УДК 621.391

АЛГОРИТМ ПОСТРОЕНИЯ РЕКУРСИВНЫХ СВЕРТОЧНЫХ КОДОВ

А.С. Постольный
(Харьковский университет Воздушных Сил)

Исследуются алгебраические методы построения рекурсивных сверточных кодов, состоящие в обобщении циклических кодов на случай бесконечной длины. Предлагается алгоритм построения сверточных кодов.

циклический код, рекурсивный сверточный код, алгоритм построения кода

Постановка проблемы в общем виде, анализ литературы. Последним достижением в области помехоустойчивого кодирования являются параллельные каскадные схемы с рекурсивными сверточными кодами в систематическом виде (Recursive Systematic Convolutional Codes). В отечественной и зарубежной литературе такие схемы получили название турбокодов. Турбокодирование, как показано в работах [1 – 3], позволяет получить энергетический выигрыш, близкий к теоретическому пределу.

Основным недостатком сверточных кодов остается сложность их построения: большинство хороших сверточных кодов получено переборным методом, сложность которого растет экспоненциально от длины кодового ограничения. В работах [4 – 6] предложен алгебраический подход, состоящий в обобщении циклических кодов на случай бесконечной длины. **Целью статьи** является разработка алгоритма построения рекурсивных сверточных кодов, исследование особенностей его работы при использовании различных циклических кодов.

Алгебраические методы построения сверточных кодов. Разработанные методы построения рекурсивных сверточных кодов состоят в обобщении циклических блоковых кодов на непрерывный случай [4 – 6]. Это позволяет выразить конструктивные параметры алгебраически заданных сверточных кодов через соответствующие параметры циклических кодов. Основные результаты представим следующими теоремами.

Теорема 1 [5]. Зафиксируем конечное множество H элементов поля $GF(q^m)$, $\log_q |H| = k^0$, $m \ge k^0$. Тогда проверочный многочлен h(x) циклического (N, K, D) кода над $GF(q^m)$ полностью определяет рекурсивный сверточный (n, k, d) код в несистематическом виде над GF(q) с информационным кадром длины k^0, длиной кодового ограничения $\nu = K \cdot k^0$ и параметрами:

$$n^0 = m;\ k = (K+1)\cdot k^0;\ n = (K+1)\cdot n^0;\ R = k^0/m;\ d_\infty \ge D. \qquad (1)$$

***Теорема* 2** [6]. Порождающий многочлен g(x) циклического (N, K, D) кода над GF(q^m) полностью определяет рекурсивный сверточный (n, k, d) код в систематическом виде над GF(q) с кодовым ограничением $\nu = (N - K)\cdot K\cdot \lfloor \log_q H \rfloor$ и параметрами:

$$\begin{cases} k^0 = K \cdot \lfloor \log_q H \rfloor; \\ n^0 = (N-K)\cdot m + K \cdot \lfloor \log_q H \rfloor; \\ k = (N-K+1)\cdot K \cdot \lfloor \log_q H \rfloor; \\ n = (N-K+1)\cdot \left((N-K)\cdot m + K \cdot \lfloor \log_q H \rfloor\right); \\ R = \dfrac{K \cdot \lfloor \log_q H \rfloor}{(N-K)\cdot m + K \cdot \lfloor \log_q H \rfloor}; \\ d_\infty \geq D. \end{cases} \qquad (2)$$

Теоремы 1 – 2 позволяют алгебраически задавать рекурсивные сверточные коды в систематическом и несистематическом виде. Для практического использования полученных результатов разработаем алгоритм алгебраического построения сверточных кодов.

Алгоритм построения рекурсивных сверточных кодов. Для алгебраического построения рекурсивного сверточного кода с конструктивными (n, k, d) параметрами необходимо и достаточно задать порождающий и/или проверочный многочлен циклического (N, K, D) кода. При этом конструктивные параметры сверточного (n, k, d) кода будут аналитически связаны с параметрами циклического (N, K, D) кода и задаваться выражениями (1) – (2). В общем виде *алгоритм построения рекурсивных сверточных кодов* представим в виде последовательности шагов.

ШАГ 1. Ввод параметров рекурсивного сверточного (n, k, d) кода и мощности алфавита кодовых символов q.

ШАГ 2. Выбор варианта построения сверточного кода над GF(q):

– рекурсивный сверточный (n, k, d) код с $R = k^0/m$ в несистематическом виде (см. теорему 1);

– рекурсивный сверточный (n, k, d) код с

$$R = (K\cdot \lfloor \log_q H \rfloor)/((N-K)\cdot m + K\cdot \lfloor \log_q H \rfloor)$$

в систематическом виде (см. теорему 2).

ШАГ 3. Расчет параметров циклического (N, K, D) кода над GF(q^m).

ШАГ 4. Выбор и формирование порождающего и/или проверочного многочлена циклического (N, K, D) кода над GF(q^m).

ШАГ 5. Выбор способа обработки кодовых символов. Формирование порождающих многочленов рекурсивного сверточного (n, k, d) кода над GF(q) и построение схемы его кодера.

Разработанный алгоритм позволяет конструктивным способом за конечное число шагов построить рекурсивный сверточный код с требуемыми параметрами. Схема алгоритма представлена на рис. 1. После ввода параметров сверточного кода (шаг 1) и выбора варианта его построения (шаг 2) на третьем шаге алгоритма производится расчет параметров циклического (N, K, D) кода над $GF(q^m)$. Рассмотрим его подробно.

Предположим, что на втором шаге алгоритма выбран первый вариант построения сверточного кода. Воспользуемся результатами теоремы 1. Зафиксируем конечное поле GF(q) и параметры рекурсивного сверточного (n, k, d) кода с $R = k^0/m$ в несистематическом виде над GF(q). По теореме 1 такой код однозначно задается многочленом h(x) циклического (N, K, D) кода над $GF(q^m)$. Воспользуемся выражением (1), выразим параметры циклического (N, K, D) кода над $GF(q^m)$ через фиксированные параметры рекурсивного сверточного (n, k, d) кода в несистематическом виде над GF(q). Получим:

$$\begin{cases} K = k / k^0 - 1; \\ D = d_\infty; \\ m = n \cdot k^0 / k. \end{cases} \qquad (3)$$

Если при этом требуется построить сверточный код с длиной кодового ограничения v, то необходимо использовать циклический (N, K, D) код над $GF(q^m)$ с $K = v/k^0$. На этом третий шаг алгоритма для первого варианта построения рекурсивного сверточного кода завершен.

Предположим, что на втором шаге алгоритма выбран второй вариант построения сверточного кода. Воспользуемся результатами теоремы 2. Зафиксируем конечное поле GF(q) и параметры рекурсивного сверточного (n, k, d) кода в систематическом виде над GF(q). По теореме 2 такой код с

$$R = \frac{K \cdot \left|\log_q H\right|}{(N - K) \cdot m + K \cdot \left|\log_q H\right|}$$

однозначно задается проверочным многочленом h(x) циклического (N, K, D) кода над $GF(q^m)$. Воспользуемся выражением (2), выразим параметры циклического (N, K, D) кода над $GF(q^m)$ через фиксированные параметры рекурсивного сверточного (n, k, d) кода в систематическом виде над GF(q). Получим:

$$\begin{cases} N = \dfrac{v}{K \cdot \left|\log_q H\right|} + K,\ K = \dfrac{k^0}{\left|\log_q H\right|}; \\ D = d_\infty,\ m = \dfrac{n^0 - k^0}{N - K}. \end{cases} \qquad (4)$$

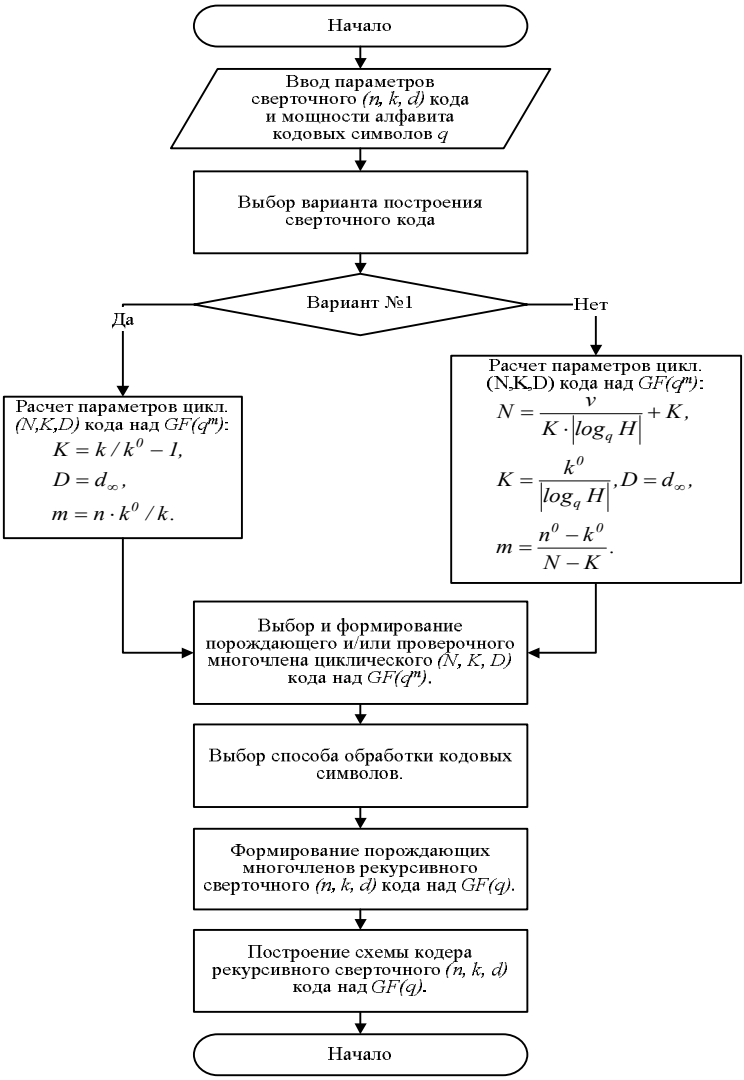

Рис. 1. Схема алгоритма построения рекурсивных сверточных кодов

На этом третий шаг алгоритма для второго варианта построения рекурсивного сверточного кода завершен.

Рассмотрим особенности выполнения четвертого шага разработанного алгоритма, на котором производится выбор схемы кодирования циклического кода (через порождающий или проверочный многочлен), что определяет также схему кодирования рекурсивного сверточного кода.

Предположим, что в качестве циклического кода выбран примитивный код БЧХ, его длина равна $N = (q^m)^M - 1$ [7 – 9]. 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

$$g(x) = НОК(f_1, f_2, \dots, f_{2t}), \quad (5)$$

где $D = 2t + 1$, f_i – минимальный многочлен над $GF(q^m)$ элементов $\alpha^i \in GF((q^m)^M)$.

Проверочный многочлен $h(x)$ определим как сомножитель $g(x)$ в разложении двучлена $x^N - 1$:

$$h(x) = (x^N - 1)/g(x). \quad (6)$$

Последнее выражение эквивалентно следующему:

$$h(x) = НОК(\varphi_1, \varphi_2, \dots), \quad (6')$$

где φ_j – минимальный многочлен над $GF(q^m)$ элементов $\alpha^j \in GF((q^m)^M)$, причем $\alpha^i \neq \alpha^j$.

Рассмотрим случай, когда в качестве циклического кода выбран непримитивный код БЧХ. По определению [7 – 9], длина непримитивного кода БЧХ равна одному из сомножителей в разложении числа $(q^m)^M - 1$ (если, конечно, число $(q^m)^M - 1$ не является простым), т.е.

$$N = ((q^m)^M - 1)/g$$

для произвольного целого g, делящего нацело число $(q^m)^M - 1$. Очевидно, что должно выполняться также условие $r < N$.

Порождающий многочлен непримитивного кода БЧХ задается в виде

$$g(x) = НОК(f_1, f_2, \dots, f_{2t}), \quad (7)$$

где $D = 2t + 1$, f_i – минимальные многочлены над $GF(q^m)$ элементов $\beta^i \in \in GF((q^m)^M)$ такие, что их порядок равен N, т.е. $\beta^i = \alpha^{jg}$, $j = 1, 2, \dots, M/2$.

Проверочный многочлен определяется аналогично случаю, рассмотренному выше – выражение (6) или (6') соответственно.

Рассмотрим случай, когда в качестве циклического кода выбран код Рида-Соломона (РС). По определению [7-9], порождающий многочлен кода РС задается в виде

$$g(x) = (x - \alpha^i) \cdot (x - \alpha^{2i}) \cdot \dots \cdot (x - \alpha^{2ti}), \quad (8)$$

где: $D = 2t + 1$; $\alpha^i \in GF(q^m)$.

Аналогично рассмотренному выше случаю формируется проверочный многочлен $h(x)$ – по выражению (6).

На шестом шаге алгоритма выбирается способ обработки кодовых символов: по одному элементу из GF(q) или пакетами по m элементов из GF(q) – по одному символу из $GF(q^m)$, в соответствии с которым формируются порождающие многочлены рекурсивного сверточного кода.

Выводы. Проведенные исследования показали, что математический аппарат циклического кодирования позволяет алгебраически задавать рекурсивные сверточные коды в систематическом и несистематическом виде. Предложен алгоритм построения сверточных кодов, который позволяет использовать примитивные и непримитивные коды БЧХ, коды Рида-Соломона для алгебраического формирования сверточных кодов. ***Перспективным направлением дальнейших исследований*** является разработка и исследование алгоритмов построения турбокодов на основе алгебраически заданных рекурсивных сверточных кодов в систематическом виде.

ЛИТЕРАТУРА

1. *Berrou C., Glavieux A., Thitimajshima P. Near Shannon Limit Error-Correcting Coding and Decoding: Turbo-Codes // Proceedings of ICC'93, Geneva, Switzerland. – 1993. – P. 1064 – 1070.*
2. *Berrou C., Glavieux A. Near Optimum Error Correcting Coding and Decoding: Turbo-Codes // IEEE Trans. On Comm. – 1996. – Vol. 44, No. 10. – P. 334 – 338.*
3. *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, No 3 – 4. – [Электр. ресурс]. – Режим доступа: http://www.tele.dtu.dk/~jda/.*
4. *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.*
5. *Кузнецов А.А., Тимочко А.И., Приходько С.И., Постольный А.С. Алгебраический метод построения рекурсивных сверточных кодов для стандартов космической связи // Авиационно-космическая техника и технология. – Х.: ХАИ. – 2005. – № 1 (17). – С. 78 – 85.*
6. *Кузнецов А.А., Тимочко А.И., Приходько С.И., Постольный А.С. Алгебраический метод построения рекурсивных сверточных кодов в систематическом виде // Східно-Європейський журнал передових технологій. – Х.: Технологический центр. – 2005 – № 2 (14). – С. 64 – 72.*
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. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.*

Поступила 2.03.2005

Рецензент: доктор физико-математических наук, профессор С.В. Смеляков, Харьковский университет Воздушных Сил.