УДК 621.391.176

С. И. ПРИХОДЬКО, канд. техн. наук, *А. Г. СНИСАРЕНКО*

ПРИВЕДЕНИЕ ДВОИЧНЫХ СВЕРТОЧНЫХ КОДОВ К НЕДВОИЧНЫМ СУЖЕННЫМ ЦИКЛИЧЕСКИМ КОДАМ

При многих положительных свойствах сверточных кодов (СК), находящих все более широкое применение на практике, им присущ такой недостаток, как сложность их выбора и построения [1].

Методы построения порождающих многочленов СК можно разделить на две группы: переборные и конструктивные. Первая группа базируется на применении компьютеров, что даже с учетом тенденций их развития представляет значительные трудности в инженерной практике. Методы, имеющие конструктивный характер, обладают тем недостатком, что с их помощью можно получить СК только с ограниченным спектром свойств и характеристик. Причина этого заключается в том, что СК плохо описываются математически, в отличие, например, от циклических кодов. Отсюда вытекает задача математического описания СК, которое впоследствии стало бы основой для разработки конструктивных методов их построения.

Для решения задачи приведения математической модели, описывающей процесс кодирования информации двоичным сверточным кодером, к математической модели кодера какого-либо известного кода рассмотрим двоичный несистематический сверточный (n_0, k_0) код со скоростью $R = 1/2$. Пусть многочлен

$$M(x) = a_{k_0}x^{k_0} + a_{k_0-1}x^{k_0-1} + \ldots a_1x + a_0 \qquad (1)$$

— информационная последовательность, подлежащая кодированию (в общем случае многочлен $M(x)$ может быть бесконечной длины), а многочлены

$$P_1(x) = a_{r_{0_1}}x^{r_{0_1}} + a_{r_{0_1}-1}x^{r_{0_1}-1} + \ldots + a_{1_1} + a_{0_1};$$
$$P_2(x) = a_{r_{0_2}}x^{r_{0_2}} + a_{r_{0_2}-1}x^{r_{0_2}-1} + \ldots + a_{1_2} + a_{0_2}. \qquad (2)$$

будут порождающими многочленами данного сверточного кода, где коэффициенты при x в выражениях (1), (2) — элементы поля $GF(2)$. Пусть многочлены $P_1(x)$ и $P_2(x)$ вида (2) будут одинаковой степени, т. е. в случае, если один из многочленов имеет меньший показатель степени, то добавим в этом многочлене необходимое до большего количества число ненулевых коэффициентов при x. Тогда запишем

$$P_1(x) = a_{r_{0_1}}x^{r_0} + a_{r_{0_1}-1}x^{r_0-1} + \ldots + a_{1_1}x + a_{0_1};$$
$$P_2(x) = a_{r_{0_2}}x^{r_0} + a_{r_{0_2}-1}x^{r_0-1} + \ldots + a_{1_2}x + a_{0_2}. \qquad (3)$$

Процесс кодирования информации рассматриваемым сверточным кодером представим следующим образом. Информационная последовательность $M(x)$ вида (1) поступает в кодер сверточного кода, где происходит ее умножение на многочлены $P_1(x)$ и $P_2(x)$ вида (3) и получение последовательностей $F_1(x)$ и $F_2(x)$ соответственно

$$F_1(x) = M(x)P_1(x) = S_{k_0} + r_{0_1}{}^{k_0+r_0} + S_{k_0+r_{0_1}-1}x^{k_0+r_0-1} + \ldots + S_{1_1}x + S_{0_1};$$
$$F_2(x) = M(x)P_2(x) = t_{k_0+r_{0_2}}x^{k_0+r_0} + t_{k_0+r_{0_2}-1}x^{k_0+r_0-1} + \ldots + t_{1_2}x + t_{0_2},$$

где

$$S_i = \sum_{l+f=i}(a_c)_f(a_h)_l, \quad t_i = \sum_{l+f=i}(a_l)_f(a_v)_l; \qquad (4)$$
$$i = 0, 1, \ldots k_0 + r_{0_j} - 1, k_0 + r_{0_j}; \; j = 1, 2; \; c = 0, 1, \ldots, k_0 - 1, k_0;$$
$$h = 0, 1, \ldots, r_{0_1} - 1, r_{0_1}; \; p = 0, 1, \ldots, r_{0_2} - 1, r_{0_2},$$

т. е. коэффициенты при x — результат произведения таких коэффициентов при x у многочленов $M(x)P_1(x)$ и $P_2(x)M(x)$, сумма индексов которых равна i, и сложения всех таких произведений. Далее, на выходе кодера происходит перемежение выходных последовательностей $F_1(x)$ и $F_2(x)$ и получение последовательности $F_3(x)$,

т. е. осуществляется попарное считывание коэффициентов в выражениях для $F_1(x)$ и $F_2(x)$ вида (4) при одинаковых степенях x:

$$F_3(x) = (S_{k_0+r_{0_1}} x^{k_0+r_0},\ (t_{k_0+r_{0_2}} x^{k_0+r_0}) + (S_{k_0+r_0-1} x^{k_0+r_0-1}),$$
$$(t_{k_0+r_{0_0}-1} x^{k_0+r_0-1}) + \ \ldots\ + (S_{1_1} x),\ t_{1_2} x) + S_{0_1},\ t_{0_2}. \qquad (5)$$

Так как $k_0 + r_0 = n_0$, то

$$F_3(x) = [(S_{k_0+r_{0_1}}),\ (t_{k_0+r_{0_2}})]\, x^{n_0} + [(S_{k_0+r_0-1}),\ (t_{k_0+r_{0_0}-1})]\, x^{n_0-1} + \ \ldots\ +$$
$$+ [(S_{1_1}),\ (t_{1_2})]\, x + S_{0_1},\ t_{0_2}. \qquad (6)$$

Проанализируем коэффициенты при x в выражении (6). Из (4) видно, что коэффициенты S_i, t_i — элементы поля GF (2), причем каждый из коффициентов S_i, t_i содержит по одному элементу поля GF (2). Поскольку в (6) содержится по два коэффициента t_i и S_i, то, следовательно, при каждом значении x в (6), определяющем выходную последовательность сверточного кодера, будет находиться по два элемента поля GF (2).

Проведем аналогичные рассуждения для двоичного $(n_0,\ k_0)$ сверточного кода со скоростью $R = 1/3$. В этом случае в выражении (3) будет по три порождающих многочлена сверточного кода $P_1(x)$, $P_2(x)$, $P_3(x)$. Отсюда и в соотношении (6) будет при соответствующих степенях x по три элемента поля GF (2). Таким образом, по индукции, если скорость двоичного $(n_0,\ k_0)$ кода $R = 1/m$, то в выражении (6) будет по m элементов поля GF (2) при соответствующих степенях x:

$$F_m(x) = (T_1,\ T_2,\ \ldots,\ T_m)\, x^{n_0} + (T_1,\ T_2,\ \ldots,\ T_m)\, x^{n_0-1} +$$
$$+ (T_1,\ T_2,\ \ldots,\ T_m)\, x + (T_1,\ T_2,\ \ldots,\ T_m), \qquad (7)$$

где T_i — коэффициенты при x вида (4) для $j = 1,\ 2,\ \ldots,\ m$ и $i = 1,\ 2,\ \ldots,\ m$. Однако любые m элементов поля GF (2) можно выразить одним элементом поля GF (2^m), так как элементы любого поля $GF(q)$, где $q = p^m$, а p — простое число, можно представить m-многочленами с коэффициентами из поля $GF(p)$. Тогда, обозначив в (7) коэффициенты при x через q_i, получим

$$F_c(x) = q_{n_0} x^{n_0} + q_{n_0-1} x^{n_0-1} + \ \ldots\ + q_1 x + q_0. \qquad (8)$$

Здесь q_i — элементы поля $GF(2^m)$, $i = 0,\ 1,\ \ldots,\ 2^m - 1$. Коэффициенты при x в выражении (8), определяющем выходную последовательность сверточного кодера, будут определяться коэффициентами при x в информационной последовательности $M(x)$ вида (1) и коэффициентами при x в порождающих сверточный код многочленах $P_1(x),\ P_2(x),\ \ldots,\ P_m(x)$ вида (3). Пусть теперь $M(x) = 1$, т. е. приравняем к нулю все коэффициенты при x, кроме x^0. Тогда коэффициенты при x в многочленах $P_1(x),\ P_2(x),\ \ldots,\ P_m(x)$ — вида (3). Следовательно, выражение (8) в этом случае будет определять сверточный $(n_0,\ k_0)$ код над полем GF (2) со скоростью $R = 1/m$, т. е. будет определять его порождающие многочлены. Отсюда вытекают следующие утверждения.

Утверждение 1. Порождающие многочлены сверточного (n_0, k_0) кода над полем $GF(2)$ $P_1(x)$, $P_2(x)$, ..., $P_m(x)$ со скоростью $R = 1/m$ вида (3) можно представить одним многочленом $F_c(x)$ вида (8) над полем $GF(2^m)$, полностью определяющим тот же самый сверточный код.

Назовем такое представление порождающих многочленов двоичного сверточного кода обобщенным представлением. Установим теперь связь между двоичными сверточными кодами и циклическими кодами на основании обобщенного представления двоичных сверточных кодов. Рассмотрим для этого недвоичный циклический (n, k) код, порождающий многочлен которого выбран из поля разложения двухчлена $(x^n - 1)$ над полем $GF(2^m)$, где m — мультипликативный порядок 2 по модулю n:

$$G(x) = a_r x^r + a_{r-1} x^{r-1} + \ldots + a_1 x + a_0. \tag{9}$$

Пусть

$$M(x) = a_{k-1} x^{k-1} + a_{k-2} x^{k-2} + \ldots a_1 x + a_0 \tag{10}$$

— информационный многочлен, подлежащий кодированию. Тогда выходная последовательность или кодовая последовательность имеет вид

$$F(x) = M(x) G(x) = a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \ldots + a_1 x + a_0, \tag{11}$$

где коэффициенты при x в выражениях (9) — (11) — элементы поля $GF(2^m)$. Циклический (n, k) код над полем $GF(2^m)$ можно также задать с помощью порождающей матрицы

$$G = \begin{bmatrix} a_r & a_{r-1} & \ldots & a_1 & a_0 & 0 & \ldots & 0 \\ 0 & a_r & a_{r-1} & \ldots & a_1 & a_0 & \ldots & 0 \\ & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \\ 0 & & & & a_1 & & & a_0 \end{bmatrix}. \tag{12}$$

Предпримем теперь следующее. Пусть множество коэффициентов при x у многочлена, подлежащего кодированию циклическим кодером, $M(x)$ вида (10) будет ограничено, т. е. пусть кодированию подлежат только многочлены с коэффициентами при x, принадлежащими только полю $GF(2)$. Однако при этом на выходе кодера получим множество кодовых слов $F(x)$ вида (11), у которых коэффициенты при x по-прежнему принадлежат полю $GF(2^m)$, хотя возможно, что у части кодовых многочленов коэффициенты при x принадлежат только полю $GF(2^m)$. Назовем такой код суженным (n_c, k_c) недвоичным кодом вида (13).

Утверждение 2. Если многочлены $G(x)$ вида (9) порождают циклический (n, k) код над полем $GF(2^m)$ с кодовым расстоянием d, то найденный из него суженный циклический (n_c, k_c) код вида (13) над полем $GF(2^m)$ с порождающим многочленом $G_c(x) = G(x)$ и кодовым расстоянием d обладает $d_c \geqslant d$.

Действительно, обозначим через V_1 и V_2 пространства кодовых слов для циклического и суженного циклического кодов. Так как

множество кодовых слов суженного циклического кода получается с помощью введения ограничения на множество кодовых слов циклического кода, то пространство V_2 является подпространством V_1. Пусть V_1' — подпространство кодовых слов с минимальным весом d пространства V_1. Тогда пространство V_2 может включать в себя полностью, частично или вообще не включать пространство V_1'. Следовательно, выбрав пространство V_2 так, чтобы оно не включало в себя подпространство V_1', можно тем самым увеличить кодовое расстояние суженного циклического кода d_c или оставить его равным d, но уменьшить его невозможно, поскольку V_1', V_2 — подпространства одного пространства V_1. Отсюда суженный циклический код будет обладать максимально возможным кодовым расстоянием d_c в том случае, если кодовые слова, имеющие вес не менее d_c, в циклическом коде есть результат кодирования информационных многочленов, у которых коэффициенты при x будут принадлежать только полю GF (2).

Вернемся к рассмотренному двоичному сверточному (n_0, k_0) коду со скоростью $R = 1/m$. Зададим его с помощью матрицы

$$D = \begin{bmatrix} D_0 & D_1 & \dots & D_n \\ 0 & D_0 & D_1 & \dots & D_{n-1} \\ & \cdot & \cdot & \cdot & \cdot \\ & \cdot & \cdot & \cdot & D_0 \end{bmatrix}, \tag{14}$$

где n — наибольшая из степеней, порождающих код многочленов, а D_i — подматрица вида

$$D_i = \begin{bmatrix} a_1^1 & a_2^1 & \dots & a_{n_0}^1 \\ a_1^2 & a_2^2 & \dots & a_{n_0}^2 \\ & \cdot & \cdot & \cdot \\ a_1^{k_0} & \cdot & \cdot & a_{n_0}^{k_0} \end{bmatrix}, \tag{15}$$

элементы которой — коэффициенты при x в порождающих многочленах вида (2). Для сверточных кодов со скоростью $R = 1/m$ матрицу D_i вида (15) представим в виде $D_i' = |\, a_1\ a_2 \dots a_{n_0}|$ **(16)**. Для несистематического сверточного кода число m определяется количеством порождающих код многочленов, т. е. $n_0 = m$. Отсюда

$$D_i'' = |\, a_1\ a_2 \dots a_m|. \tag{17}$$

Проанализируем матрицу D_i'' вида (17). Каждый элемент матрицы a_i принадлежит полю GF (2) и является коэффициентом при соответствующей степени x в порождающих сверточный код многочленах вида (2) или, что то же самое, каждая подматрица D_i'' вида (17) матрицы D вида (14) — совокупность коэффициентов при определенной степени x всех порождающих код многочленов. Следовательно, на основании утверждения 1 каждую подматрицу D_i'' вида (17) мат-

рицы D вида (14) можно заменить на соответствующий элемент a^i поля $GF(2^m)$ и получить матрицу

$$P = \begin{bmatrix} a_0 & a_1 & \dots & a_n & 0 & \dots \\ 0 & a_0 & a_1 & \dots & a_n & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \end{bmatrix}. \qquad (18)$$

При сравнении матрицы G вида (12) и матрицы P вида (18) можно заметить, что при ограничении числа строк и столбцов в матрице P матрицы будут одинаковыми. Иными словами, если эти матрицы одной размерности и обладают одними и теми же ненулевыми элементами, то они могут быть порождающими матрицами. Однако по условию матрица G вида (12) задает суженный циклический код вида (13), а матрица P вида (18) — порождающая матрица двоичного сверточного (n_0, k_0) кода со скоростью $R = 1/m$ над полем $GF(2)$.

Утверждение 3. Если многочлен $G(x)$ вида (9) порождает циклический (n, k) код над полем $GF(2^m)$, то полученный из него суженный циклический (n_c, k_c) код вида (13) полностью задает сверточный (n_0, k_0) код над полем $GF(2)$ со скоростью $R = 1/m$ и порождающим многочленом $F_c(x)$ вида (8), причем $G(x) = F_c(x)$.

На основании Утверждения 3 работу двоичного сверточного кодера со скоростью $R = 1/m$ можно описать следующим образом. Пусть задан циклический (n, k) код над полем $GF(2^m)$. Кодер такого кода реализуем с помощью регистра сдвига с длиной, определяемой степенью порождающего код многочлена $G(x)$ вида (9), связанного по модулю поля $GF(2^m)$, количество и связи которого с регистром сдвига определяются многочленом $G(x)$. На вход кодера поступают информационные многочлены $M(x)$ вида (10) с коэффициентами из поля $GF(2^m)$. В кодере происходит умножение многочлена $M(x)$ на многочлен $G(x)$ и получение многочлена $F(x)$ вида (11) с коэффициентами из поля $GF(2^m)$. Далее многочлен $F(x)$ представляется в виде многочлена над полем $GF(2)$, при этом каждый элемент поля $GF(2^m)$ задается последовательностью из m элементов поля $GF(2)$. Приведенная к двоичному $F(x)$ представляет собой кодовую последовательность $F_з(x)$ вида (6) сверточного (n_0, k_0) кода над полем $GF(2)$, соответствующую переданной входной последовательности $M(x)$ вида (10) с коэффициентами из поля $GF(2)$. Таким образом мы реализуем процесс кодирования информации двоичным сверточным кодером. Если циклический (n, k) код существует над полем $GF(2^m)$, то на каждый входной символ кодера, являющегося элементом поля $GF(2)$, на выходе кодера появится m символов, принадлежащих полю $GF(2)$, т. е. скорость сверточного кода будет равна $R = 1/m$.

Итак, на основании утверждения 3 можно получать порождающие многочлены сверточных кодов над полем $GF(2)$ со скоростью $R = 1/m$, используя для этого порождающие многочлены циклических кодов над полем $GF(2^m)$. Вместе с тем Утверждение 3 не определяет значение кодового расстояния полученного при этом двоичного

сверточного кода. Отсюда возникает задача выбора порождающих многочленов недвоичных циклических кодов для нахождения порождающих многочленов двоичных сверточных кодов с заранее заданными характеристиками и свойствами.

Список литературы: 1. *Нейфах А. Э.* Сверточные коды для передачи дискретной информации. М., 1979. 222 с. 2. *Теория* кодирования / Т. Касами, Н. Токура, Е. Ивадари, Я. Инагаки. М., 1978. 576 с. 3. *Кларк Дж., Кейн Дж.* Кодирование с исправлением ошибок в системах цифровой связи. М., 1987. 392 с.

Поступила в редколлегию 29.01.88