УДК 621.391

АЛГЕБРАИЧЕСКОЕ ПОСТРОЕНИЕ НЕСИСТЕМАТИЧЕСКИХ СВЕРТОЧНЫХ КОДОВ

к.т.н. С.И. Приходько, к.т.н. А.А. Кузнецов, С.А. Гусев, И.Е. Кужель
(представил д.т.н., проф. О.Н. Фоменко)

Предлагается алгоритм алгебраического построения несистематических сверточных кодов с заданными конструктивными свойствами. Приведен пример алгебраического построения сверточных кодов через порождающий многочлен кода Рида-Соломона (РС).

Введение. Одним из наиболее эффективных средств защиты передаваемых данных от возникающих ошибок являются методы помехоустойчивого кодирования. Перспективным направлением в их развитии являются сверточные коды, которые позволяют получить наибольший выигрыш от кодирования [1 – 2]. Основной проблемой при их построении является сложность переборных алгоритмов их поиска. В работах [3 – 5] исследована связь несистематических сверточных кодов с недвоичными циклическими кодами, получены аналитические выражения, связывающие их параметры. **Целью статьи** является разработка практических алгоритмов алгебраического построения несистематических сверточных кодов.

Алгебраический алгоритм построения сверточных кодов. Алгебраический метод построения несистематического сверточного (n, k, d) кода над GF(q) состоит в представлении его порождающих многочленов через порождающий многочлен недвоичного циклического (N, K, D) кода над $GF(q^m)$. Это позволяет использовать мощный математический аппарат циклического кодирования для алгебраического вычисления конструктивных параметров сверточных кодов. Основные результаты такого подхода представлены следующими теоремами [4 – 5].

Теорема 1. Несистематический сверточный (n, k, d) код над GF(q) со скоростью кодирования R = 1/m однозначно задается порождающим многочленом P(x) (N, K, D) циклического кода над $GF(q^m)$. Конструктивные параметры сверточного кода определяются соотношениями: $k^0 = 1$; $n^0 = m$; $\nu = r$; $k = r + 1$; $n = k \cdot m$; $R = 1/m$; $d_\infty \geq D$; $C(x) = I(x) \cdot P(x)$, где k^0 – длина информационного (входного) кадра; n^0 – длина входного кадра; r – длинна регистра сдвига сверточного кодера; d_∞ – свободное минимальное расстo-

яние сверточного кода; I(x) и C(x) – информационный и кодовый многочлены соответственно.

Теорема 2. Зафиксируем конечное множество H элементов поля $GF(q^m)$, $\log_q |H| = k^0$, $m \geq k^0$. Тогда 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 параметрами: $n^0 = m$; $\nu = r \cdot k^0$; $k = (r + 1) \cdot k^0$; $n = k \cdot n^0 / k^0$; $R = k^0 / m$; $m \geq k^0$; $d_\infty \geq D$.

Результаты теорем 1 – 2 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 [3 – 5]. 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

$$P(x) = НОК(f_1, f_2, \ldots, f_{2t}),$$

где t – число ошибок, которые должен исправлять циклический (N, K, D) код, $N = (q^m)^M - 1$, $r = \deg P(x)$, $K = N - r$, $D = 2t + 1$, 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 в качестве циклического кода выбран непримитивный код БЧХ. 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 $(q^m)^M - 1$ [1 – 2]. Очевидно, что также должно выполняться условие $r < N$. Порождающий многочлен непримитивного кода БЧХ задается в виде

$$P(x) = НОК(\varphi_1, \varphi_2, \ldots, \varphi_{2t}),$$

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. $\beta^i = \alpha^{jg}$, j = 1, 2, …, 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. Если порождающий многочлен P(x) циклического (N, K, D) кода над $GF(q^m)$

$$P(x) = \alpha_{r-1}x^{r-1} + \alpha_{r-2}x^{r-2} + \ldots + \alpha_1 x + \alpha_0,\ \alpha_i \in GF(q^m)$$

записать в виде

$$P(x) = (p_{1,r-1}, p_{2,r-1}, \ldots, p_{m,r-1})x^{r-1} + (p_{1,r-2}, p_{2,r-2}, \ldots, p_{m,r-2})x^{r-2} + \ldots + (p_{1,1}, p_{2,1}, \ldots, p_{m,1})x + (p_{1,0}, p_{2,0}, \ldots, p_{m,0}),\ p_{i,j} \in GF(q),$$

то многочлены:

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

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

…

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

будут являться порождающими многочленами искомого сверточного кода. Алгоритм формирования порождающих многочленов представлен на рис. 1.

Подставим в общую схему несистематического сверточного кодера (рис. 2) параметры полученных многочленов $P_1(x)$, … , $P_m(x)$. 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).

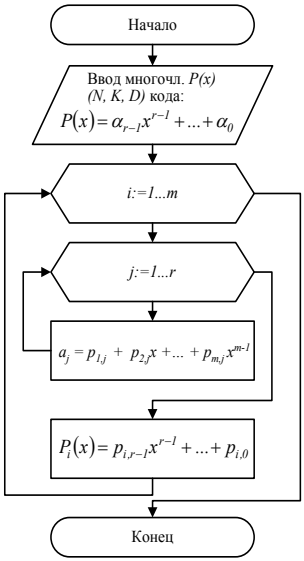

Рис. 1. Схема алгоритма формирования порождающих многочленов сверточного кода

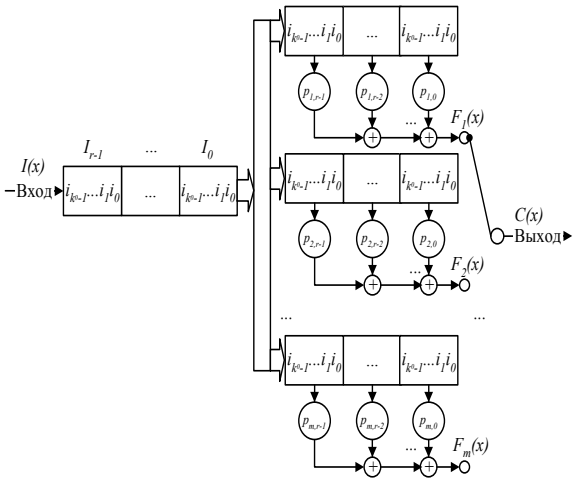

Рис. 2. Несистематический сверточный кодер

Таблица 1

Конструктивные характеристики двоичных сверточных кодов

(N, K, D)	(n, k, d)	v	R	$d_П$	d_∞
(7, 1, 7)	(21, 7, 7)	6	1 / 3	12	15
	(21, 14, 7)	12	2 / 3	12	13
(7, 2, 6)	(18, 6, 6)	5	1 / 3	10,3	11
	(18, 12, 6)	10	2 / 3	10,3	12
(7, 3, 5)	(15, 5, 5)	4	1 / 3	8,6	9
	(15, 10, 5)	8	2 / 3	8,6	10
(7, 4, 4)	(12, 4, 4)	3	1 / 3	6,9	7
	(12, 8, 4)	6	2 / 3	6,9	8
(7, 5, 3)	(9, 3, 3)	2	1 / 3	5,1	6
	(9, 6, 3)	4	2 / 3	5,1	7
(7, 6, 2)	(6, 2, 2)	1	1 / 3	3,4	4
	(6, 4, 2)	2	2 / 3	3,4	5

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, предсказанное значение свободного кодового расстояния и истинное кодовое расстояние.

Выводы. Проведенные исследования показали, что недвоичный циклический код однозначно задает порождающие многочлены несистематического сверточного кода. 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.Дж., Слоэн Н.Дж.А. 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. *Краснобаев В.А., Приходько С.И., Снисаренко А.Г. Помехоустойчивое кодирование в АСУ. – Х.: ХВВКИУ РВ, 1990. – 155 с.*
4. *Приходько С.И., Кузнецов А.А., Гусев С.А. Алгебраический метод сверточного кодирования // Інформаційно-керуючі системи на залізничному транспорті. — 2004. – №4. – С. 17 – 21.*
5. *Приходько С.И., Кузнецов А.А., Гусев С.А. Алгебраический метод сверточного кодирования // Современные методы кодирования в электронных системах. Материалы международной НТК 26-27 октября 2004 г. – Сумы: СМКЭС. – 2004. – С. 11 – 12.*

Поступила 13.08.2004

***ПРИХОДЬКО Сергей Иванович**, канд. техн. наук, доцент, нач. кафедры ХУ ВС. В 1978 году закончил ХВВКИУ. Область научных интересов – помехоустойчивое кодирование, методы обработки и передачи информации.*

***КУЗНЕЦОВ Александр Александрович**, канд. техн. наук, с.н.с., нач. НИЛ ХУ ВС. В 1996 году закончил ХВУ. Область научных интересов – помехоустойчивое кодирование, методы обработки и передачи информации.*

***ГУСЕВ Сергей Анатольевич**, преподаватель кафедры ХУ ВС. В 1993 году закончил ХВВКИУ. Область научных интересов – помехоустойчивое кодирование, методы обработки и передачи информации.*

***КУЖЕЛЬ Игорь Евгеньевич**, научный сотрудник НИЛ кафедры ХУ ВС. В 1995 году закончил ХИЛ ВВС. Область научных интересов – помехоустойчивое кодирование, методы обработки и передачи информации.*