УДК 621.391

С.И. Приходько, Д.М. Кузьменко

Харьковская государственная академия железнодорожного транспорта

ОЦЕНКА НИЖНЕЙ ГРАНИЦЫ СВОБОДНОГО КОДОВОГО РАССТОЯНИЯ АЛГЕБРАИЧЕСКИ ЗАДАННЫХ СВЕРТОЧНЫХ КОДОВ

Исследуются алгебраические методы построения сверточных кодов, основанные на полиномиальном описании непрерывного линейного кода множеством порождающих многочленов. Сформулированы необходимые и достаточные условия выполнения нижней границы свободного кодового расстояния алгебраически заданного сверточного кода.

сверточный код, порождающий многочлен, кодовое расстояние

Введение

Постановка проблемы в общем виде и анализ литературы. Перспективным направлением повышения помехоустойчивости передачи дискретных сообщений в телекоммуникационных системах и сетях являются методы сверточного кодирования [1 – 7]. Их применение позволяет получить наибольший энергетический выигрыш от кодирования в дискретных каналах с независимыми и группирующимися случайными ошибками [7]. В то же время, существующие подходы к построению сверточных кодов основаны на неалгебраических процедурах переборного поиска и не дают конструктивного механизма синтеза кодов с большой длиной кодового ограничения [1 – 6]. Кроме того, известные методы декодирования сверточных кодов предполагают наличие специальной структуры синдромов и проверочной матрицы кода (самоортогональные и ортогонализируемые коды) либо ограничены вычислительными возможностями (декодер Витерби и последовательный поиск по решетке). Актуальным направлением является разработка алгебраических методов построения сверточных кодов с требуемыми свойствами, исследование эффективных алгоритмов алгебраического декодирования, оценка нижней границы свободного кодового расстояния алгебраически заданных сверточных кодов.

Полиномиальное описание сверточных кодов. Основное отличие сверточных кодов от блочных состоит в наличии функциональной зависимости проверочных символов блока от информации, содержащейся в различных блоках. Это определяется непрерывностью процесса кодирования и декодирования информации сверточными кодами, что в свою очередь хорошо согласуется с последовательной и непрерывной обработкой информации [3 – 6].

Полиномиальное представление сверточного кодирования состоит в описании работы регистров сдвига кодера с помощью соответствующих порождающих многочленов. Процедуру кодирования в этом случае удобно рассматривать как умножение информационных многочленов

$$I_1(x),\ I_2(x),\ \ldots,\ I_{k_0}(x)$$

на порождающие многочлены

$$\begin{aligned} g_1(x) &= g_{1,r-1}x^{r-1} + g_{1,r-2}x^{r-2} + \ldots + g_{1,1}x + g_{1,0}, \\ g_2(x) &= g_{2,r-1}x^{r-1} + g_{2,r-2}x^{r-2} + \ldots + g_{2,1}x + g_{2,0}, \\ &\ldots, \\ g_{n_0}(x) &= g_{n_0,r-1}x^{r-1} + g_{n_0,r-2}x^{r-2} + \ldots + g_{n_0,1}x + g_{n_0,0} \end{aligned} \quad (1)$$

сверточного (n, k, d_∞) кода,

$$k = (r + 1) \cdot k_0,$$
$$n = (r + 1) \cdot n_0 = k \cdot n_0 / k_0,$$
$$d_{r+1} \le d_{r+2} \le \ldots \le d_\infty,$$

где минимальные веса d_i, $i = 1, 2, 3, \ldots$ кодовых слов соответствуют i различным информационным кадрам, а свободное кодовое расстояние определяется по выражению

$$d_\infty = \max(d_i).$$

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

$$\begin{aligned} F_1(x) &= I_1(x) \cdot g_1(x); \\ F_2(x) &= I_2(x) \cdot g_2(x); \\ &\ldots, \\ F_{n_0}(x) &= I_{k_0}(x) \cdot g_{n_0}(x). \end{aligned} \quad (2)$$

Конкретный набор многочленов

$$F_1(x),\ F_2(x),\ \ldots,\ F_{n_0}(x)$$

задается логикой сверточного кодера и над алфавитом из q символов может быть определен q^{rk_0} различными способами.

Проблема синтеза эффективных сверточных кодов состоит в выборе такого набора многочленов $F_i(x)$, $i = 1, 2, \ldots, n_0$, который при заданных кодовых параметрах n и k максимизирует свободное кодовое расстояние d_∞.

Проведенный анализ показал, что для построения сверточных кодов используются неалгебраические процедуры переборного поиска, которые не

дают конструктивного механизма синтеза кодов с большой длиной кодового ограничения $\nu = r \cdot k_0$ [3 – 5]. Особое место в теории сверточного кодирования занимают алгебраические методы синтеза, которые оперируют развитым математическим аппаратом высшей алгебры и позволяют сроить коды с заданными кодовыми параметрами n и k.

Алгебраическое описание сверточных кодов. Алгебраический подход к решению проблемы синтеза сверточных кодов впервые предложен в работах [8, 9], а затем развит в [10, 11]. Суть этого подхода состоит в использовании порождающих многочленов недвоичных циклических кодов для выбора многочленов $F_i(x)$, $i = 1, 2, \ldots, n_0$, задающих логику сверточного кодера и описания процесса формирования кодового слова.

Зафиксируем конечное поле $GF(q^{n_0})$, построенное по кольцу многочленов с коэффициентами над $GF(q)$, и линейный блоковый циклический (N, K, D) код, заданный порождающим многочленом

$$G(x) = G_{r-1}x^{r-1} + G_{r-2}x^{r-2} + \ldots + G_1 x + G_0,$$

где $G_l \in GF(q^{n_0})$, $l = 0, 1, \ldots, r-1$, $r = N - K$.

Рассмотрим произведение

$$I_j(x) \cdot G(x),\ j = 1, 2, \ldots, k_0,$$

где коэффициенты многочлена $I_j(x)$ принадлежат $GF(q)$. Пусть $\{g_{1,l}, g_{2,l}, \ldots, g_{n_0,l}\}$ – коэффициенты $G_l \in GF(q^{n_0})$. Тогда произведение

$$I_j(x) \cdot G(x)$$

при посимвольной записи тождественно

$$I_j(x) \cdot g_1(x),\ I_j(x) \cdot g_2(x),\ \ldots,\ I_j(x) \cdot g_{n_0}(x).$$

Обобщив последнее выражение для всех $j = 1, \ldots, k_0$, получим обобщение линейного блокового циклического кода на непрерывный случай сверточного кодирования, причем справедливы выражения [8 – 11]:

$$\nu = (N - K) \cdot k^0,\ k = (N - K + 1) \cdot k^0,$$
$$n = k \cdot n^0 / k^0,\ R = k^0 / m. \qquad (3)$$

Таким образом, развитый в работах [10, 11] подход позволяет по порождающему многочлену линейного блокового циклического (N, K, D) кода над $GF(q^{n_0})$ строить сверточный (n, k, d_∞) код над $GF(q)$, причем параметры n и k конструктивно выражаются через соответствующие значения (N, K, D). Кроме того, построенные таким образом сверточные коды являются обобщением соответствующего циклического кода, следовательно, можно утверждать, что для большинства случаев $d_\infty \geq D$. В то же время, на сегодняшний день нет строгого математического доказательства оценки $d_\infty \geq D$, равно как и научно обоснованных рекомендаций по выбору $G(x)$.

Проанализируем, для каких случаев справедлива оценка $d_\infty \geq D$.

По определению, циклический (N, K, D) код над $GF(q^{n_0})$ – это линейный блоковый код, заданный порождающим многочленом $G(x)$. В результате кодирования каждому информационному вектору длины K символов из $GF(q^{n_0})$ ставится в соответствие кодовое слово длины N символов из $GF(q^{n_0})$, причем расстояние между произвольными кодовыми словами не менее D символов. В терминах полиномиального описания блоковых кодов циклический (N, K, D) код над $GF(q^{n_0})$ соответствует множеству многочленов $C_i(x)$, $i = 1, 2, \ldots, q^K$. Каждый из многочленов $C_i(x)$ представим в виде

$$C_i(x) = I_i(x) \cdot G(x), \qquad (4)$$

следовательно, имеем:

$$\begin{cases} N - 1 > \deg(C_i(x)) \geq \deg(G(x)), & \text{при } I_i(x) \neq 0; \\ \deg(C_i(x)) = 0, & \text{при } I_i(x) = 0. \end{cases}$$

Таким образом, ненулевое кодовое слово (при $I_i(x) \neq 0$) циклического (N, K, D) кода соответствует многочлену $C_i(x)$, степень которого не превосходит степени двучлена $(x^{N-1} - 1)$, делителем которого является порождающий многочлен $G(x)$. Следовательно, для любого $I_i(x)$ при $\deg(I_i(x)) \leq K - 1$ и многочленах (1), образованных из $G(x)$, соответствующее кодовое слово $C(x)$, сформированное посредством последовательного считывания символов при одинаковых степенях многочленов (2) суть кодовое слово $C_i(x)$ циклического (N, K, D) кода. Соответственно, выполняются следующие выражения:

$$d_\infty \geq d_{K-1} \geq D, \qquad (5)$$

т.е., справедлива оценка, полученная в [10, 11] (справедливы также выражения (3)). Выполнение неравенства в выражении (5) возможно ввиду отображения элементов кодового слова $C(x)$ над $GF(q^{n_0})$ на множество элементов из $GF(q)$.

Рассмотрим случай $\deg(C_i(x)) \geq N - 1$ и $I_i(x) \neq 0$. Тогда ненулевой многочлен, полученный в результате произведения (4) суть кодовое слово циклического $(\deg(C_i(x)), K, D^*)$ кода, причем не всегда $D^* \geq D$. Так, например, если $I_i(x)$ есть второй делитель двучлена $(x^{N-1} - 1)$, т.е.,

$$(x^{N-1} - 1) = I_i(x) \cdot G(x),$$

имеем: $\deg(C_i(x)) = N - 1$ и $D^* = 2$ (как вес двучлена $(x^{N-1} - 1)$). Таким образом, *необходимым условием* выполнения границы (5) есть неразложимость произвольного двучлена

$$(x^M - 1) = I_i(x) \cdot G(x)$$

для любого $I_i(x) \neq 0$ и соответствующего

$$M = \deg(I_i(x)) + \deg(G(x)).$$

Достаточным условием выполнения границы (5) есть условие $D^* \geq D$ для всякого циклического $(\deg(C_i(x)), K, D^*)$ кода, как множества многочленов $C_i(x) = I_i(x) \cdot G(x)$ для произвольного $\deg(I_i(x))$. Следует отметить, что последнее условие не может быть необходимым ввиду отображения элементов кодового слова $C(x)$ над $GF(q^{n_0})$ на множество элементов из $GF(q)$. Другими словами, элементы $I_i(x)$ также как и элементы $C(x)$ (сформированного путем последовательного считывания символов при одинаковых степенях многочленов (2)) принадлежат полю $GF(q)$, а условие $D^* \geq D$ гарантирует выполнение границы (5) для многочленов с элементами из $GF(q^{n_0})$.

Выводы

Таким образом, в результате проведенных исследований получило дальнейшее развитие алгебраическое описание сверточных кодов через множество порождающих многочленов, коэффициенты которых определены через отображение коэффициентов порождающего многочлена недвоичного циклического кода на произвольное подполе. Сформулированы необходимые и достаточные условия выполнения нижней границы свободного кодового расстояния алгебраически заданного сверточного кода.

Список литературы

1. *Финк Л.М. Теория передачи дискретных сообщений. – М.: Сов. радио, 1970. – 728 с.*
2. *Elias P. Coding for Noisy Channel // IRE Convention Record. – 1955. – Part 4. – P. 37-46.*
3. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.*
4. *Кларк Дж., мл., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи. – М.: Радио и связь, 1987. – 392 с.*
5. *Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. – М.: Мир, 1986. – 576 с.*
6. *Касами Т., Токура Н., Ивадари Е., Инагаки Я. Теория кодирования. – М.: Мир, 1978. – 576 с.*
7. *Бернард Скляр. Цифровая связь. Теоретические основы и практическое применение. – М.: Вильямс, 2003. – 1104 с.*
8. *Краснобаев В.А., Приходько С.И., Снисаренко А.Г. Помехоустойчивое кодирование в АСУ. – Х.: ХВВКИУРВ, 1990. – 155 с.*
9. *Приходько С.И. Алгебраические сверточные коды // Інформаційно-керуючі системи на залізничному транспорті. – Х.: ХарДАЗТ. – 1999. – №2(17). – С. 62-64.*
10. *Приходько С.И., Кузнецов А.А., Гусев С.А., Кужель И.Е. Алгебраическое построение несистематических сверточных кодов // Системи обробки інформації. – Х.: ХВУ. – 2004. – Вип. 8 (36). – С. 170-175.*
11. *Приходько С.И., Кузнецов А.А., Гусев С.А., Кужель И.Е. Алгебраический метод сверточного кодирования // Комп'ютерні системи та інформаційні технології. – Х.: ХАИ, 2005.– № 1. – С.35-43.*

Поступила в редколлегию 24.03.2007

Рецензент: **д**-р техн. наук, проф. С.В. Смеляков, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.