Матрица остатков содержит r столбцов и n строк.

Построение матрицы М

3. Матрица остатков м.б. разделена на две подматрицы. Первая подматрица является единичной транспонированной квадратной матрицей E_r^T размером $r \times r$. Остальные k строк приписанной матрицы остатков образуют вторую подматрицу остатков от деления одночлена ошибки x^i степени $i \geq (n-k)$ на ОП $P(x)$*.

Построение матрицы М

Вывод

Составленная таким образом матрица **М** отображает все варианты одиночных ошибок и остатки от деления кодовых комбинаций, содержащих указанные одиночные ошибки.

Пример

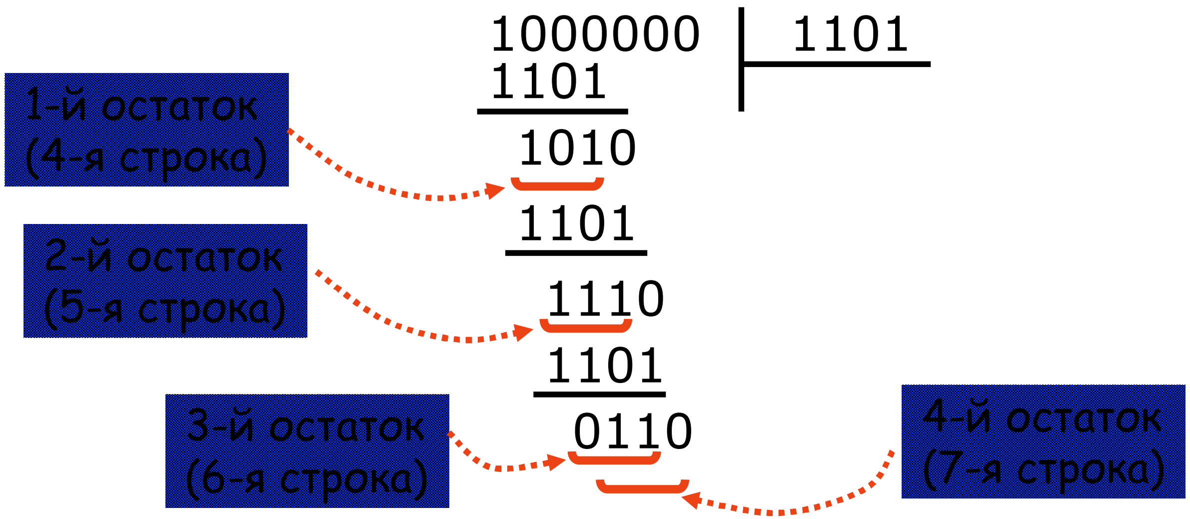
Построим матрицу $M^1_{7,10}$ для ЦК (4,7) с ОП $P(x)=x^3+x^2+1$

$$
\begin{array}{c|ccccccc|ccc|c}
 & x^6 & x^5 & x^4 & x^3 & x^2 & x^1 & x^0 & & & & \\
\hline
 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\
 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 2 \\
 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 3 \\
M_{7,10} = & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 4 \\
 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 5 \\
 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 6 \\
 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 7 \\
\hline
 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & e_3 & e_2 & e_1 &
\end{array}
\qquad (2)
$$

Пример

Получение подматрицы остатков

- Определим остатки для четвертой — седьмой строк матрицы (2).
- Разделим комбинацию 1000000 на ОП (1101)



Выводы

1. Первая подматрица имеет строки, которые являются векторами ошибок от первого до седьмого разрядов, а последние три столбца являются опознавателями ошибок. Столбцы матриц остатков обозначены e_1, e_2 и e_3. Т.к. все остатки для одиночных ошибок ненулевые, то данный код обнаруживает все одиночные ошибки.

Выводы

2. Данный код обнаруживает и все двойные ошибки. Чтобы в этом убедиться, достаточно сложить по mod2 любые две строки матрицы (2).

   Например, просуммируем первую и вторую строки.

$$\begin{array}{r} \oplus\begin{array}{l} 0000001\ \ 001 \\ \underline{0000010\ \ 010} \end{array} \\ 0000011\ \ 011 \end{array}$$

   Т.к. полученный остаток ненулевой, то это означает, что код обнаружит данную двукратную ошибку.

Выводы

3. Данный код обнаруживает часть трехкратных ошибок. Например, складывая первую, вторую и третью строки матрицы (2) получим ненулевой остаток.

ошибки (левая подматрица)	остатки (правая подматрица)
0000001	001
⊕ 0000010	010
0000100	100
0000111	111

Выводы

4. Часть трехкратных ошибок код не обнаруживает. Например, складывая первую, вторую и шестую строки матрицы (2) получим нулевой остаток.

ошибки (левая подматрица)	остатки (правая подматрица)
0000001	001
$\oplus$ 0000010	010
0100000	011
0100011	000

Выводы

- Рассматривая матрицу остатков, можно заметить, что нулевые остатки получаются при сложении одной строки остатка весом $w=2$ с двумя соответствующими строками остатков, имеющих вес $w=1$. Таких вариантов три: (1,2,6); (1,3,4); (2,3,7).
- Нулевые строки остатков получаются при суммировании элементов двух строк из нижней подматрицы с одной строкой из верхней подматрицы: (2,4,5); (3,5,6); (1,5,7).
- Еще один нулевой остаток получается при суммировании трех строк из нижней подматрицы: (4,6,7).

Выводы

1. Таким образом, из общего количества 35 тройных ошибок

$$C_7^3 = \frac{7 \cdot 6 \cdot 5}{1 \cdot 2 \cdot 3} = 35 \qquad (C_n^i = \frac{n!}{i!(n-i)!})$$

код не обнаруживает 7 вариантов, т.е. доля необнаруживаемых трехкратных ошибок составляет 20% (η=7/35=0,2).

3. Способ вычисления необнаруживаемых ошибок ЦК

- Для матрицы **М** больших размеров можно применить следующий способ вычисления необнаруживаемых ошибок.
- **1-шаг**

  Осуществляется полный перебор вариантов для ошибок минимальной кратности и строится таблица.

№	Номера строк, дающих в сумме нулевой остаток
1	1,2,6
2	1,3,4
3	2,3,7
4	2,4,5
5	3,5,6
6	1,5,7
7	4,6,7

Способ вычисления необнаруживаемых ошибок ЦК

- **2-шаг**

  Для определения необнаруживаемых ошибок более высокой кратности делаем перебор таблицы: попарно складываем по mod2 ее строки.

Например (а)

$\oplus$	(1)	1,2,6
	(2)	1,3,4
	(1,2)	2,3,4,6

	010
	100
$\oplus$	101
	011
	000

Способ вычисления необнаруживаемых ошибок ЦК

или (б)

$$
\oplus\begin{array}{ll}
(1) & 1,2,6 \\
(7) & 1,5,7 \\
\hline
(1,7) & 2,5,6,7
\end{array}
\qquad\qquad
\oplus\begin{array}{r}
010 \\
111 \\
011 \\
110 \\
\hline
000
\end{array}
$$

В результате получаем таблицу необнаруживаемых четырехкратных ошибок

Способ вычисления необнаруживаемых ошибок ЦК

№	№ строки
1,2	2,3,4,6
1,7	2,5,6,7
и т.д.	

Способ вычисления необнаруживаемых ошибок ЦК

Выводы

1. При передаче кодированных сообщений по КС необходимо принимать меры по устранению ошибок в тех разрядах, которые максимально часто встречаются в необнаруживаемых ошибках.
2. Обнаружение ошибок ЦК может осуществляться как для одиночных искажений, так и для пакетов ошибок, длина которых не превышает количества проверочных символов ($l \leq r$).

6. Укороченный ЦК

- В системах передачи данных с исправлением ошибок число информационных символов k_{Σ} обычно д.б. кратно длине первичного кода k_1:

$$k_{\Sigma}=ak_1 ,$$

где $a=1,2,\ldots,$ а значение $n_{\Sigma} = k_{\Sigma} + r$.

- Число проверочных символов r должно удовлетворять заданным $t_и$ и $t_о$.
- Например, ЭВМ обмениваются машинными словами в виде байтов (т.е. k_1=8). При этом n_{Σ} и k_{Σ} не совпадают с табулированными в ЦК.

Укороченный ЦК

- В этом случае по таблицам находят ЦК, соответствующий $r=n-k$ для классического ЦК, а затем уменьшают n_Σ и k_Σ до $n-l$ и $k_\Sigma=k-l$, получая укороченный ЦК (УЦК).

Правило построения УЦК

- УЦК ($n-l$, $k-l$) получают из полных ЦК, используя только кодовые комбинации, содержащие слева l нулей, т.е. УЦК можно получить вычеркиванием первых l столбцов и l строк из ОМ.

Укороченный ЦК

- Полученный код не будет строго циклическим, т.к. циклический сдвиг не всегда будет приводить к разрешенной кодовой комбинации.

Свойства УЦК (квазициклических кодов)

1. Образуются делением x^n+1 на ОП.
2. Сумма разрешенных комбинаций УЦК является разрешенной комбинацией.
3. Имеет ту же кратность $t_о$ и $t_и$.
4. Используются те же схемы кодеков, при условии, что каждому усеченному коду спереди приписывается l нулей.

Укороченный ЦК

- ## Пример

- Необходимо передать сообщение, закодированное кодом МТК-2 ($k=5$). Обеспечить у получателя $t_и=1$.

Решение

- Однократная ошибка исправляется при $d_{min}=3$. Подходят коды (7,4); (15,11);(31,26) и т.д.
- Код (7,4) не подходит, т.к. k д.б. равно 5. Выбираем код (15,11).

Пример

- Необходимо исключить l=6 первых столбцов и строк ОМ $G_{11,15}$. Получаем УЦК (9,5).
- Выбираем ОП с учетом разложения

  $x^{15}+1=(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)\ (x^4+x^3+x^2+x+1)$

  Учитывая, что r=9-5=4, выбираем $P(x)=x^4+x+1$.
- Строим ОМ

Пример

$$
G_{11,15} = \begin{array}{c|ccccccccccccccc|c}
 & 1&0&0&1&1&0&0&0&0&0&0&0&0&0&0 & 1\\
 & 0&1&0&0&1&1&0&0&0&0&0&0&0&0&0 & 2\\
 & 0&0&1&0&0&1&1&0&0&0&0&0&0&0&0 & 3\\
 & 0&0&0&1&0&0&1&1&0&0&0&0&0&0&0 & 4\\
 & 0&0&0&0&1&0&0&1&1&0&0&0&0&0&0 & 5\\
 & 0&0&0&0&0&1&0&0&1&1&0&0&0&0&0 & 6\\
 & 0&0&0&0&0&0&1&0&0&1&1&0&0&0&0 & 7\\
 & 0&0&0&0&0&0&0&1&0&0&1&1&0&0&0 & 8\\
 & 0&0&0&0&0&0&0&0&1&0&0&1&1&0&0 & 9\\
 & 0&0&0&0&0&0&0&0&0&1&0&0&1&1&0 & 10\\
 & 0&0&0&0&0&0&0&0&0&0&1&0&0&1&1 & 11\\
\hline
 & 1&2&3&4&5&6&7&8&9&10&11&12&13&14&15 &
\end{array}
$$

(1)

Пример

Усеченная матрица

$$G_{5,9} = \begin{array}{c} \begin{vmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{vmatrix} \end{array} \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \qquad (2)$$

Пример

- Приведем усеченную матрицу (2) к каноническому виду

$$G_{к(5,9)} = \left|\begin{array}{ccccc:cccc} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{array}\right|$$

$$\underbrace{}_{E}$$

$1=1\oplus4\oplus5$

$2=2\oplus5$

$3=3$ (3)

$4=4$

$5=5$

7. Примитивные многочлены

- Многочлен $g(x)$ степени r является **примитивным**, если $x^n + 1$ делится на $g(x)$ для $n=2^r-1$ и не делится на $g(x)$ ни для какого меньшего значения n.

Примеры примитивных g(x)

$x^3 + x^2 + 1$

- делит $x^7 + 1$;
- не делит $x^j + 1$ при $j<7$

$x^4 + x^3 + 1$

- делит $x^{15} + 1$;
- не делит $x^j + 1$ при $j<15$

3. Коды БЧХ

- В 1960 году независимо Боуз (Bose), Чоудхури (Chaudhuri) и Хоквенгем (Hocquengem) открыли способ построения полиномиальных кодов с заданным минимальным расстоянием между кодовыми словами. Эти коды получили название БЧХ-кодов (BCH codes).
- Различают двоичные БЧХ-коды и недвоичные (коды Рида-Соломона (Reed, Solomon)).
- БЧХ-коды являются обобщением кодов Хэмминга на случай исправления нескольких независимых ошибок ($t_и>1$).

Коды БЧХ

Частные случаи БЧХ-кодов

1. Коды Файра, предназначенные для обнаружения и исправления серийных ошибок («пачек»).
2. Код Голея – исправляет одиночные, двойные и тройные ($d_{min}=7$) ошибки.
3. Коды Рида-Соломона (РС-коды), у которых символами являются многоразрядные двоичные числа.

Построение образующего полинома кода БЧХ

1. Задают n – длину блока кода БЧХ
2. Находят примитивный многочлен минимальной степени q*:

$$q \geq \log_2(n+1)$$

$$(n \leq 2^q - 1)$$

Построение образующего полинома кода БЧХ

- Пусть α — корень минимального многочлена.
- Тогда*

$$g(x) = \text{НОК}(m_1(x),\dots,m_{d-1}(x))$$

где $m_1(x),\dots,m_{d-1}(x)$

— многочлены минимальной степени с корнями $\alpha, \alpha^2,\dots, \alpha^{d-1}$.

$g(x)$ задает требуемые n и d.

Пример построения кода БЧХ

- Зададим n=15, d=5.
- Тогда

$$q = \log_2(n+1) = 4$$

— степень примитивного полинома $x^4 + x^3 + 1$.

Пусть α — его корень (как α^2 и α^4)*.
α^3 является корнем полинома

$$x^4 + x^3 + x^2 + x + 1$$

Пример построения кода БЧХ

$$g(x) = \text{НОК}(x^4 + x^3 + 1, x^4 + x^3 + x^2 + x + 1) =$$
$$(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1) = x^8 + x^4 + x^2 + x + 1$$

- Получили образующий полином кода БЧХ (15,7). Кодовое слово получают как и при циклическом кодировании.

Пример построения кода БЧХ

- Пусть 0010001— информационная последовательность: $Q(x)= x^4 +1$.
- Тогда ей соответствует кодовое слово 001000001100111.

$$(g(x)\cdot Q(x)= x^{12}+x^6+x^5+x^2+x+1).$$

4. Код Файра

- Код Файра (КФ) относится к систематическим (линейным) блочным разделимым (n, k)-кодам, в которых k первых разрядов представляют собой комбинацию первичного кода, а последующие $r=(n-k)$ разрядов являются проверочными. Предназначен КФ для обнаружения и исправления одиночной пачки ошибок длиной b, возникающих при передаче кодовых комбинаций по каналу связи.

Код Файра

- Образующий полином

$$P(x) = g(x)(x^c + 1) \qquad (1)$$

g(x) — неприводимый полином степени t, принадлежащий степени m, c — простое число.

t	2	3	4	5
g(x)	111	1011	10011	100101 101111 110111

Код Файра

Определение

Многочлен $g(x)$ принадлежит некоторой степени m, если m – наименьшее положительное число такое, что двучлен x^m+1 делится на $g(x)$ без остатка.

Для любого t существует, по крайней мере, один неприводимый многочлен $g(x)$ степени t, принадлежащий степени m.

Пример

- Пусть $t=2$.
- Тогда многочлен $g(x) = x^2+x+1$ принадлежит степени $m=2^2-1=3$, т.е.

$$(x^3+1) = (x+1)(x^2+x+1)$$

Параметры кода Файра

- Степень g(x)

$$t \geq b \ * \qquad (2)$$

- Число корней g(x)

$$m = 2^t - 1 \qquad (3)$$

- Степень $(x^c + 1)$

$$c > t \qquad (4)$$

- Длина кодовой комбинации:

$$n = \text{НОК}\ (c \times m) \qquad (5)$$

- Число проверочных разрядов

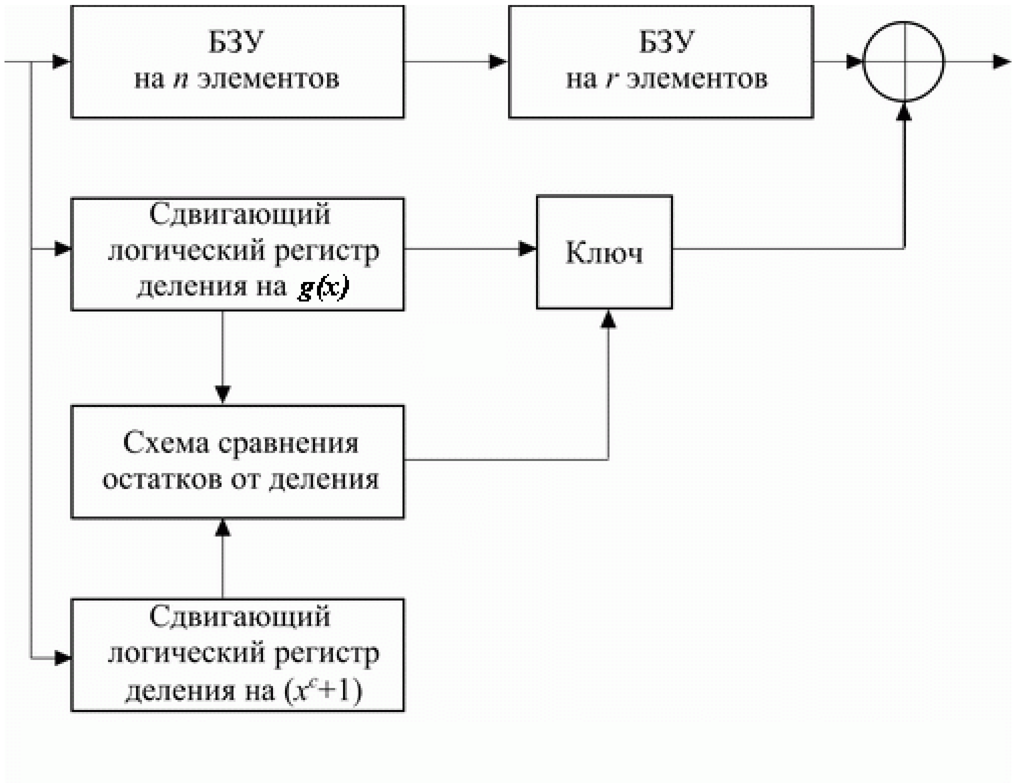
$$r = c + t \qquad (6)$$

Код Файра

Кодирование

1. К информационной комбинации дописывается r нулей (в младшие разряды кодовой комбинации).
2. Полученное число делится на образующий полином P(x).
3. Информационная комбинация, дополненная r нулями суммируется по mod2 с полученным в п.2 остатком*.
4. Кодовая комбинация передается в КС.

Код Файра
(структурная схема декодера)



Код Файра

Декодирование

- При декодировании производится раздельное деление принятой кодовой комбинации на полином $g(x)$ степени t и на полином (x^c+1).
- В результате такого деления в сдвигающих логических регистрах (СПР), соответствующих многочленам $g(x)$ и (x^c+1), получаются остатки $R1(x)$ и $R2(x)$, которые будут нулевыми, если ошибок не было. Если же прошла одиночная пачка ошибок длиной $b \le t$, то остатки будут отличны от нуля и не равны между собой.

Код Файра

Декодирование

- Для исправления данной пачки ошибок продолжают деление, сдвигая кодовые комбинации в СЛР до совпадения остатков. При этом входная кодовая комбинация сдвигается и в буферном регистре.
- Совпадение остатков означает обнаружение пакета ошибок.
- Количество дополнительных сдвигов без числа проверочных разрядов указывает на место, которое занимает ошибочный пакет в декодируемой кодовой комбинации.

Код Файра

Коррекция ошибок

- Кодовая комбинация остатка от деления на g(x) является корректирующей комбинацией, которая добавляется к искаженно принятой комбинации в момент открытия ключа.