УДК 621.391

А.А. КУЗНЕЦОВ, С.И. ПРИХОДЬКО, С.А. ГУСЕВ, И.Е. КУЖЕЛЬ

Харьковский университет Воздушных Сил, Украина

АЛГЕБРАИЧЕСКИЙ МЕТОД СВЕРТОЧНОГО КОДИРОВАНИЯ

Предлагается алгебраический метод сверточного кодирования, состоящий в представлении порождающих многочленов сверточного кода через порождающий многочлен недвоичного циклического кода, ограниченного на произвольное подполе. Его использование позволяет алгебраически строить сверточные коды с заданными конструктивными свойствами.

сверточный код, порождающий многочлен, циклический код

Постановка проблемы в общем виде, анализ литературы

Одним из перспективных направлений в развитии теории помехоустойчивого кодирования является разработка методов сверточного кодирования [1 – 4]. Суть этих методов состоит в представлении информационного потока данных блоками (кадрами) длины k^0 и сопоставлении с каждым из них блока кодовых символов. При этом каждый полученный кадр кодовых символов формируется с учетом предыдущих r кадров информационных символов.

На рис. 1 представлена обобщенная схема сверточного кодера. Информационная последовательность вводится в кодер, начиная с нулевого момента времени и до бесконечности. Поток входящих информационных символов разбивается на кадры по k^0 символов. В течение каждого момента времени в регистр сдвига вводится новый кадр информационных символов.

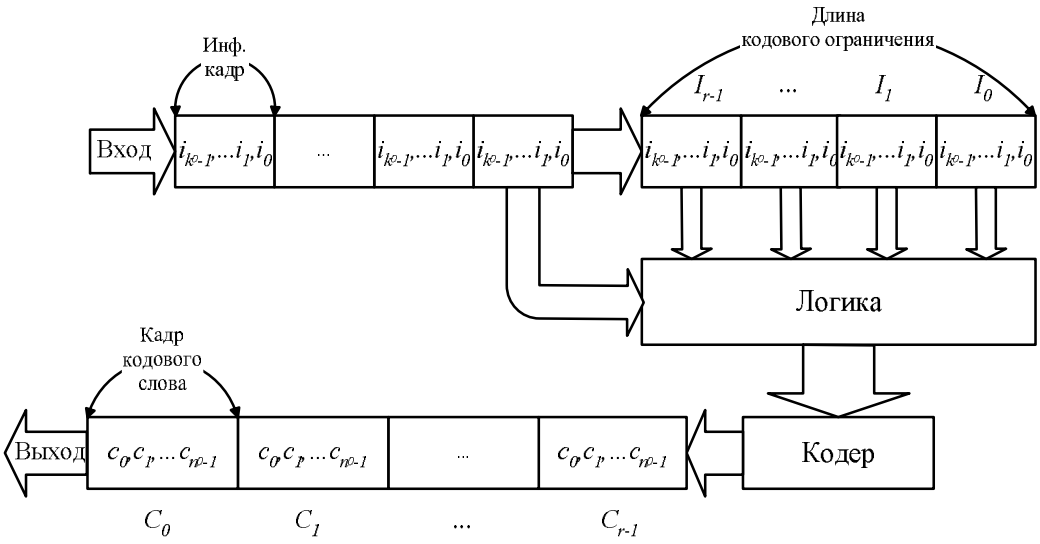

Рис. 1. Сверточный кодер в виде регистра сдвига

Кодер по введенному кадру и r хранящимся в нем кадрам вычисляет один кадр кодового слова, имеющий длину n^0 символов. Каждым k^0 информационным символам соответствуют n^0 кодовых символов. Скорость R определяется как $R = k^0 / n^0$. Величина $\nu = r \cdot k^0$ называется длиной кодового ограничения. Минимальным кодовым расстоянием d называется минимальное расстояние для любых различных кодовых слов, соответствующих $r + 1$ различным информационным кадрам.

Набор минимальных весов d_l, l = 1, 2, 3, ..., произвольных кодовых слов, соответствующих l различным информационным кадрам, называется дистанционным профилем сверточного кода. Свободным расстоянием называется $d_\infty = max(d_l)$. Очевидно, что $d = d_{r+1} \le d_{r+2} \le ... \le d_\infty$.

Подавляющее большинство хороших и наиболее употребимых сверточных кодов получено переборным методом [1 – 4]. Основным его недостатком является быстрый рост вычислительных затрат. Так, выходная последовательность произвольного сверточного кода зависит от $\nu = r \cdot k^0$ входных символов (рис. 1), т.е. произвольный сверточный код над $GF(q)$ можно однозначно задать только путем определения логики преобразований входных символов, которая может быть представлена регистром сдвига с ν ячейками. Следовательно, для полного перебора всех возможных сверточных кодов с кодовым ограничением ν следует перебрать, как минимум,

$$N = \sum_{i=0}^{v} (q-1)^i C_v^i = q^v = q^{rk^0}$$

вариантов. Так, для перебора всех двоичных сверточных кодов с кодовым ограничением 100 бит необходимо выполнить перебор $2^{100} \approx 10^{30}$ различных вариантов и выбрать лучший из них, что является практически неразрешимой задачей. На практике переборным методом реализован поиск хороших двоичных сверточных кодов до $\nu \le 14$ [3]. Очевидно, что с практической точки зрения переборный метод построения сверточных кодов малоэффективен по причине своей низкой производительности. ***Актуальным направлением*** является разработка и исследование алгебраических методов построения сверточных кодов.

Целью статьи является разработка алгебраического метода сверточного кодирования, позволяющего алгебраически задавать коды и конструктивно определять их параметры.

1. Алгебраический метод построения сверточных кодов для $R = 1/m$

Рассмотрим несистематический сверточный (n, k) код над $GF(q)$ с параметрами: $k^0 = 1$, $n^0 = m \cdot k^0 = m$, $k = r+1$, $n = (r+1) \cdot n^0 = k \cdot m$ и скоростью $R = 1/m$, кодер которого представлен на рис. 2.

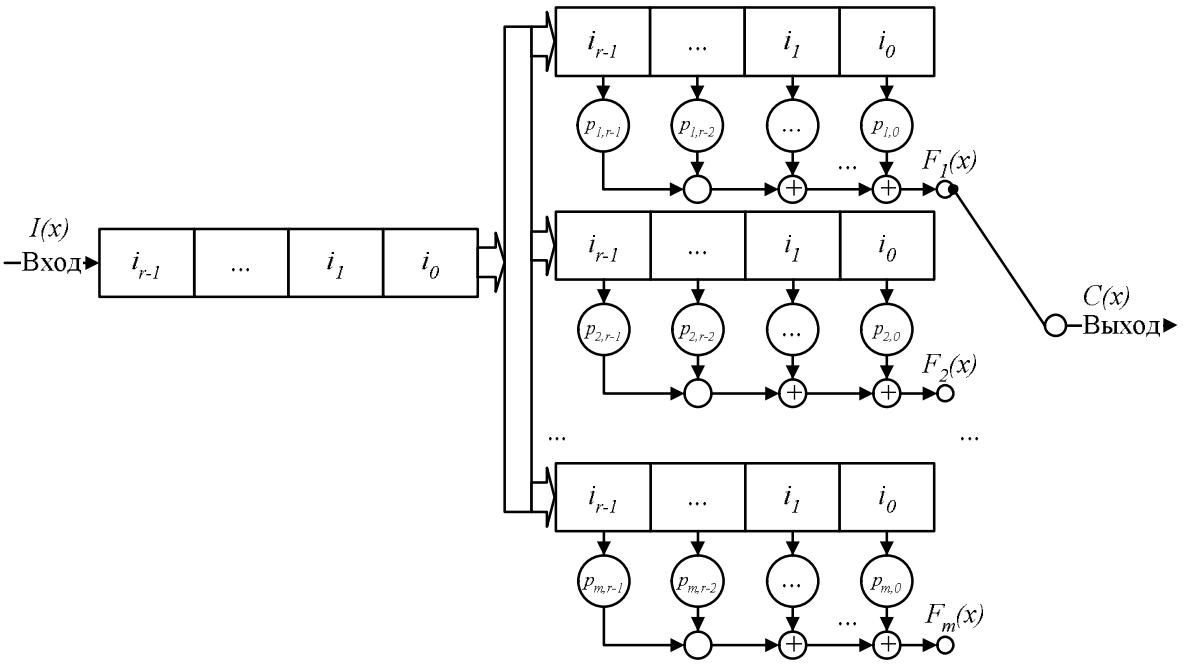

Рис. 2. Несистематический сверточный кодер, $R = 1/m$

Для описания процесса кодирования информации несистематическим сверточным кодером воспользуемся подходом, состоящим в формальном определении сверточного кода через недвоичный циклический код над $GF(q^m)$, где степень расширения поля m соответствует числу q-ичных многочленов сверточного кода. Пусть многочлен

$$I(x) = i_{r-1}x^{r-1} + i_{r-1}x^{r-1} + \ldots + i_1 x + i_0 \qquad (1)$$

является информационной последовательностью, подлежащей кодированию, а многочлены:

$$P_1(x) = p_{1,r-1}x^{r-1} + p_{1,r-2}x^{r-2} + \ldots + p_{1,1}x + p_{1,0};$$

$$P_2(x) = p_{2,r-1}x^{r-1} + p_{2,r-2}x^{r-2} + \ldots + p_{2,1}x + p_{2,0}; \qquad (2)$$

$$\ldots$$

$$P_m(x) = p_{m,r-1}x^{r-1} + p_{m,r-2}x^{r-2} + \ldots + p_{m,1}x + p_{m,0}$$

будут порождающими многочленами данного сверточного кода. Информационная последовательность $I(x)$ вида (1) поступает в кодер сверточного кода, где происходит ее умножение на многочлены $P_1(x)$ ... $P_m(x)$ вида (2) и получение последовательностей $F_1(x)$ ... $F_m(x)$ соответственно:

$$F_1(x) = I(x)P_1(x) = s_{1,2r-2}x^{2r-2} + \ldots + s_{1,1}x + s_{1,0};$$

$$F_2(x) = I(x)P_2(x) = s_{2,2r-2}x^{2r-2} + \ldots + s_{2,1}x + s_{2,0}; \qquad (3)$$

$$\ldots$$

$$F_m(x) = I(x)P_m(x) = s_{m,2r-2}x^{2r-2} + \ldots + s_{m,1}x + s_{m,0},$$

где $s_{i,j}$ – коэффициент в многочлене $F_i(x)$ при x^j, полученный в результате преобразования коэффициентов многочленов $I(x)$ и $P_i(x)$ при их перемножении над $GF(q)$.

Кодовое слово $C(x)$ формируется путем последовательного считывания символов при одинаковых степенях многочленов $F_1(x)$ ... $F_m(x)$, т.е.

$$C(x) = \left(s_{1,2r-2}, s_{2,2r-2}, \ldots, s_{m,2r-2}\right)x^{2r-2} + \ldots + \left(s_{1,0}, s_{2,0}, \ldots, s_{m,0}\right).$$

Если на вход сверточного кода подать информационный вектор вида {0, 0, …, 1}, то информационный многочлен запишется как $I(x)$=1, а кодовое слово запишется в виде

$$P(x) = \left(p_{1,r-1}, p_{2,r-1}, \ldots, p_{m,r-1}\right)x^{r-1} + \ldots + \left(p_{1,0}, p_{2,0}, \ldots, p_{m,0}\right). \qquad (4)$$

Последнее выражение однозначно определяет несистематическое правило сверточного кодирования.

Рассмотрим конечное поле $GF(q^m)$, построенное по кольцу многочленов с коэффициентами над $GF(q)$. В (4) каждому набору $\{p_{1,i}, p_{2,i}, \ldots, p_{m,i}\}$ сопоставим элемент поля $\beta_i \in GF(q^m)$ такой, что

$$\beta_i = p_{1,i} + p_{2,i}x + \ldots + p_{m,i}x^m.$$

Выражение (5) перепишем в виде

$$P(x) = \beta_{r-1}x^{r-1} + \beta_{r-2}x^{r-2} + \ldots + \beta_1 x + \beta_0. \qquad (5)$$

Если выражение (6) суть порождающий многочлен недвоичного (N, K, D) циклического кода над $GF(q^m)$, то справедлива следующая теорема [5 – 8].

Теорема 1. Несистематический сверточный код над $GF(q)$ (рис. 2) с $R = 1/m$ однозначно задается многочленом $P(x)$ над $GF(q^m)$ вида (5). Если многочлен (5) задает недвоичный (N, K, D) циклический код над $GF(q^m)$, то он однозначно определяет (n, k) несистематический сверточный код над $GF(q)$ с параметрами: $k^0 = 1$; $n^0 = m$; $\nu = r \cdot k^0 = r$; $k = r + 1$; $n = (r + 1) \cdot n^0 = k \cdot m$; $R = 1/m$; $d_\infty \geq D$; $C(x) = I(x) \cdot P(x)$.

Доказательство. Действительно, недвоичный (N, K, D) циклический код над $GF(q^m)$, порожденный многочленом $P(x)$ степени r, однозначно определяет набор регистров сдвига, соединенных связями (рис. 2), и задает рекуррентное правило кодирования, т.е. однозначного соответствия входной (информационной) последовательности кодовой (выходной) последовательности: $C(x) = I(x) \cdot P(x)$. Параметры несистематического кода соответствуют рассмотренному выше примеру (рис. 2), т.е. $k^0 = 1$, $n^0 = m$. Степень r порождающего многочлена $P(x)$ циклического (N, K, D) кода над $GF(q^m)$ задает длину регистра сдвига и соответственно число хранящихся в кодере информационных кадров. Следовательно, длина кодового ограничения ν, конструктивные параметры n и k и скорость R сверточного кода определяются, соответственно, выражениями:

$\nu = r \cdot k^0 = r;\ k = r + 1;\ n = (r+1) \cdot n^0 = k \cdot m;\ R = 1/m.$

Если на вход кодера подать информационный блок данных длиной K q-ичных символов, то считанная с выхода кодовая последовательность длиной N q^m-ичных символов – кодовое слово циклического (N, K, D) кода над $GF(q^m)$. Следовательно, два любых кодовых блока, соответствующих двум произвольным входным последовательностям длиной K q-ичных символов, будут отличаться, по крайней мере, в D q^m-ичных символов. Последовательное считывание символов при одинаковых степенях многочленов $F_1(x)$ ... $F_m(x)$ суть отображение элементов поля $GF(q^m)$ в элементы образующего поля $GF(q)$, которое не уменьшает кодовое расстояние между произвольными q-ичными кодовыми словами длины $N \cdot m$. По условию теоремы, длина информационного кадра $k^0 = 1$, следовательно, для кодовых слов, соответствующих K различным информационным кадрам $d_K \geq D$. По определению дистанционного профиля непрерывных кодов выполняется равенство $d = d_{r+1} \leq d_{r+2} \leq \ldots \leq d_\infty$. Если выполняется условие $K \leq r$, то, очевидно, $d_\infty \geq d \geq d_K$. Если $K > r$, то выполняется лишь равенство $d_\infty \geq d_K$, что и завершает доказательство.

Рассмотренное обобщение несистематического сверточного (n, k) кода и результат теоремы 1 позволяют алгебраически задавать параметры сверточного кода для произвольной длины кодового ограничения. С использованием такого подхода в работах [5 – 7] подробно рассмотрены алгоритмы формирования порождающих многочленов сверточного кода и алгебраические алгоритмы построения двоичных сверточных кодов на их основе. Отметим, что в результате выполнения этих алгоритмов удается упростить процедуру построения сверточных кодов с предварительной оценкой их параметров. Уточнение кодового расстояния (условие $d_\infty \geq D$) позволяет, как правило, улучшить кодовые характеристики. К сожалению, рассмотренный алгебраический метод позволяет строить сверточные коды только для скорости $R = 1 / m$, где m – степень расширения базового поля, над которым задается порождающий многочлен циклического кода. Это обстоятельство сужает область практического использования рассмотренного метода. Кроме того, наибольший энергетический выигрыш от кодирования большинство линейных кодов дает при скорости $R \approx 1/2 – 2/3$ [1 – 4].

2. Алгебраический метод построения сверточных кодов для $R = k^0/m$

Для снятия ограничения по скорости кодирования предлагается алгебраический метод построения сверточных кодов, в основе которого лежит ограничение недвоичного циклического кода над $GF(q^m)$ на произвольное подмножество $H \subseteq GF(q^m)$, $|H| \geq |GF(q)|$. Если $|H| = |GF(q)|$, получим, как частный случай, вышеизложенный метод.

Рассмотрим несистематический сверточный (n, k)-код над $GF(q)$ со скоростью $R = k^0 / m$, кодер которого представлен на рис. 3. Разобьем входную информационную последовательность на информационные кадры по $k^0 \geq 1$ символов, каждый символ которых принадлежит $GF(q)$. В общем случае информационная последовательность может быть бесконечной длины, т.е. состоять из бесконечного числа информационных кадров по k^0 символов. Сопоставим каждому информационному кадру из k^0 символов один символ из множества $H \subseteq GF(q^m)$, $|H| \geq |GF(q)|$. Запишем информационный многочлен в виде

$$I(x) = I_{r-1}x^{r-1} + I_{r-1}x^{r-1} + \ldots + I_1 x + I_0, \qquad (6)$$

где $I_j \in H,\ j = 0,\ldots, r–1;\ log_q |H| = k^0,\ m \geq k^0$.

Пусть многочлены $P_1(x)$, $P_2(x)$, ..., $P_m(x)$ – порождающие многочлены представленного на рис. 3 несистематического сверточного кодера. Информационная последовательность $I(x)$ вида (6) поступает в кодер (рис. 3), где происходит ее умножение на многочлены $P_1(x)$ ... $P_m(x)$ вида (2).

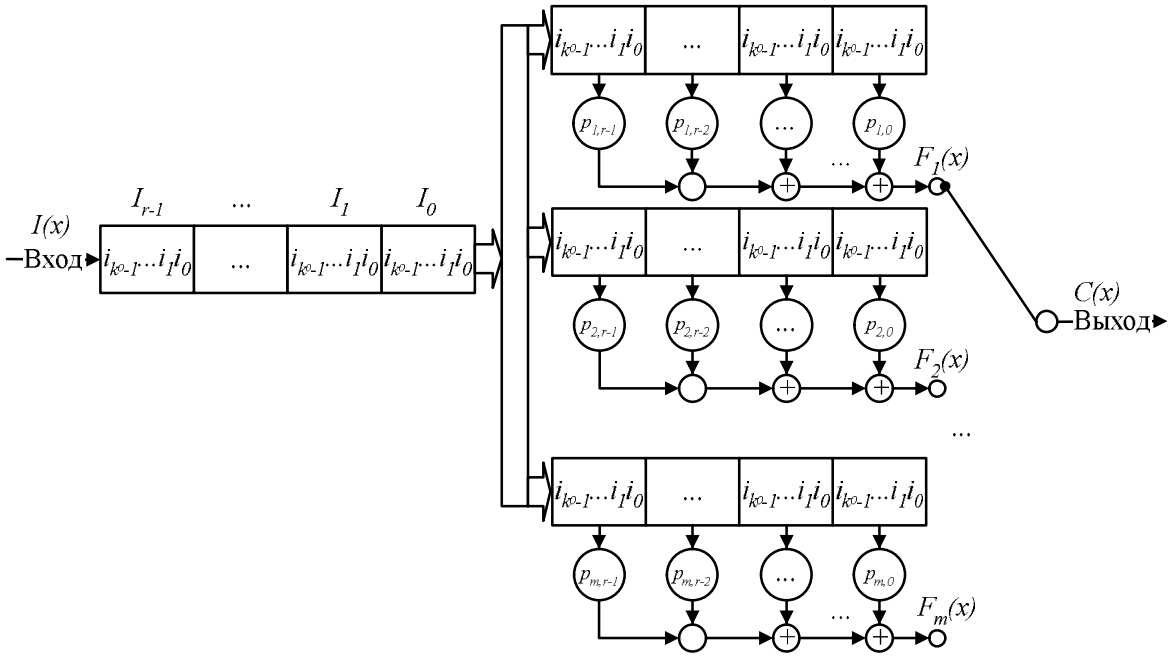

Рис. 3. Несистематический сверточный кодер, $R=k^0/m$

Получим последовательности $F_1(x)$ ... $F_m(x)$:

$$F_1(x) = I(x)P_1(x) = S_{1,2r-2}x^{2r-2} + ... + S_{1,1}x + S_{1,0};$$

$$F_2(x) = I(x)P_2(x) = S_{2,2r-2}x^{2r-2} + ... + S_{2,1}x + S_{2,0}; \quad (7)$$

…

$$F_m(x) = I(x)P_m(x) = S_{m,2r-2}x^{2r-2} + ... + S_{m,1}x + S_{m,0},$$

где $S_{i,j}$ – коэффициент в многочлене $F_i(x)$ при x^j, полученный в результате преобразования коэффициентов многочленов $I(x)$ вида (6) и $P_i(x)$ вида (2) при их перемножении над $GF(q)$. Кодовое слово $C(x)$ формируется путем последовательного считывания символов при одинаковых степенях многочленов $F_1(x)$ ... $F_m(x)$, т.е.

$$C(x) = (S_{1,2r-2},...,S_{m,2r-2})x^{2r-2} + ... + (S_{1,0},...,S_{m,0}). \quad (8)$$

Если на вход сверточного кода подать информационный вектор вида {0, 0, …, 1}, то информационный многочлен запишется как $I(x) = 1$, а кодовое слово (8) запишется в виде порождающего многочлена циклического кода, т.е. $C(x) = P(x)$. Таким образом, порождающий многочлен циклического кода однозначно определяет несистематическое правило сверточного кодирования. Справедлива следующая теорема.

Теорема 2. Зафиксируем конечное множество H элементов поля $GF(q^m)$, причем $\log_q |H| = k^0$, $m \geq k^0$. Тогда произвольный многочлен степени r с коэффициентами над $GF(q^m)$ полностью определяет несистематический сверточный (n, k) код над $GF(q)$ с информационным кадром длины k^0 и параметрами:

$$n^0 = m; \quad \nu = r \cdot k^0; \quad k = (r+1)\cdot k^0;$$

$$n = k \cdot n^0/k^0; \quad R = k^0/m; \quad m \geq k^0.$$

Доказательство. Кодирование, по определению, представляет собой процесс однозначного сопоставления (соответствия) информационной и кодовой последовательностей. Пусть задан произвольный многочлен $P(x)$ над $GF(q^m)$ степени r вида (5) и входная последовательность над $GF(q)$. Представим информационную последовательность в виде многочлена (6) с коэффициентами над H, т.е. коэффициенты многочлена $I(x)$ в выражении (7) являются многочленами над $GF(q)$ степени $m - 1$:

$$I_j = z_{m-1}x^{m-1} + ... + z_{k^0}x^{k^0} + ... + z_1x + z_0, \quad (9)$$

где $z_i \in GF(q)$, причем $m - k^0$ коэффициентов z_i равны нулю. Положим, для определенности, $z_i = 0$ для $i = k^0, ..., m - 1$. Первые k^0 элементов z_i в выражении

(9) образуют информационный кадр k^0 символов над $GF(q)$. Определенное таким образом отображение символов $GF(q)$ в символы $GF(q^m)$ является однозначным соответствием.

Недвоичный (N, K, D) циклический код над $GF(q^m)$, порожденный многочленом $P(x)$ степени r однозначно определяет набор регистров сдвига соединенных связями (рис. 3) и задает рекуррентное правило кодирования, т.е. однозначное соответствие входной (информационной) и кодовой (выходной) последовательности: $C(x) = I(x) \cdot P(x)$. Параметры несистематического кода соответствуют рассмотренному выше примеру (рис. 3), т.е. каждому информационному кадру длиной k^0 символов над $GF(q)$ (или, что эквивалентно, каждому символу из множества H) ставится в соответствие кадр кодовых символов длиной n^0. Степень r порождающего многочлена $P(x)$ циклического (N, K, D) кода над $GF(q^m)$ задает длину регистра сдвига и, соответственно, число хранящихся в кодере информационных кадров. Следовательно, длина кодового ограничения ν, конструктивные параметры n и k и скорость R сверточного кодирования определяются, соответственно, следующими выражениями:

$\nu = r \cdot k^0$ $k = (r + 1) \cdot k^0$; $n = k \cdot n^0 / k^0$; $R = k^0 / m$; $m \geq k^0$.

Лемма 1. Если существует такое целое w, что $m = w \cdot k^0$, то порождающий многочлен степени r (N, K, D) циклического кода над $GF(q^m)$ полностью определяет несистематический сверточный (n_*, k_*, d_*) код над $GF\left(q^{k^0}\right)$ с параметрами: $k_*{}^0 = 1$; $n_*{}^0 = m$; $\nu_* = r \cdot k_*{}^0 = r$; $k_* = r_* + 1$; $n_* = (r + 1) \cdot n_*{}^0 = k_* \cdot m_*$; $R = 1 / w$; $C(x) = I(x) \cdot P(x)$.

Доказательство. Согласно теореме 2, произвольный многочлен степени r с коэффициентами над $GF(q^m)$ полностью определяет несистематический сверточный (n, k, d) код над $GF(q)$ с кодовым ограничением ν, причем $n^0 = m$, $\nu = r \cdot k^0$, $k = (r + 1) \cdot k^0$, $n = k \cdot n^0 / k^0$, $R = k^0 / m$, $m \geq k^0$, $k^0 = log_q |H|$, $H \subseteq GF(q^m)$. Если каждый информационный кадр длиной k^0 q-ичных символов представить одним q^{k^0}-ичным символом, то получим несистематический сверточный (n_*, k_*, d_*) код над $GF\left(q^{k^0}\right)$, где $GF\left(q^{k^0}\right)$ изоморфно множеству H. На вход такого кодера поступает K информационных кадров по одному q^{k^0}-ичному символу, следовательно, $k_*{}^0 = 1$. С выхода кодера снимается кодовая последовательность длиной N q^m-ичных символов. Если при этом выполняется равенство $m = w \cdot k^0$ для произвольного целого w, то $n_*{}^0 = w$. Тогда, очевидно, выполняются равенства: $\nu = r$, $k = r + 1$, $n = k \cdot w$, $R = 1/w$, а по теореме 2: $C(x) = I(x) \cdot P(x)$, что соответствует обобщению теоремы 1 на случай несистематических сверточных кодов над $GF\left(q^{k^0}\right)$.

Лемма 2. Если $|H| = |GF(q)|$ получим, как частный случай теоремы 2, алгебраически заданный сверточный код для $R = 1/m$, что соответствует результату теоремы 1.

Доказательство. Действительно, если $|H| = |GF(q)|$, то по теореме 2 получим $k^0 = 1$. Следовательно, процесс сверточного кодирования соответствует ограничению поля $GF(q^m)$ на подполе $GF(q)$ и $k^0 = 1$, $n^0 = m$, $\nu = r \cdot k^0 = r$, $k = r + 1$, $n = k \cdot n^0 / k^0$, $R = 1 / m$, $C(x) = I(x) \cdot P(x)$, что соответствует результату теоремы 1.

Лемма 3. Если $q = 2^{m^*}$ то получим, как частный случай теоремы 2, алгебраически заданный двоичный сверточный код с $R = k^0/u$, причем $u = m \cdot m^*$.

Доказательство. По теореме 2 имеем несистематический сверточный (n, k, d) код над $GF(q)$ с кодовым ограничением $\nu = r \cdot k^0$ и параметрами: $n = k \cdot n^0 / k^0$, $k = (r + 1) \cdot k^0$, $R = k^0 / m$. Если на вход такого кодера подать информационный кадр из $m^* \cdot k^0$ двоичных символов (что эквивалентно подаче кадра из k^0 q-ичных символов), а снятый с выхода

кадр кодового слова – q^m-ичный символ преобразовать в $m \cdot m^*$ бит, получим однозначное отображение – двоичное правило кодирования. Подставив эти параметры в результат теоремы 2, получим: длина двоичного информационного кадра $k_2^0 = m^* \cdot k^0$; $n_2^0 = u$; $\nu_2 = r \cdot m^* \cdot k^0$; $k_2 = (r+1) \cdot m^* \cdot k^0$; $n_2 = k \cdot n^0 / (m^* \cdot k^0)$; $R = m^* \cdot k^0 / u$; $u \ge m^* \cdot k^0$; $k^0 = log_q |H|$; $H \subseteq GF(q^m)$.

Теорема 3. Порождающий многочлен степени r (N, K, D) циклического кода над $GF(q^m)$ полностью определяет несистематический сверточный (n, k, d)-код над $GF(q)$ с кодовым ограничением $\nu = r \cdot k^0$ и параметрами: $n = k \cdot n^0 / k^0$, $k = (r+1) \cdot k^0$, $R = k^0 / m$, $d_\infty \ge D$.

Доказательство. Согласно теореме 2, произвольный многочлен степени r с коэффициентами над $GF(q^m)$ полностью определяет несистематический сверточный (n, k, d) код над $GF(q)$ (рис. 3) с кодовым ограничением ν, причем $n^0 = m$, $\nu = r \cdot k^0$, $k = (r+1) \cdot k^0$, $n = k \cdot n^0 / k^0$, $R = k^0 / m$, $m \ge k^0$, $k^0 = log_q |H|$, $H \subseteq GF(q^m)$.

Если на вход устройства (рис. 3) подать K информационных кадров по k^0 q-ичных символов (что эквивалентно подаче K кадров по одному q^{k^0}-ичному символу), то снятая с выхода кодовая последовательность длиной N q^m-ичных символов суть кодовое слово циклического (N, K, D) кода над $GF(q^m)$. Следовательно, два любых кодовых блока, соответствующих двум произвольным входным последовательностям длиной K q^{k^0}-ичных символов будут отличаться, по крайней мере, в D q^m-ичных символов. Последовательное считывание символов при одинаковых степенях многочленов $F_1(x)$ ... $F_m(x)$ суть отображение элементов поля $GF(q^m)$ в элементы образующего поля $GF(q)$, которое не уменьшает кодовое расстояние между произвольными q-ичными кодовыми словами длины $N \cdot m$. По условию теоремы длина информационного кадра равна k^0, следовательно, $d_K \ge D$. По определению дистанционного профиля непрерывных кодов выполняется равенство $d = d_{r+1} \le d_{r+2} \le \ldots \le d_\infty$. Если выполняется условие $K \le r$, то, очевидно, $d_\infty \ge d \ge d_K$. Если $K > r$, то выполняется лишь неравенство $d_\infty \ge d_K$, что и завершает доказательство.

Результаты теорем 1 – 3 позволяют алгебраически задавать несистематический сверточный код порождающим многочленом циклического кода с предварительной оценкой его конструктивных параметров. Основным недостатком рассмотренного подхода построения сверточных кодов является низкая конструктивная величина свободного минимального расстояния [8 – 9]. Ниже предлагается подход по предсказанию (прогнозированию) свободного кодового расстояния несистематических сверточных кодов, заданных с помощью порождающего многочлена циклического кода.

Предложение. Предсказанное (прогнозируемое) свободное минимальное расстояние $d_П$ несистематического сверточного (n, k, d) кода над $GF(q)$, алгебраически заданного порождающим многочленом (N, K, D) циклического кода над $GF(q^m)$ определяется выражением

$$d_П = mD(q^m - q^{m-1})/(q^m - 1).$$

Вывод этого выражения основан на подсчете ненулевых q-ичных символов в выходной кодовой последовательности несистематического сверточного (n, k, d) кода, алгебраически заданного с помощью порождающего многочлена (N, K, D) циклического кода над $GF(q^m)$. По теоремам 1 – 2, несистематический сверточный код эквивалентен ограничению недвоичного циклического кода над $GF(q^m)$ на подполе $GF(q)$, т.е. отображению символов кодовых слов циклического кода над $GF(q^m)$ в символы сверточного кода над $GF(q)$. Мощность множества прообразов равна q^m, а без нулевого символа поля $GF(q^m)$ мощность множества ненулевых прообразов равна $q^m - 1$. Каждому символу над $GF(q^m)$ соответствует m q-ичных символов, т.е. мощность множества образов равна $m \cdot q^m$. Количество ненулевых q-ичных символов в множестве образов равно $m \cdot (q^m - q^{m-1})$. Таким

образом, при алгебраическом построении сверточных кодов множество из $q^m - 1$ ненулевых символов над $GF(q^m)$ отображаются в множество из $m \cdot (q^m - q^{m-1})$ ненулевых q-ичных символов. Следовательно, среднее число ненулевых q-ичных символов на выходе несистематического сверточного кода будет определяться как $m \cdot D \cdot (q^m - q^{m-1})/(q^m - 1)$, где D – минимальное кодовое расстояние (N, K, D) циклического кода над $GF(q^m)$.

Алгоритм построения сверточного (n, k, d) кода над $GF(q)$ определим в виде последовательности следующих шагов.

ШАГ 1. Выбор конструктивных параметров сверточного кода над $GF(q)$.

ШАГ 2. Расчет параметров образующего поля $GF(q^m)$. Выбор циклического кода, расчет его конструктивных (N, K, D) параметров над $GF(q^m)$.

ШАГ 3. Выбор порождающего многочлена циклического (N, K, D) кода $GF(q^m)$. Расчет прогнозируемого свободного расстояния $d_П$ сверточного кода.

ШАГ 4. Определение порождающих многочленов несистематического сверточного (n, k, d) кода, построение схемы кодера.

ШАГ 5. Уточнение минимального кодового расстояния и свободного кодового расстояния несистематического сверточного (n, k, d) кода.

После ввода конструктивных параметров сверточного (n, k, d) кода над $GF(q)$ – параметров ν, n^0, k^0 и q, на втором шаге алгоритма выполняется расчет параметров образующего поля $GF(q^m)$, осуществляется выбор циклического кода и расчет его конструктивных (N, K, D) параметров над $GF(q^m)$. Для этого выражения, связывающие параметры сверточного и циклических кодов, перепишем в виде: $R = k^0 / n^0$, $m = n^0$, $r = \nu / k^0$, $D \le d_\infty$. После расчета параметров образующего поля $GF(q^m)$ необходимо выбрать циклический код, порождающий многочлен которого будет задавать сверточный код.

Рассмотрим случай, когда в качестве циклического кода выбран примитивный код БЧХ. Для расчета его конструктивных (N, K, D) параметров зафиксируем двучлен $(x^M - 1)$ так, что конструктивная длина примитивного кода БЧХ равна $N = (q^m)^M - 1$. Далее, определив степень r порождающего многочлена примитивного кода БЧХ, рассмотрим поле разложения двучлена $(x^M - 1)$ на минимальные многочлены элементов поля $GF((q^m)^M)$ над $GF(q^m)$. Порождающий многочлен примитивного кода БЧХ задается в виде $P(x) = HOK(f_1, f_2, ..., f_{2t})$, где t – число ошибок, которые должен исправлять циклический (N, K, D) код; $N = (q^m)^M - 1$; $r = degP(x)$; $K = N - r$; $D = 2t + 1$; f_i – минимальные многочлены над $GF(q^m)$ элементов $\alpha^i \in GF((q^m)^M)$ [1 – 2]. После расчета $d_П$ третий шаг алгоритма для примитивных кодов БЧХ завершен.

Рассмотрим случай, когда выбран непримитивный код БЧХ. Длина непримитивного кода БЧХ равна одному из сомножителей в разложении числа $(q^m)^M - 1$ (если число $(q^m)^M - 1$ не является простым), т.е. $N = ((q^m)^M - 1)/g$ для произвольного целого g делящего нацело $(q^m)^M - 1$ [1 – 2]. Очевидно, что должно выполняться также условие $r < N$. Порождающий многочлен непримитивного кода БЧХ задается в виде $P(x) = HOK(\varphi_1, \varphi_2, \ldots, \varphi_{2t})$, где t – число ошибок, которые должен исправлять циклический (N, K, D) код; $N = ((q^m)^M - 1)/g$; $r = degP(x)$; $K = N - r$; $D = 2t + 1$; φ_I – минимальные многочлены над $GF(q^m)$ элементов $\beta^i \in GF((q^m)^M)$ такие, что их порядок равен N, т.е. $\beta^j = \alpha^{jg}$, $j = 1, \ldots, M/2$. После расчета $d_П$ третий шаг алгоритма для непримитивных кодов БЧХ завершен.

Рассмотрим случай, когда в качестве циклического кода выбран код РС. Порождающий многочлен кода РС задается в виде: $P(x) = (x - \alpha^i) \cdot (x - \alpha^{2i}) \cdot \ldots \cdot (x - \alpha^{2ti})$, где t – число ошибок, которые должен исправлять (N, K, D) код РС; $N = q^m - 1$; $r = degP(x)$; $K = N - r$; $D = 2t + 1$; $\alpha^i \in GF(q^m)$ [1 – 2]. После вычисления (N, K, D) параметров кода РС, выбора порождающего многочлена и расчета $d_П$ третий шаг алгоритма для рассмотренного случая завершен.

На четвертом шаге определяются порождающие многочлены сверточного кода над $GF(q)$, строится схема кодера. Коэффициенты многочленов $P_1(x)$ ... $P_m(x)$ однозначно определяют регистр сдвига, т.е. однозначно задают схему кодера искомого сверточного (n ,k, d) кода. На пятом шаге путем тестирования производится уточнение кодового расстояния (при необходимости).

Приведем *пример*. Зафиксируем $GF(2^3)$ и рассмотрим коды РС с параметрами: $N = 2^3 - 1 = 7$, $7 - K = D - 1$. В табл. 1 представлены параметры кодов РС над $GF(2^3)$, конструктивные параметры сверточных (n, k, d) кодов, алгебраически заданных порождающим многочленом кода РС и предсказанное значение свободного кодового расстояния.

Таблица 1

Конструктивные характеристики двоичных сверточных кодов

(N, K, D)	(n, k, d)	v	R	$d_П$
(7, 1, 7)	(21, 7, 7)	6	1 / 3	12
	(21, 14, 7)	12	2 / 3	12
(7, 2, 6)	(18, 6, 6)	5	1 / 3	10,3
	(18, 12, 6)	10	2 / 3	10,3
(7, 3, 5)	(15, 5, 5)	4	1 / 3	8,6
	(15, 10, 5)	8	2 / 3	8,6
(7, 4, 4)	(12, 4, 4)	3	1 / 3	6,9
	(12, 8, 4)	6	2 / 3	6,9
(7, 5, 3)	(9, 3, 3)	2	1 / 3	5,1
	(9, 6, 3)	4	2 / 3	5,1
(7, 6, 2)	(6, 2, 2)	1	1 / 3	3,4
	(6, 4, 2)	2	2 / 3	3,4

Выводы

Разработан метод алгебраического построения сверточных кодов над $GF(q)$, позволяющий однозначно представить несистематический сверточный код через порождающий многочлен недвоичного циклического кода. Результаты теорем 1 – 3 связывают параметры сверточного кода с кодовыми характеристиками недвоичного циклического кода и позволяют алгебраически определять коды с заранее заданными конструктивными свойствами. Предложен конструктивный подход по предсказанию (прогнозированию) свободного кодового расстояния несистематических сверточных кодов, заданных с помощью порождающего многочлена циклического кода. Разработан практический алгоритм алгебраического построения сверточных кодов, приведен пример его использования.

Литература

1. Мак-Вильямс Ф., Слоэн Н. Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.

2. Кларк Дж. мл., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи. – М.: Радио и связь, 1987. – 392 с.

3. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер.с англ. – М.: Мир, 1986. – 576 с.

4. Касами Т., Токура Н., Ивадари Е., Инагаки Я. Теория кодирования. – М.: Мир, 1978. – 576 с.

5. Краснобаев В.А., Приходько С.И., Снисаренко А.Г. Помехоустойчивое кодирование в АСУ. – Х.: ХВВКИУРВ, 1990. – 155 с.

6. Приходько С.И. Алгебраические сверточные коды // Інформаційно-керуючі системи на залізничному транспорті. – Х.: ХарДАЗТ. – № 2. – 1999. – С. 62 – 64.

7. Приходько С.И. Алгебраические процедуры декодирования сверточных кодов // Современные методы кодирования в электронных системах. Материалы международной НТК 23 – 24 апреля 2002. – Сумы: СМКЭС. – 2002. – С. 11 – 12.

8. Приходько С.И., Кузнецов А.А., Гусев С.А. Алгебраический метод сверточного кодирования // Современные методы кодирования в электронных системах. Материалы междунар. НТК 26 – 27 октября 2004. – Сумы: СМКЭС. – 2004. – С. 11 – 12.

Поступила в редакцию 16.12.2004

Рецензент: д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет «ХАИ», Харьков.