Лекция 6

Сверточные коды

Сверточные коды относятся к классу древовидных. В отличие от блоковых кодов последовательность информационных символов в них не разделяется на фрагменты, а обрабатывается непрерывно по мере поступления. Количество символов в такой последовательности не ограничено.

Вариант схемы простейшего сверточного кодера представлен на рис.1. Сверточный кодер может быть построен на основе регистра сдвига, содержимое которого сдвигается на один разряд вправо при введении в него слева нового двоичного символа (содержимое самого правого разряда при этом теряется) рис. 1,а. Кроме того, сверточный кодер содержит сумматоры по модулю 2, соединенные с определенными ячейками регистра сдвига. На выходе кодера, изображенного на рис. 1, установлены ключи, скорость переключения которых в два раза больше скорости поступления символов на вход кодера. Таким образом, на один двоичный входной символ в кодере формируются два выходных.

Для сверточных кодов как и для блоковых существует понятие - **скорость кода (*R_0*),** которая равна отношению количеств двоичных символов в единицу времени на входе (k_0) и выходе (n_0) кодера

$$R_0 = k_0 / n_0 . \qquad (1)$$

Для рассматриваемых кодов есть также понятие - **длина кодового ограничения *L***, которая численно равна количеству ячеек в регистре сдвига. Этот параметр показывает, какое количество информационных символов одновременно участвует в формировании символов, поступающих на выход кодера.

Кроме того, для сверточного кодера, изображенного на рис.1, можно ввести понятие - **состояние кодера**. Состояние сверточного кодера совпадает с двумя последними входными двоичными символами, введенными в кодер. Самый последний поступивший символ это и есть последний символ состояния. Состояние сверточного кодера рис. 1,а совпадает с содержимым двух левых ячеек регистра сдвига, причем считывать значения символов следует справа налево.

Название сверточных кодов обусловлено тем, что последовательность символов на выходе сверточного кодера можно рассматривать как свертку импульсной характеристики кодера с входной последовательностью. Если, к примеру, на вход кодера рис. 1, а или б поступает последовательность 10000000… , то соответствующая выходная последовательность имеет вид 11 10 11 00 00 00 00 00… (первым на выход поступает символ с верхнего сумматора, вторым - с нижнего).

Выходная последовательность, соответствующая произвольной входной последовательности, получается путем сложения по модулю 2 сдвигов этой последовательности . Порождающая матрица для данного кода может быть представлена в виде

$$G = \begin{bmatrix} 11\,10\,11\,00\,00\,00\,00\,00 \cdots & \\ 00\,11\,10\,11\,00\,00\,00\,00\,00 \cdots & \\ 00\,00\,11\,10\,11\,00\,00\,00\,00\,00 \cdots & \\ 00\,00\,00\,11\,10\,11\,00\,00\,00\,00\,00 \cdots & \\ . & \\ . & \\ . & \end{bmatrix} \qquad (2)$$

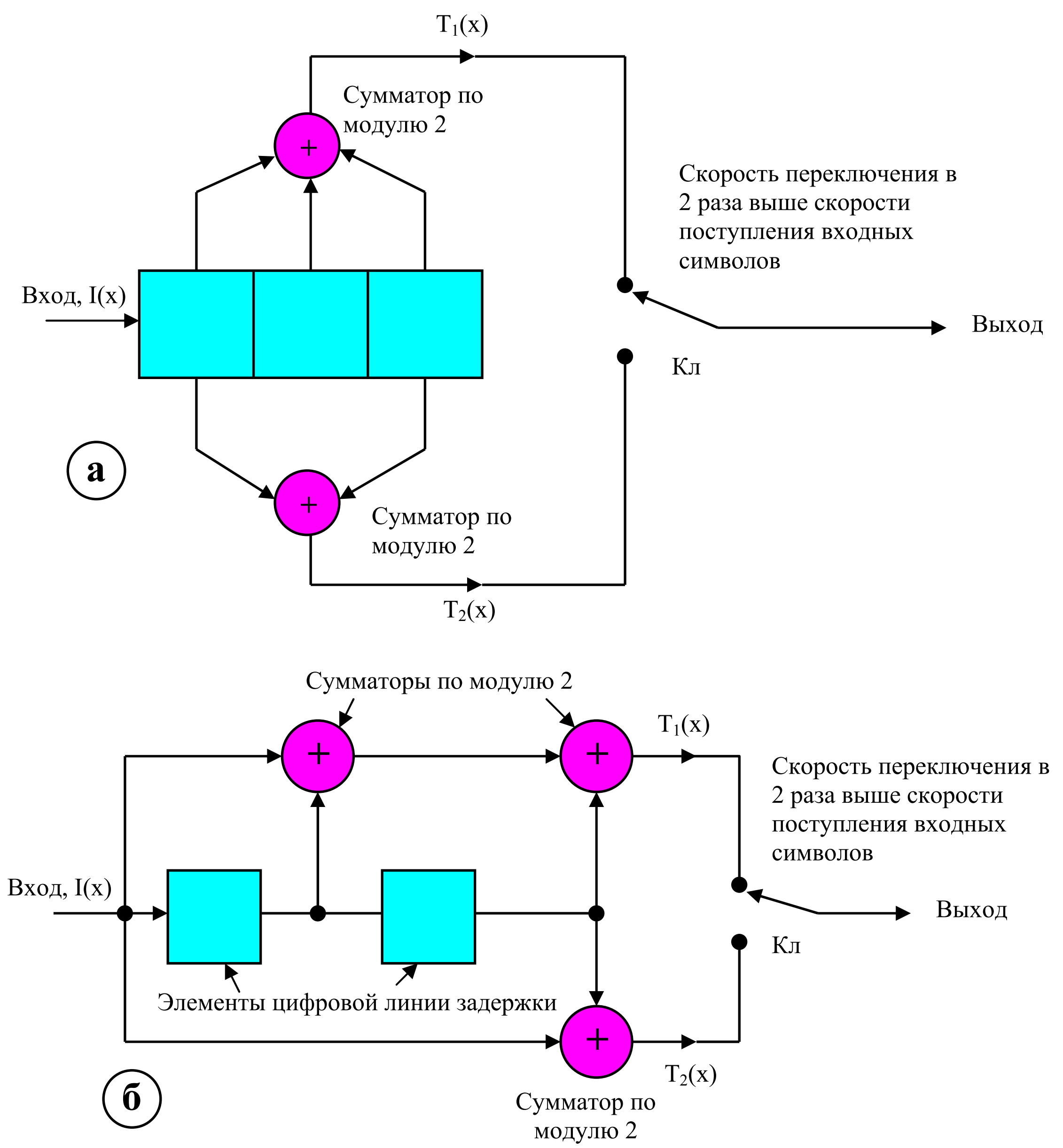

Рис.1. Варианты построения схемы сверточного кодера с параметрами: скорость кода R0 = 1/2; длина кодового ограничения L = 3;
а – сверточный кодер, построенный на основе регистра сдвига; б – сверточный кодер, построенный на основе цифровой линии задержки.

Как отмечалось выше, длина информационной последовательности в сверточных кодах не ограничена и в идеале может быть бесконечной. Поэтому порождающую матрицу (2) иногда называют полубесконечной.

Допустим, что на вход кодера поступила последовательность информационных символов 11010000… Тогда выходную последовательность можно определить, сложив посимвольно по модулю 2 первую, вторую и четвертую строки порождающей матрицы (2)

$$\begin{array}{r} 11\;10\;11\;00\;00\;00\;00\;00\cdots \\ \oplus\; 00\;11\;10\;11\;00\;00\;00\;00\cdots \\ 00\;00\;00\;11\;10\;11\;00\;00\cdots \\ \hline \end{array}$$

$$\left.\begin{array}{l} \textit{выходная} \\ \textit{последова} - \\ \textit{тельность} \end{array}\right\} 11\;01\;01\;00\;10\;11\;00\;00\cdots$$

Аналогичным образом с помощью порождающей матрицы можно определить последовательность выходных символов для произвольного сочетания входных.

Связи между ячейками регистра сдвига или отводами цифровой линии задержки с сумматорами по модулю 2 описываются порождающими многочленами, комбинациями двоичных символов, а также числами в восьмеричной системе счисления. Один разряд комбинации двоичных символов соответствует наличию или отсутствию связи данной ячейки регистра сдвига (отвода цифровой линии задержки) с сумматором по модулю 2. При этом символ 1 указывает на то, что такая связь есть, а символ 0 - что связи нет. Для верхних сумматоров, установленных в кодерах рис. 1, комбинация двоичных символов - 111, в восьмеричной форме записи – число 7, что соответствует порождающему полиному $g_1(x) = x^2 + x + 1$. Нижние сумматоры этих кодеров связаны с крайними ячейками регистра сдвига (отводами цифровой линии задержки). Связи с центральной ячейкой (отводом) нет, поэтому комбинация двоичных символов - 101, в восьмеричной форме записи - число 5, порождающий многочлен имеет вид $g_2(x) = x^2 + 1$.

Недвоичные коды

Допустим, что кодовое слово имеет вид

$$Z = a_{n-1}, a_{n-2}, ..., a_2, a_1, a_0 .$$

В случае двоичного кода каждый из символов кодового слова является двоичным символом 0 или 1 и содержит один бит информации. Однако, существуют коды, в которых каждый символ кодового слова содержит по несколько двоичных символов (битов информации). Такие коды называются недвоичными. Обычно количество двоичных символов в одном символе кодового слова недвоичного кода равно степени числа 2. Пояснить это можно с помощью таблицы 1. Первая строка табл. 1 соответствует двоичному коду, у которого, как отмечалось выше, в одном символе кодового слова содержится один двоичный символ (бит информации), основание кода $q=2^1=2$ (отсюда и название), алфавит кода (т. е. все множество символов, из которых составляются кодовые слова) содержит два числа 0 и 1.

Таблица 1

Количество двоичных символов в одном символе кодового слова m	Основание кода $q = 2^m$	Алфавит кода (содержит $q=2^m$ символов)	Обозначение поля Галуа
1	$q = 2^1$	0, 1	GF(2)
2	$q = 2^2 = 4$	00, 01, 10, 11	GF(2^2)
3	$q = 2^3 = 8$	000, 001, 010, 011, 100, 101, 110, 111	GF(2^3)
4	$q = 2^4 = 16$	0000, 0001, 0010, 0011 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111	GF(2^4)
. . .	. . .	. . .	. . .
8	$q = 2^8 = 256$	00000000, 00000001, 00000010, 00000011,… , 11111111	GF(2^8)
. . .	. . .	. . .	. . .

Если в каждом символе кодового слова содержится два двоичных символа (бита информации) $m = 2$, то основание кода $q=2^2=4$, алфавит кода содержит четыре символа, по два двоичных разряда в каждом: 00, 01, 10, 11. Из этих двухразрядных символов образуются кодовые слова, и т. д.

Недвоичные коды относятся к классу полиномиальных. Кодовые слова в них представляются в виде степенных многочленов, а символы кодовых слов являются коэффициентами при составляющих многочленов с различными степенями x, причем эти символы сами могут быть представлены в виде степенных многочленов.

Укороченные циклические коды

При заданном линейном (n,k)-коде всегда можно построить линейный $(n-i, k-i)$-код, заменяя первые i информационных символов нулями и исключая их из кодовых векторов. В случае циклического кода это соответствует исключению первых i строк и столбцов из порождающей матрицы или первых i столбцов из проверочной матрицы. Полученный таким образом код не будет, однако, циклическим кодом, потому что циклический сдвиг кодового вектора не всегда является кодовым вектором. Такой код называется **укороченным циклическим кодом**.

Коды Рида-Соломона

Коды Рида – Соломона, или РС-коды, относятся к недвоичным циклическим кодам, т. е. кодам, символы которых взяты из конечного поля, содержащего $q > 2$ элементов и обозначаемого $GF(q)$, где q – степень некоторого простого числа. Например, в системах CD и DVD используются РС-коды, символы которых берутся из поля $GF(2^8)$.

Определение Кодом Рида-Соломона (РС-кодом) называют циклический (N,K)-код, при $N = q-1$, множество кодовых комбинаций которого представляется многочленами степени $N-1$ и менее с коэффициентами из поля $GF(q)$, где $q > 2$ и является степенью простого числа. Корнями порождающего многочлена кода Рида-Соломона являются $N-K$ последовательных степеней: $\alpha, \alpha^2, \alpha^3, \ldots, \alpha_{D-1}$, некоторого элемента $\alpha \in GF(q)$, где D – минимальное кодовое расстояние (N,K)-кода.

$$g(x) = (x-\alpha)(x-\alpha^2)\ldots(x-\alpha^{D-1})$$

РС-коды также могут быть укороченными. Например, коды РС (32,28) и (28,24), используемые в системе CD для коррекции ошибок, являются укороченными, образованными из кода РС максимальной длины (255, 251).