6. Konspekt lekcii “Principy postroenija ciklicheskih blochnyh kodov”

Циклические коды

Циклические коды являются линейными блочными кодами, которые могут декодироваться с помощью проверочных уравнений и синдромов, способ получения которых был указан выше. Однако в кодовых словах циклических кодов символы связаны дополнительными алгебраическими зависимостями, что позволяет упростить кодирование и декодирование.

Основным свойством циклических кодов является то, что циклический сдвиг символов кодового слова на один символ также образует разрешенное кодовое слово. Циклические коды, таким образом, образуют подгруппу. Например:

B_1=0110001

B_2=1100010

B_3=1000101

B_4=0001011

B_5=0010110

B_6=0101100

B_7=1011000

B_8=0000000

плюс все инверсии этих слов, итого 16 слов.

Кодовые слова двоичного циклического кода можно условно представить в виде многочленов $B(x)$ от фиктивной переменной x в различных степенях, с коэффициентами 0 и 1. Если число разрядов кодового слова равно m, то наивысшая степень многочлена равна m–1, например, $B_2(x) = x^6 + x^5 + x$.

Циклический сдвиг на 1 символ соответствует умножению многочлена на x с заменой коэффициента при x^0 на коэффициент при x^n. Например,

$$xB_2(x) = x^5 + x^2 + 1 = B_3(x).$$

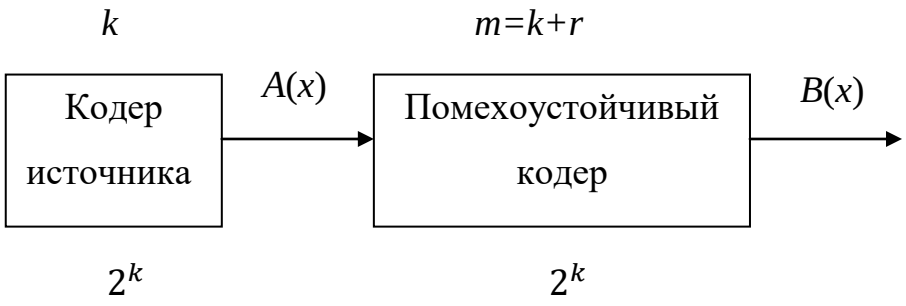
Среди комбинаций циклического кода можно найти такую, которая соответствует многочлену минимальной степени. Для показанного выше

набора кодовых слов это будет $B_4(x) = x^3 + x + 1$. Обозначим этот многочлен $P(x)$. Можно показать, что для циклических кодов $P(x)$ является делителем любого $B(x)$ и что комбинация $B(x)$ из m символов принадлежит коду (то есть является разрешенной) тогда и только тогда, когда она делится на $P(x)$ без остатка. Поэтому $P(x)$ называют образующим (порождающим, производящим) многочленом циклического кода.

Таким образом, все кодовые слова циклического кода делятся без остатка на образующий многочлен $P(x)$. Если $P(x)$ – многочлен r-й степени, то он содержит $r+1$ разрядов, а частное от деления представляет собой многочлен степени не более $m–1–r=k–1$, причем все частные различны, поскольку различны m-разрядные кодовые слова. Таким образом, с помощью циклического кода можно образовать $2^{m-r} = 2^k$ различных m-разрядных слов, без остатка делящихся на $P(x)$, а деление использовать в качестве проверочной процедуры при декодировании. Если остаток при делении равен нулю, то кодовое слово является разрешенным, если нет, то оно содержит ошибки.

Анализ остатка, полученного при делении, позволяет исправить ошибки, если избыточность кода для этого достаточна. Если остаток равен нулю, то кодовое слово принято правильно или в нем содержится необнаруживаемые ошибки. Таким образом, остаток является синдромом.

Пример



	Количество разрядов	Степень полинома
Безызбыточное слово	k	$\leq k–1$

источника		
Порождающий полином циклического кода	$r+1$	r
Избыточное m-разрядное слово	m	$\leq m-1$
Частное от деления избыточного слова на порождающий полином	$m-r$	$\leq m-1-r$
Остаток от деления избыточного слова на порождающий полином	$\leq r$	$\leq r-1$