8. Prakticheskoe zanjatie “Sostavlenie algoritmov sistematicheskogo i nesistematicheskogo ciklicheskogo kodirovanija”

Процедура кодирования безызбыточного *к*-разрядного исходного слова $A(x)$ может быть осуществлена двумя путями:

1. $B(x)=A(x)\cdot P(x)$. Эта процедура неудобна, так как в блоках $B(x)$, сформированных таким путем, нет четкого разделения информационных и проверочных символов, то есть такое кодирование – *несистематическое*.

2. Рассмотрим процедуру *систематического* кодирования с помощью циклических кодов. Для этого безызбыточное *к*-разрядное исходное слово запишем вначале в виде многочлена $A(x)$ степени $к–1$. Затем умножим его на x^r, где $r=m–k$, m – число разрядов циклического кода, в результате чего степень каждого одночлена, входящего в $A(x)$, увеличивается на r, то есть к $A(x)$ приписывается справа r нулей. Например, пусть $A(x) = x^3 + x + 1$, $r=3$. Тогда $x^3 \cdot A(x) = x^6 + x^4 + x^3$, В числовой форме $A(x)\rightarrow 1011$ (это слово не циклическое, поэтому циклический перенос здесь не делается), $x^3A(x)\rightarrow 1011000$. Здесь и далее стрелка – знак соответствия.

Получаем многочлен степени $k–1+r=m–1$, содержащий m разрядов. Разделим его на порождающий многочлен $P(x)$ степени r:

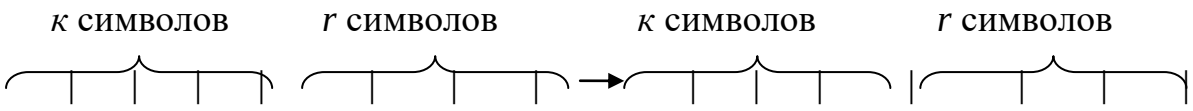
$$\frac{x^r \cdot A(x)}{P(x)} = Q(x) + \frac{R(x)}{P(x)}, \qquad (*)$$

где частное $Q(x)$ – многочлен степени $m–1–r=k–1$, $R(x)$ – остаток имеющий степень не более $r–1=m–k–1$, то есть кодовая группа $R(x)$ содержит не более $m-k=r$ разрядов. Но многочлен $x^r \cdot A(x)$ содержит справа r нулей. Умножим левую и правую часть выражения (*) на $P(x)$ и прибавим (по mod2) $R(x)$, тогда получим

$$x^r \cdot A(x) + R(x) = Q(x) \cdot P(x),$$

то есть $x^r \cdot A(x) + R(x)$ делится на $P(x)$ без остатка.

Результат кодирования поясняется приведенной ниже диаграммой:



$A(x)$ же при дел нули ступи $A(x)$ $R(x)$ на $P(x)$ остаток $R(x)\neq 0$, то это свидет информацион- проверочные ким образом, остаток $R(x)$ от деления н ные символы символы ере является синдромом для «лечения» кодовой комбинац

Кодирование – это в данном случае преобразование $к$-разрядного безызбыточного кода в m-разрядный циклический код. При систематическом кодировании, как мы видели, алгоритм кодирования должен включать в себя:

1) Сдвиг $A(x)$ влево на r разрядов, получение $x^r \cdot A(x)$.

2) Вычисление остатка от деления $x^r A(x)$ на $P(x)$.

3) Приписывание к $A(x)$ остатка $R(x)$ вместо r нулей:

$$B(x) = x^r A(x) + R(x).$$

Декодирование – это обратное преобразование m-разрядного циклического кода в $к$-разрядный безызбыточный код. Оно включает в себя:

1) Деление поступившей комбинации $B^*(x)$ на $P(x)$.

2) Если остаток равен нулю, то в слове $B^*(x)$ отбрасываются r последних разрядов и формируется выходное слово $A(x)$.

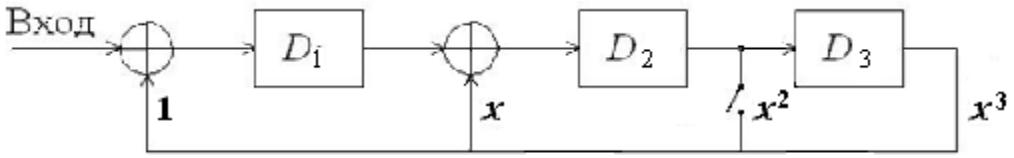
3) Если остаток не равен нулю, то он анализируется (подобно анализу синдрома при использовании алгебраического кода общего вида) и синдром дешифруется, то есть вырабатывается вектор ошибок $e(x)$, который нужно прибавить к $B^*(x)$, чтобы после удаления r последних разрядов получить выходное слово $A(x)$.

9. Prakticheskoe zanjatie “Razrabotka strukturnoj shemy ciklicheskogo kodera”

Итак, и для кодирования, и для декодирования необходимы устройства, осуществляющие деление многочленов $B^*(x)$ на порождающий многочлен $P(x)$. Эти устройства выполняются на регистрах сдвига с обратными связями.

Например, пусть порождающий многочлен $P(x) = x^3 + x + 1 \rightarrow 1011$.

Тогда регистр – делитель на порождающий полином имеет вид, показанный на рисунке ниже.



Обратные связи соответствуют структуре порождающего многочлена: они есть в тех разрядах, в которых коэффициенты порождающего многочлена раны 1, и отсутствуют в тех разрядах, где эти коэффициенты равны нулю.

Рассмотрим процесс кодирования на примере.

Пусть $A(x) = x^3 + x \rightarrow 1100$, r=3, $P(x) = x^3 + x + 1 \rightarrow 1011$.

Тогда $x^r A(x) = x^3 A(x) = x^6 + x^5 \rightarrow 1100000\backslash$

$$
\begin{array}{r|l}
1100000 & 1011 \\
\underline{1011} & \overline{111} \\
1110 & \\
\underline{1011} & \\
1010 & \\
\underline{1011} & \\
0010 \rightarrow R(x)=x &
\end{array}
$$

Этот остаток приписывается справа к слову $A(x)$. Тогда получаем

$$B(x) = x^3 A(x) + R(x) = x^6 + x^5 + x \rightarrow 100010 \rightarrow B_2(\text{x}).$$

При этом четыре первых символа – информационные, три следующих – проверочные.