УДК 621.391

А.А. КУЗНЕЦОВ, А.И. ТИМОЧКО, С.И. ПРИХОДЬКО, А.С. ПОСТОЛЬНЫЙ

Харьковский университет Воздушных Сил, Украина

АЛГЕБРАИЧЕСКИЙ МЕТОД ПОСТРОЕНИЯ РЕКУРСИВНЫХ СВЕРТОЧНЫХ КОДОВ ДЛЯ СТАНДАРТОВ КОСМИЧЕСКОЙ СВЯЗИ

Предлагается алгебраический метод построения рекурсивных сверточных кодов в несистематическом виде. Получены аналитические выражения, устанавливающие связь между параметрами недвоичных циклических кодов и алгебраически заданных рекурсивных сверточных кодов в несистематическом виде.

рекурсивный сверточный код, порождающий многочлен, циклический код

1. Постановка проблемы в общем виде, анализ литературы

Важным показателем эффективности спутниковых систем связи является помехоустойчивость, т.е. способность системы функционировать в условиях воздействия помех всех видов. Мощным средством борьбы с ошибками в каналах спутниковой связи является помехоустойчивое кодирование. Перспективным направлением в его развитии является разработка и исследование параллельных каскадных схем с рекурсивными сверточными кодами, т.н. турбокодов (ТК).

В настоящее время ТК утверждены несколькими стандартами космической связи [1 – 4]: в 1999 г. американским комитетом CCSDS (Consultative Committee for Space Data Systems) в стандарте передачи телеметрической информации с космических аппаратов [1]; в феврале 2000 г. консорциумом DVB в стандарте DVB-RCS [2 – 4] для передачи информации по обратному спутниковому каналу (Return Channel for Satellite — RCS), т.е. в направлении от спутника к абоненту; в новом стандарте спутниковой системы связи Inmarsat. Кроме того, компанией TurboConcept в партнерстве с европейским спутниковым оператором Eutelsat разработан турбодекодер TC1000 в соответствии со стандартом DVB-RCS. Широкое применение ТК обусловлено их высокой энергетической эффективностью, которая приближается, в некоторых случаях, к теоретическому пределу [5, 6]. Однако отсутствие регулярных алгебраических алгоритмов построения рекурсивных сверточных кодов с хорошими конструктивными параметрами и большой длиной кодового ограничения сдерживает дальнейшее развитие ТК. Большинство хороших сверточных кодов получено переборным методом [7, 8], сложность которого растет экспоненциально. Следовательно, разработка и исследование алгебраических методов построения рекурсивных сверточных кодов является актуальной научно-технической задачей, имеющей важное научное и прикладное значение для повышения качества спутниковой связи путем совершенствования стандартов и протоколов помехоустойчивого кодирования.

2. Алгебраические методы построения сверточных кодов

Сверточные коды принадлежат подклассу древовидных линейных кодов и являются в общетеоретическом плане обобщением линейных блоковых кодов на случай бесконечной длины. В то же время, в отличие от блоковых кодов, развитие которых шло преимущественно с использованием алгебраических методов, большинство хороших сверточных кодов получено переборным методом. В этом смысле сверточные коды относят преимущественно к случайным непрерывным кодам [7, 8]. Существенным преимуществом сверточных кодов является их энергетическая эффективность, существенно превосходящая энергетический выигрыш от кодирования большинства линейных блоковых кодов. Полученные верхние и нижние границы для вероятности ошибки при декодировании методом Витерби показывают, что кодовые характеристики сверточных кодов лучше, чем у блоковых кодов той же длины [7 – 10]. Строгое доказательство и вывод границ Витерби приведено в [9, 10].

Недостатком большинства известных методов построения сверточных кодов является быстрый рост сложности переборного алгоритма. Так, для сверточного кода с длиной кодового ограничения v, выходная последовательность зависит от v входных символов, 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 v ячейками (рис. 1).

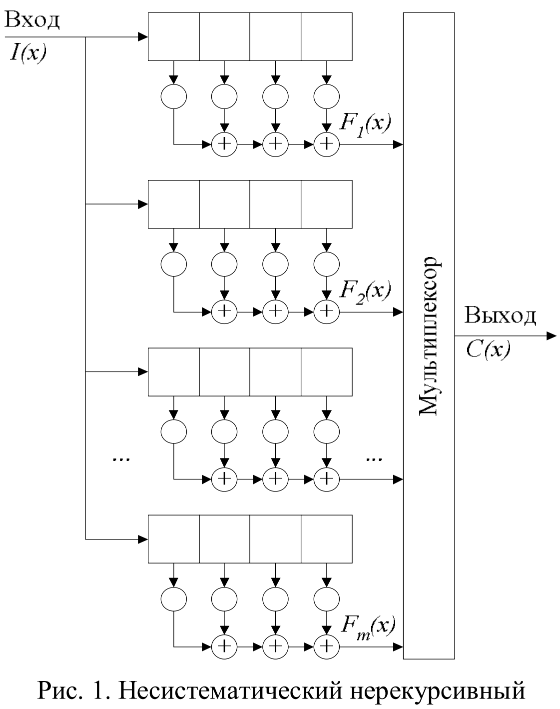

Рис. 1. Несистематический нерекурсивный сверточный кодер

Действительно, если сверточный код представить в полиномиальном виде через порождающие многочлены $g_1(x)$, $g_2(x)$, …, $g_m(x)$ следующего вида:

$$g_1(x) = g_{1,r-1}x^{r-1} + g_{1,r-2}x^{r-2} + \ldots + g_{1,1}x + g_{1,0}\,;$$
$$g_2(x) = g_{2,r-1}x^{r-1} + g_{2,r-2}x^{r-2} + \ldots + g_{2,1}x + g_{2,0}\,; \quad (1)$$
$$\ldots$$
$$g_m(x) = g_{m,r-1}x^{r-1} + g_{m,r-2}x^{r-2} + \ldots + g_{m,1}x + g_{m,0}\,,$$

то сверточный кодер (рис. 1) будет представлять собой цепь регистров сдвига с отводами, заданными коэффициентами порождающих многочленов (1). Запишем информационную последовательность в виде многочлена

$$I(x) = I_{r-1}x^{r-1} + I_{r-1}x^{r-1} + \ldots + I_1 x + I_0\,, \qquad (2)$$

где I_j – информационные кадры, причем $I_j = \{i_1, i_2, \ldots, i_{k0}\}$ и в большинстве случаев $k^0 = 1$.

Кодовое слово $C(x)$ формируется путем последовательного считывания символов при одинаковых степенях многочленов:

$$F_1(x) = I(x)g_1(x); \quad \ldots\,; F_m(x) = I(x)g_m(x).$$

Следовательно, для полного перебора всех возможных сверточных кодов с кодовым ограничением $v = r \cdot k^0$ следует перебрать, как минимум,

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

вариантов, где r – максимальная степень порождающих многочленов $g_1(x)$, $g_2(x)$, …, $g_m(x)$ сверточного кода; k^0 – длина информационного кадра; q – мощность ансамбля кодовых символов.

Даже для небольших r, k^0 и q сложность переборного алгоритма неприемлемо высока.

Другой подход построения сверточных кодов состоит в использовании мощного математического аппарата циклических кодов и обобщении их до бесконечной длины.

В работах [11 – 14] предложен конструктивный метод алгебраического построения нерекурсивных сверточных кодов в несистематическом виде со скоростью кодирования $R = 1/m$, где m – степень расширения базового поля $GF(q^m)$, над которым фиксируется циклический код. Конструктивные параметры построенного таким образом сверточного кода определяются следующей теоремой.

Теорема 1 [14]. Несистематический сверточный код над $GF(q)$ (рис. 1) с $R = 1/m$ однозначно задается многочленом $g(x)$ над $GF(q^m)$. Если многочлен $g(x)$ 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: $k^0 = 1$; $n^0 = m$; $\nu = r \cdot k^0 = r$; $k = r + 1$; $n = (r + 1) \cdot n^0 = k \cdot m$; $R = 1 / m$; $d_\infty \geq D$; $C(x) = I(x) \cdot P(x)$.

Теорема 1 дает мощный механизм для алгебраического построения сверточных кодов. Действительно, зная порождающий многочлен

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

недвоичного (N, K, D) циклического кода над $GF(q^m)$ всегда можно найти порождающие многочлены $g_1(x)$, $g_2(x)$, …, $g_m(x)$ нерекурсивного сверточного кода в несистематическом виде. Конструктивные параметры такого кода алгебраически связаны с параметрами исходного циклического (N, K, D) кода над $GF(q^m)$. Недостатком рассмотренного способа является ограничение по скорости кодирования сверточных кодов – результат теоремы 1 позволяет алгебраически задавать сверточные коды только с $R = 1/m \leq 1/2$.

В работах [13, 14] развит математический аппарат алгебраического построения нерекурсивных сверточных кодов в несистематическом виде через порождающий многочлен $g(x)$ недвоичного (N, K, D) циклического кода над $GF(q^m)$ и снято ограничение по скорости кодирования. Основной результат представим следующей теоремой.

Теорема 2 [14]. Зафиксируем конечное множество H элементов поля $GF(q^m)$ причем $\log_q |H| = k^0$, $m \geq k^0$. Тогда произвольный многочлен $g(x)$ степени r с коэффициентами над $GF(q^m)$ полностью определяет несистематический сверточный (n, k) код над $GF(q)$ с информационным кадром длины k^0. Если многочлен $g(x)$ 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: $n^0 = m$; $\nu = r \cdot k^0$; $k = (r+1) \cdot k^0$; $n = k \cdot n^0 / k^0$; $R = k^0/m$; $m \geq k^0$; $d_\infty \geq D$.

Теорема 2 обобщает результат теоремы 1 на случай $k^0 \geq 1$ и позволяет алгебраически строить нерекурсивные сверточные коды в несистематическом виде с требуемыми параметрами.

В [13, 14] рассмотрены алгоритмы построения сверточных кодов и формирования их порождающих многочленов, предложен конструктивный подход по прогнозированию (уточнению) истинного свободного кодового расстояния d_∞, алгебраически заданного нерекурсивного сверточного кода в несистематическом виде.

Теоремы 1, 2 оперируют недвоичными нерекурсивными циклическими кодами. Построенные на их основе сверточные коды являются, по сути, обобщением исходного циклического кода на случай бесконечной длины и также являются нерекурсивными схемами. В то же время, как показано в работе [15], применение рекурсивного сверточного кодера с бесконечным импульсным откликом позволяет получить наиболее благоприятную форму дистанционного спектра турбокода для минимизации вероятности ошибочного декодирования, а использование нерекурсивных схем нецелесообразно. Актуальными представляются разработка и исследование алгебраических методов построения рекурсивных сверточных кодов.

3. Разработка алгебраических рекурсивных сверточных кодов

Для построения алгебраических рекурсивных сверточных кодов в несистематическом виде воспользуемся свойствами цикличных кодов [7, 8, 16, 17]. Каждый линейный (n, k, d) код над $GF(q)$ является подпространством $GF^k(q)$ пространства $GF^n(q)$. Циклический код является частным случаем подпространства, так как обладает дополнительным свойством цикличности. Каждый вектор из $GF^n(q)$ представим многочленом от формальной переменной x степени не выше $n - 1$. Компоненты вектора отождествим с коэффициентами многочлена. Множество многочленов обладает структурой векторного пространства, идентичной структуре пространства $GF^n(q)$, а также структурой кольца многочленов $GF(q)[x]/(x^n - 1)$.

В кольце многочленов определено умножение

$$p_1(x)\cdot p_2(x) = R_{x^n-1}\left[p_1(x)\cdot p_2(x)\right].$$

Циклический сдвиг запишется в виде выражения

$$x\cdot p(x) = R_{x^n-1}\left[x\cdot p(x)\right].$$

Если кодовые слова (n, k, d) кода над $GF(q)$ задаются в виде многочленов, то код является подмножеством кольца $GF(q)[x]/(x^n - 1)$. Код является циклическим, если вместе с кодовым словом $c(x)$ он содержит также многочлен $x \cdot c(x)$.

Любой циклический код можно задать через порождающий многочлен $g(x)$, что доказывает следующая теорема.

Теорема 3 [16]. Единственный приведенный ненулевой многочлен $g(x)$ наименьшей степени $r = n - k$ однозначно задает (n, k, d) циклический код над $GF(q)$ и обозначается порождающим многочленом, причем

$$g(x) = \prod_i (x - \beta^i),$$

где $\beta^i \in GF(q^m)$.

Теорема 3 дает мощный механизм построения циклических кодов. Как показано выше, его использование позволяет эффективно реализовать процедуру кодирования, используя нерекурсивные цифровые фильтры. В то же время циклический код можно однозначно задать другим многочленом – мультипликативно обратным многочлену $g(x)$. Справедлива лемма.

Лемма 1. Единственный многочлен $h(x)$ (проверочный многочлен) – мультипликативно обратный приведенному ненулевому многочлену $g(x)$ однозначно задает (n, k, d) циклический код над $GF(q)$ и обозначается проверочным многочленом, причем, если

$$g(x) = \prod_i (x - \beta^i),$$

то

$$h(x) = \prod_j (x - \beta^j),$$

где $\beta^i, \beta^j \in GF(q^m), j \neq i$.

Доказательство. Многочлен $g(x)$ делит многочлен $x^n - 1$, который, в свою очередь, делит многочлен $x^m - 1$, так что $g(x)$ делит также $x^{q^m-1} - 1$. Пусть α – примитивный элемент поля $GF(q^m)$, пусть $q^m - 1 = n \cdot b$, и пусть $\beta = \alpha^b$. Тогда все корни многочлена $x^n - 1$, как и корни многочлена $g(x)$, исчерпываются степенями элемента β. Простые делители многочлена $x^n - 1$ имеют своими корнями только такие элементы. Следовательно, в кольце многочленов $GF(q)[x]/(x^n - 1)$ существует некоторый многочлен $h(x)$, являющийся сомножителем $g(x)$ в разложении двучлена $x^n - 1$, т.е. существует многочлен $h(x)$ – делитель $x^n - 1$ и корни многочлена $h(x)$ также исчерпываются степенями элемента β. Это означает, что произвольный циклический код можно однозначно задать либо порождающим многочленом $g(x)$, либо мультипликативно обратным ему в кольце $GF(q)[x]/(x^n - 1)$ многочленом $h(x)$, причем, если $g(x) = \prod_i (x - \beta^i)$, то $h(x) = \prod_j (x - \beta^j)$, где $\beta^i, \beta^j \in GF(q^m), j \neq i$.

Следствие. $deg\, h(x) = n - deg\, g(x) = n - r = k$.

Воспользуемся проверочным многочленом для построения правила циклического кодирования в несистематическом виде. Запишем кодовое слово несистематического циклического кода

$$C(x) = I(x)\cdot g(x).$$

Выразим порождающий многочлен $g(x)$ через проверочный многочлен $h(x)$ и двучлен $x^n - 1$:

$$g(x) = (x^n - 1)/h(x),$$

с операцией деления в кольце многочленов $GF(q)[x]/(x^n - 1)$. После подстановки получим

$$C(x) = I(x)/h(x). \tag{3}$$

Для реализации процедуры деления на многочлен воспользуемся цифровым фильтром с бесконечным импульсным откликом (рекурсивным фильтром) [16, 17]. На рис. 2 приведена структурная схема цифрового рекурсивного фильтра.

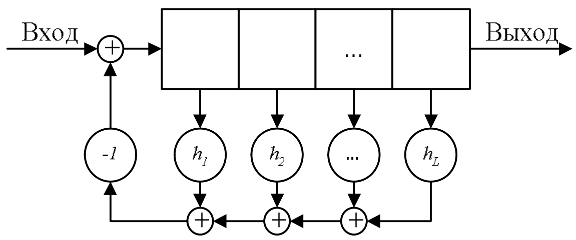

Рис. 2. Цифровой рекурсивный фильтр

Если на вход цифрового рекурсивного фильтра подать последовательность символов $\{i_k, \ldots, i_1, \ldots, i_0\}$, то считанная с выхода последовательность $\{c_k, \ldots, c_1, \ldots, c_0\}$ удовлетворяет рекурсии:

$$c_j = -\sum_{i=1}^{L} h_i i_{j-i} + i_j .$$

Пусть проверочный многочлен задан в виде

$$h(x) = h_0 + h_1 x + h_2 x^2 + \ldots + h_k x^k. \qquad (4)$$

Тогда несистематический кодер, реализующий правило (3), представим в виде схемы на рис. 2.

Воспользуемся выражением (3) для построения алгебраических рекурсивных сверточных кодов в несистематическом виде. Рассмотрим процедуру сверточного кодирования с $R = 1/m$. Зададим рекурсивный кодер в виде рекурсивного фильтра как на рис. 2. Подадим на вход устройства информационный многочлен (2), в общем случае бесконечной длины. Выходную последовательность с символами из $GF(q^m)$ отобразим в последовательность символов из $GF(q)$. Справедлива следующая теорема.

Теорема 4. Несистематический сверточный код над $GF(q)$ с $R = 1/m$ однозначно задается многочленом $h(x)$ над $GF(q^m)$ вида (4). Если многочлен (4) – проверочный многочлен недвоичного (N, K, D) циклического кода над $GF(q^m)$, то он однозначно определяет (n, k) несистематический рекурсивный сверточный код над $GF(q)$ с правилом кодирования $C(x)=I(x)/h(x)$, длиной кодового ограничения $\nu = K$ и конструктивными параметрами:

$$\begin{cases} k^0 = 1, n^0 = m; \\ k = K + 1; \\ n = (K+1)\cdot n^0 = k \cdot m; \\ R = 1/m, d_\infty \ge D. \end{cases} \qquad (5)$$

Доказательство. Циклический (N, K, D) код над $GF(q^m)$ с проверочным многочленом $h(x)$ степени K однозначно определяет набор регистров сдвига, соединенных связями (рис. 2), и задает рекуррентное правило кодирования: $C(x) = I(x)/h(x)$. Если на вход устройства подать последовательность символов из $GF(q)$, то считанная с выхода кодовая последовательность длиной N q^m-ичных символов – суть кодовое слово циклического (N, K, D) кода над $GF(q^m)$, а рекурсивный сверточный код – суть обобщение исходного цикличного кода на непрерывный случай. Параметры сверточного кода связаны соотношениями: $\nu = K \cdot k^0 = r$; $k^0 = 1$; $n^0 = m$; $k = K + 1$; $n = (K + 1) \cdot n^0 = k \cdot m$; $R = 1 / m$ и два любых кодовых слова будут отличаться, по крайней мере, в D q^m-ичных символах. Отображение элементов поля $GF(q^m)$ в элементы поля $GF(q)$ не уменьшает кодовое расстояние между произвольными q-ичными кодовыми словами, следовательно, $d_K \ge D$. По определению дистанционного профиля непрерывных кодов выполняется равенство $d = d_{K+1} \le d_{K+2} \le \ldots \le d_\infty$, откуда $d_\infty \ge d_K$, что и завершает доказательство.

Рассмотрим теперь случай с $R = k^0 / m$. Сформулируем и докажем следующую теорему.

Теорема 5. Зафиксируем конечное множество H элементов поля $GF(q^m)$, причем $log_q | H | = k^0$, $m \ge k^0$. Тогда проверочный многочлен циклического (N, K, D) кода над $GF(q^m)$ полностью определяет несистематический рекурсивный сверточный (n, k, d) код над $GF(q)$ с информационным кадром длины k^0, длиной кодового ограничения $\nu = K \cdot k^0$ и параметрами:

$$\begin{cases} n^0 = m; \\ k = (K+1)\cdot k^0; \\ n = (K+1)\cdot n^0; \\ R = k^0 / m, d_\infty \ge D. \end{cases} \qquad (6)$$

Доказательство. Представим информационную последовательность в виде многочлена с коэффициентами над H, т.е. коэффициенты многочлена $I(x)$ представим в виде многочленов над $GF(q)$ степени $m-1$:

$$I_j = z_{m-1}x^{m-1} + \ldots + z_{k^0}x^{k^0} + \ldots + z_1x + z_0\,,$$

где $z_i \in GF(q)$, причем $m - k^0$ коэффициентов z_i заданы произвольно. Положим, для определенности, $z_i = 0$ для $i = k^0, \ldots, m-1$. Первые k^0 элементов z_i 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 $GF(q^m)$ с проверочным многочленом $h(x)$ однозначно задает рекуррентное правило кодирования: $C(x) = I(x)/h(x)$. При кодировании 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 K проверочного многочлена $h(x)$ циклического (N, K, D) кода над $GF(q^m)$ задает длину кодирующего регистра 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: $\nu = K \cdot k^0$; $k = (K + 1) \cdot k^0$; $n = k \cdot n^0 / k^0$; $R = k^0 / m$; $m \geq k^0$.

Если на вход устройства (рис. 2) подать K информационных кадров по k^0 q-ичных символов (что эквивалентно подаче K кадров по одному q^{k0}-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^{k0}-ичных символов, будут отличаться, по крайней мере, в D q^m-ичных символов. Отображение элементов поля $GF(q^m)$ в элементы поля $GF(q)$ не уменьшает кодовое расстояние между произвольными q-ичными кодовыми словами, следовательно, $d_K \geq D$. По определению дистанционного профиля непрерывных кодов выполняется равенство $d = d_{r+1} \leq d_{r+2} \leq \ldots \leq d_\infty$, откуда $d_\infty \geq d_K$, что и завершает доказательство.

Теоремы 4, 5 дают мощный механизм для построения алгебраических рекурсивных сверточных кодов в несистематическом виде. Их параметры алгебраически связаны с параметрами недвоичных циклических кодов, что позволяет конструктивно строить рекурсивные сверточные коды с требуемыми свойствами. Общая схема сверточного кодера приведена на рис. 3 с дополнительно включенными входными и выходными буферами для отображения символов из $GF(q^m)$ в $GF(q)$ и обратно. Такой кодер реализует обработку символов из $GF(q^m)$.

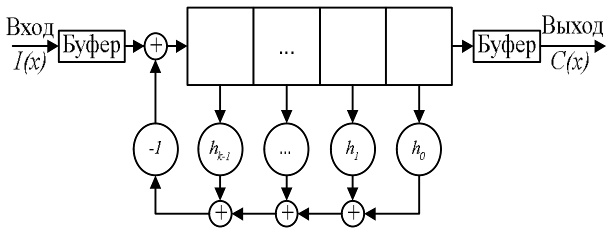

Рис. 3. Несистематический рекурсивный кодер циклического кода через проверочный многочлен

Для построения схемы рекурсивного сверточного кодера с обработкой символов из $GF(q)$ рассмотрим несистематическое кодирование через умножение информационного многочлена на порождающие многочлены $g_1(x)$, $g_2(x)$, …, $g_m(x)$. Предположим, что некоторый многочлен $g_i(x)$ является делителем двучлена x^n-1. Тогда многочлен $g_i(x)$ порождает циклический (n, k) код над $GF(q)$. Воспользуемся результатом леммы 1, получим проверочный многочлен $h_i(x)$, который также однозначно задает циклический (n, k) код над $GF(q)$. Зададим его кодер через цифровой рекурсивный фильтр (3). Получим схему рекурсивного сверточного кодера в несистематическом виде с обработкой символов из $GF(q)$, приведенную в общем виде на рис. 4.

Пример. Зафиксируем конечное поле $GF(2^3)$, построенное по кольцу многочленов по модулю многочлена x^3+x+1: $\alpha^{-\infty}=0$; $\alpha^0=1$; $\alpha^1=x$; $\alpha^2=x^2$; $\alpha^3=x+1$; $\alpha^4=x^2+x$; $\alpha^5=x^2+x+1$; $\alpha^6=x^2+1$. Зафиксируем (7, 3, 5) код Рида-Соломона (РС) над $GF(2^3)$ с порождающим многочленом $g(x) = (x+\alpha^0)(x+\alpha^1)(x+\alpha^2)(x+\alpha^3) = x^4+\alpha^2x^3+\alpha^5x^2+\alpha^5x+\alpha^6$. Мультипликативно обратный многочлену $g(x) = x^4+\alpha^2x^3+\alpha^5x^2+\alpha^5x+\alpha^6$ в кольце $GF(q)[x]/(x^n-1)$ является многочлен $h(x) = x^3+\alpha^2x^2+x+\alpha^2$. Воспользуемся результатами теорем 4, 5 и получим рекурсивные сверточные коды в несистематическом виде с параметрами:

1) двоичный сверточный (n, k, d) код с параметрами: $k^0=1$; $n^0=3$; $\nu=3$; $k=4$; $n=12$; $R=1/3$; $d_\infty \geq 5$;

2) двоичный сверточный код (n, k, d) код с параметрами: $k^0=2$; $n^0=3$; $\nu=6$; k=8; $n=12$, $R=2/3$; $d_\infty \geq 5$.

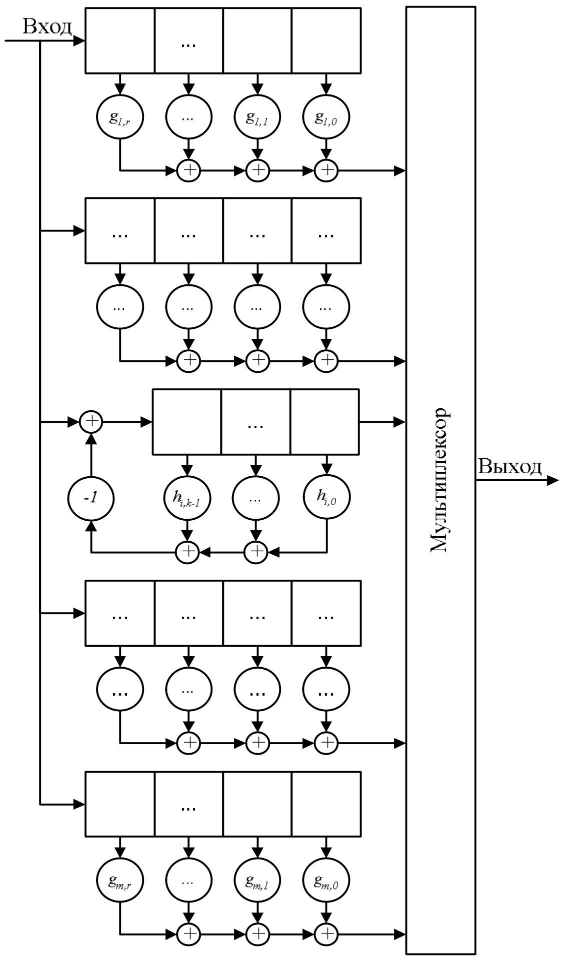

Рис. 4. Несистематический рекурсивный сверточный кодер с обработкой элементов из $GF(q)$

Построим кодер с обработкой элементов из $GF(2^3)$, т.е. пакетами по 3 бита (как на рис. 3). На рис. 5 представлено соответствующее устройство.

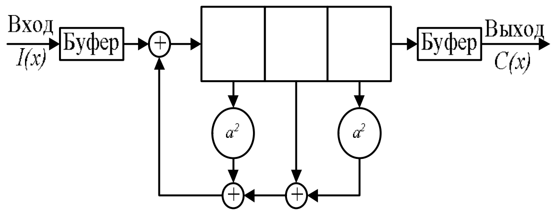

Рис. 5. Несистематический рекурсивный сверточный кодер с обработкой символов из $GF(2^3)$

Для построения кодера с обработкой двоичных символов рассмотрим порождающие многочлены алгебраического сверточного кода, заданного через порождающий многочлен РС кода: $g_1(x) = x^3 + x^2 + x + 1$; $g_2(x) = x^2 + x$; $g_3(x) = x^4 + x^2 + x + 1$.

Многочлен $g_3(x)$ является делителем двучлена $(x^n - 1)$, его мультипликативно обратный элемент в кольце $GF(q)[x]/(x^n - 1)$ является многочлен $h_3(x) = x^3 + x + 1$. Схема соответствующего рекурсивного кодера приведена на рис. 6.

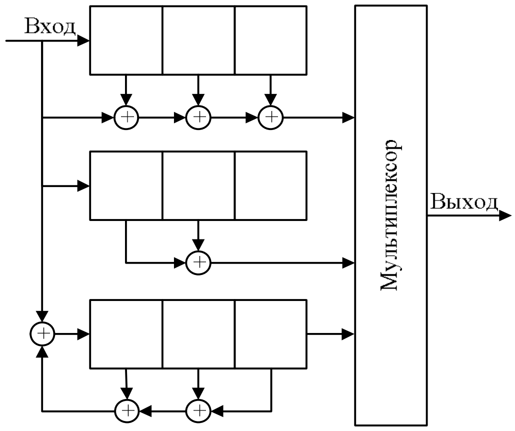

Рис. 6. Несистематический рекурсивный сверточный кодер с обработкой двоичных символов

Выводы

Получили дальнейшее развитие алгебраические методы построения сверточных кодов, отличающиеся от известных представлением сверточного кода через порождающий и/или проверочный многочлен рекурсивного циклического кода, ограниченным на произвольное подполе, что позволяет строить рекурсивные схемы сверточного кодирования в несистематическом виде с требуемыми конструктивными характеристиками. Результаты доказанных теорем 4, 5 позволяют конструктивно определять параметры алгебраически заданных рекурсивных сверточных кодов. Приведенные примеры наглядно демонстрируют конструктивность предложенного подхода.

Перспективным направлением дальнейших исследований является разработка и исследование параллельных каскадных схем (ТК) с алгебраически заданными рекурсивными сверточными кодами, исследование эффективности их использования в каналах космической связи.

Литература

1. CCSDS 101.0-B-4: Telemetry Channel Coding. Blue Book. Issue 4. May 1999. – [Электр. ресурс]. – Режим доступа : http://www.ccsds.org .
2. ETSI EN 301 790 V1.2.1 (2000 – 07) Digital Video Broadcasting (DVB); Interaction channel for satellite distribution systems (DVB – RCS). – [Электр. ресурс]. – Режим доступа : www.etsi.org.
3. Douillard C., Jezequel M., Berrou C., Brengarth N., Tousch J., Pham N. The turbo code standard for DVB – RCS // 2nd International Symposium on turbo codes. – Brest, France, Sept. – 2000.
4. Brengarth N., Novello R., Pham N., Piloni V., Tousch J. DVB – RCS turbo code on a commercial OPB statellite payload: Skyplex // 2nd Int'l Symp. on Turbo Codes. – Brest, France, Sept. – 2000.
5. Berrou C., Glavieux A, Thitimajshima P. Near Shannon Limit Error – Correcting Coding and Decoding: Turbo-Codes // Proceedings of ICC'93. – Geneva, Switzerland, May. – 1993. – P. 1064 – 1070.
6. Berrou C., Glavieux A. Near Optimum Error Correcting Coding and Decoding: Turbo-Codes // IEEE Trans. On Comm. – October, 1996. – Vol. 44, №. 10.
7. Касами Т., Токура Н., Ивадари Е., Инагаки Я. Теория кодирования. – М.: Мир, 1978. – 576 с.
8. Блейхут Р. Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986. – 576 с.
9. Галлагер Р. Простой вывод теоремы кодирования и некоторые применения // Кибернетический сборник. Новая серия. – М.: Мир. – 1966. – Вып. 3. – С. 50 – 90.
10. Витерби А. Границы ошибок для сверточных кодов и асимптотически оптимальный алгоритм декодирования // Некоторые вопросы теории кодирования. – М.: Мир, 1970. – С. 142 – 165.
11. Краснобаев В.А., Приходько С.И., Снисаренко А.Г. Помехоустойчивое кодирование в АСУ. – Х.: ХВВКИУРВ, 1990. – 155 с.
12. Приходько С.И. Алгебраические сверточные коды // Інформаційно-керуючі системи на залізничному транспорті. – Х.: ХарДАЗТ. – 1999. – № 2. – С. 62 – 64.
13. Приходько С.И., Кузнецов А.А., Гусев С.А. Алгебраический метод сверточного кодирования // Современные методы кодирования в электронных системах. Материалы международной НТК. – Сумы: СМКЭС, 2004. – С. 49 – 50.
14. Кузнецов А.А., Приходько С.И., Гусев С.А., Кужель И.Е. Алгебраический метод сверточного кодирования // Комп'ютерні системи та інформаційні технології. – Х.: ХАИ. – 2005. – № 1. – С. 46 – 52.
15. Andersen J.D. Selection of component codes for turbo coding based on convergence properties // Annales des Telecommunications. Special issue on turbo codes. – March – April, 1999. – Vol. 54, № 3 – 4. – [Электр. ресурс]. – Режим доступа: http://www.tele.dtu.dk/~jda/ .
16. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.
17. Кларк Дж. мл., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи. – М.: Радио и связь, 1987. – 392 с.

Поступила в редакцию 10.01.2005

Рецензент: д-р техн. наук, проф. Ю.В. Стасев, Харьковский университет Воздушных сил, Харьков.