КВАДРАТИЧНО-ВЫЧЕТНЫЕ КОДЫ КАК ОБОЩЕННЫЕ КОДА БОУЗА – ЧОУДХУРИ – ХОКВИНГЕМА

В. А. Липницкий, А. В. Кушнеров, Е. В. Середа

Военная академия Республики Беларусь
Минск, Беларусь
e-mail: *valipnitski@yandex.ru*

Статья посвящена особому классу помехоустойчивых кодов, так называемым квадратично-вычетным кодам. Эти коды порой являются обобщением БЧХ-кодов, что открывает перспективы их декодирования с помощью теории норм синдромов.

Ключевые слова: Помехоустойчивые коды; квадратично-вычетные коды; коды БЧХ; теория норм синдромов.

SQUARE RESIDUAL CODES AS A BOSE-CHAUDHURI-HOCQUENGHEM CODES GENERALIZATION

V. A. Lipnitski, A. V. Kushnerov, E. V. Sereda

Military Academy of Belarus
Minsk, Belarus

This article is dedicated to a special class of error-correcting codes, which is called square residual codes. Codes of that type can be generalized in several cases to a BCH-codes. It is the reason why such codes can correct errors with NST methods.

Keywords: Error-correcting codes; square residual codes; BCH-codes, norm syndrome theory.

ВВЕДЕНИЕ

Семейство кодов Боуза – Чоудхури – Хоквингема (БЧХ-кодов) является классическим в теории помехоустойчивого кодирования и наиболее популярным в приложениях, особенно в высокоскоростных системах передачи информации [1]. Цикличность, представление компонент синдромов ошибок элементами поля Галуа позволили развить алгебраические методы обработки этих кодов. Ярким примером таких методов является коррекция ошибок примитивными БЧХ-кодами решением уравнений в конечных полях. Теория норм синдромов (ТНС), последовательно применяя свойства автоморфизмов кодов, позволила предложить высокоскоростные перестановочные алгоритмы обработки БЧХ-кодов, особенно эффективные для непримитивных кодов – для коррекции ими многократных ошибок, кратность которых далеко выходит за конструктивные возможности самих кодов [2, 3].

Внимательный анализ всех четырех классов квадратично-вычетных кодов (КВ-кодов) показывает, что один из этих классов можно интерпретировать как семей-

ство обобщенных БЧХ-кодов. Это открывает новые возможности декодирования КВ-кодов, применения к ним теории полей Галуа, теории норм синдромов, разработки перестановочных норменных методов коррекции ими допустимых классов векторов-ошибок.

ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ И ФАКТЫ, СВЯЗАННЫЕ С БЧХ-КОДАМИ

В конечном поле $GF(q^m)$ из q^m элементов – расширении своего минимального подполя $GF(q)$ степени m, зафиксируем примитивный элемент α [2]. Для всякого натурального n, делящего q^m-1, в поле Галуа $GF(q^m)$ найдется элемент β порядка n (например, $\beta=\alpha^c$ для натурального $c=(q^m-1)/n$). Зафиксируем целые числа $b\ge 0$, не делящееся на n, $\delta>1$, натуральное n делящее или равное q^m-1, но не делящее q^s-1 для всех целых s, $0<s<m$. При этом значение δ должно быть таким, что выполняется неравенство: $m(\delta-1)<n$. Зафиксируем в поле $GF(q^m)$ $\delta-1$ элементов $\beta^b,\beta^{b+1},\ldots,\beta^{b+\delta-2}$. Для каждого из них в кольце полиномов $GF(p)[x]$ существует однозначно определенный неприводимый полином $g(\beta^i,x)$ с корнем β^i соответственно, $b\le i\le b+\delta-1$. Пусть $M(x)$ – наименьшее общее кратное полиномов $g(\beta^b,x), g(\beta^{b+1},x), \ldots, g(\beta^{b+\delta-2},x)$.

Определение 1. Линейный циклический код $C=J=<M(x)>$ в кольце $R_n=GF(p)[x]/<x^n-1>$ называется кодом Боуза – Чоудхури – Хоквингема над полем $GF(q^m)$ длиной n и с конструктивным расстоянием δ. При $n=q^m-1$ элемент $\beta=\alpha$ и БЧХ-код C называют примитивным, если же $n<q^m-1$, код называют непримитивным.

Согласно [1], таким образом заданный БЧХ-код C имеет в качестве одной из проверочных матрицу

$$H=\left[\begin{array}{cccc} 1 & \beta^b & \beta^{2b} & \beta^{(n-1)b} \\ 1 & \beta^{b+1} & \beta^{2(b+1)} & \beta^{(n-1)(b+1)} \\ \hline 1 & \beta^{b+\delta-2} & \beta^{2(b+\delta-2)} & \beta^{(n-1)(b+\delta-2)} \end{array}\right]=\left[\beta^{bi},\beta^{(b+1)i},\ldots,\beta^{(b+\delta-2)i}\right]^T, \qquad (1)$$

в которой каждый элемент β^i представляет собой столбец из m элементов поля $GF(q)$ – координат вектора β^i в базисе $\alpha^{m-1},\alpha^{m-2},\ldots,1$.

Неравенство $m(\delta-1)<n$ гарантирует, что ядро матрицы (1) – код C – является линейным пространством над полем $GF(q)$ размерности, не меньшей, чем $n-m(\delta-1)$ Точное значение минимального расстояния БЧХ-кодов $d\ge\delta$.

На практике наибольшее значение играют двоичные БЧХ-коды, т. е. коды C над полем $GF(q)=GF(2)$. Здесь специализацией параметров можно существенно увеличить размерность и скорость кода. Так, при значении $b=1$ элементы $\beta,\beta^2,\beta^4,\ldots$ являются сопряженными в поле $GF(2^m), m\ge 2$ т. е. являются корнями одного и того же неприводимого полинома над полем $GF(2)=Z/2Z$ (детали см. в [1–3]). Тогда, с одной стороны, степень полинома $M(x)$ существенно уменьшится, а с другой стороны, ран-

ги следующих подматриц матрицы H окажутся равными: $\mathrm{rang}\left[\beta,\beta^2,\beta^4,\ldots\right]^T=\mathrm{rang}[\beta]$ [4]. Следовательно, в H подматрица $\left[\beta,\beta^2,\beta^4,\ldots\right]^T$ заменяется подматрицей $[\beta]$. Мы получаем каноническую проверочную матрицу двоичного БЧХ-кода C с конструктивным расстоянием $\delta=2t+1$:

$$H=\left[\beta^i,\beta^{3i},\ldots,\beta^{(2t-1)i}\right]^T. \qquad (2)$$

Размерность этого кода $k=n-mt$, а минимальное расстояние $d=2t+1$ в примитивным случае, как правило, а в непримитивном – велика доля кодов со значением $d>2t+1$ [5]. При $t=1$ матрица (2) имеет вид: $H=\left[\beta^i\right]$. Задаваемый ею код известен как код Хемминга, непримитивен при $\beta\neq\alpha$.

БЧХ-КОДЫ И ИХ ОБОБЩЕНИЕ

Изучение циклотомических классов по различным модулям показывает, что существует бесчисленное море двоичных БЧХ-кодов с разнообразным и причудливым сочетанием сопряженных элементов в соответствующих полях Галуа и с весьма интересными упрощенными проверочными матрицами. Ряд подобных примеров дан в работах [2, 3].

Свойства двоичных БЧХ-кодов, а также примеры приводят к мысли о том, что двоичный линейный циклический код с проверочной матрицей

$$H=\left[\beta^{ki},\beta^{li},\beta^{si},\ldots\right]^T, \qquad (3)$$

где $1\le k<l<s<\ldots$ и среди степеней $\beta^{ki},\beta^{li},\beta^{si},\ldots$ не имеется ни одной пары сопряженных, также следует отнести к классу БЧХ-кодов, возможно, с оговоркой «к классу обобщенных БЧХ-кодов с конструктивным расстоянием $\delta=2t+1$» для количества t последовательных двоичных подматриц по m строк в каждой в матрице (3), соответствующих элементам $\beta^{ki},\beta^{li},\beta^{si},\ldots$.

К обобщенным БЧХ-кодам применима теория норм синдромов, причем в упрощенном виде, что вовсе не является недостатком, так как облегчает вычисления и применение перестановочных методов к ним.

КВАДРАТИЧНО-ВЫЧЕТНЫЕ КОДЫ И ИХ ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

Согласно [1], гл. 16, для *построения* КВ-кодов нужны два простых числа p и l, при этом l является квадратичным вычетом по модулю p. В результате получается код, определенный над полем $GF(l)$. Поскольку в реальной практике важны двоичные коды, ограничимся рассмотрением именно случая $l=2$.

Как известно (см., например, [6]), число 2 является квадратичным вычетом по простому модулю p тогда и только тогда, когда p имеет вид $8k\pm1$. Согласно теореме Дирихле, существует бесконечно много простых чисел вида $8k+1$, как и вида $8k+7$. Для построения двоичных КВ-кодов именно такие простые числа p мы и вынуждены рассматривать.

Если быть более точным, КВ-код определяется минимальным расширением поля $GF(l) = GF(2)$ – полем $GF(2^m)$, содержащим группу C_p корней p-й степени из 1. Поле $GF(2^m)$ содержит группу C_p тогда и только тогда, когда $2^m - 1$ делится на p. Действительно, все ненулевые элементы поля $GF(2^m)$ образуют циклическую группу $GF(2^m)^*$ порядка $2^m - 1$. Пусть α – образующая группы $GF(2^m)^*$ и пусть $2^m - 1 = p \cdot s$. Тогда $\beta = \alpha^s$ – является элементом поля $GF(2^m)$ порядка p, следовательно, его степени образуют циклическую подгруппу C_p порядка p в группе $GF(2^m)^*$.

Предложение 1. Для всех простых чисел p вида $8k \pm 1$ мультипликативная группа поля $GF(2^{(p-1)/2})$ содержит подгруппу C_p корней порядка p из 1. Минимальное расширение поля $GF(2)$, содержащее подгруппу C_p корней порядка p из 1, имеет вид $GF(2^m)$, где m является либо натуральным делителем числа $(p-1)/2$, либо совпадает с $(p-1)/2$.

КВ-коды имеют простую длину $n = p = 8k \pm 1$, являются циклическими, делятся на четыре класса, так как порождаются в кольце R_p как идеалы одним из полиномов следующих четырех видов: $q(x), (x-1)q(x), n(x), (x-1)n(x)$ (см. [1], с. 464). Здесь $q(x)$ и $n(x)$ – специальные полиномы степени $(p-1)/2$ из кольца $GF(2)[x]$: $q(x) = \prod_{i \in Q} (x - \beta^i)$; $n(x) = \prod_{r \in N} (x - \beta^r)$; β – примитивный корень p-ой степени из 1 в поле $GF(2^m)$; Q – циклическая подгруппа квадратов (квадратичных вычетов по модулю p) мультипликативной группы $GF(p)^*$ поля $GF(p)$; N – множество квадратичных невычетов по модулю p.

Отметим, что подгруппа Q имеет порядок $(p-1)/2$, содержит и 1, и 2, и всю циклическую группу $<2>$, порожденную классом вычетов 2 в $GF(p) = Z / pZ$. Ту же мощность $(p-1)/2$ имеет и множество N квадратичных невычетов.

КВ-коды замечательны тем, что их минимальное расстояние ограничено снизу [1]: минимальное расстояние d кода $C_{q(x)}$ длиной p удовлетворяет неравенству: $d \geq \sqrt{p}$.

КВ-КОДЫ КАК ОБОБЩЕННЫЕ БЧХ-КОДЫ

Ввиду очевидной взаимосвязи всех четырех классов КВ-кодов, в дальнейшем внимание сосредоточим на одном из них, а именно на КВ-кодах $C_{q(x)}$, порожденных полиномами $q(x) = \prod_{i \in Q} (x - \beta^i)$.

Предложение 2. Всякий двоичный КВ-код $C_{q(x)}$ длиной p, определенный над полем $GF(2^m)$ – минимальным расширением поля $Z/2Z$, содержащим все корни p-й степени из 1, является обобщенным непримитивным БЧХ-кодом, т. е. с проверочной матрицей вида (3) и с конструктивным расстоянием $\delta = 2t + 1$, где $(p-1)/2 = mt$.

Рассмотрим примеры. Пусть квадратично-вычетный код $C_{q(x)}$ имеет длину $p = 41.$ В данном случае $m = \frac{p-1}{2} = 20.$ В мультипликативной группе $GF(p)^* = Z/41Z^*$ имеется в точности 20 квадратов:

$$Q = \{1,\ 2 \equiv 17^2 (\mathrm{mod}\, 41),\ 4,\ 5 = 169 - 41\cdot 4,\ 8 = 49 - 41,\ 9,\ 10 \equiv 16^2 (\mathrm{mod}\, 41),$$
$$16,\ 18 = 100 - 82,\ 20 = 15^2 - 41\cdot 5,\ 21 = 144 - 41\cdot 3,\ 23 = 64 - 41,\ 25,\ 31 = 400 - 41\cdot 9,$$
$$32 \equiv 14^2 (\mathrm{mod}\, 41),\ 33 = 19^2 - 41\cdot 8,\ \ 36,\ 37 \equiv 18^2 (\mathrm{mod}\, 41),\ 39 = 121 - 82,\ 40 = 81 - 41\}.$$

Для примитивного элемента α поля $GF(2^{20})$ порядок мутипликативной группы $GF(2^{20})^*$ равен 1 048 575 и делится на 41, частное равно 25 575. Тогда элемент $\beta = \alpha^{25575}$ имеет порядок 41 в группе $GF(2^{20})^*$. Неприводимый над полем $GF(2)$ полином $Irr(\beta, X)$ с корнем β должен иметь степень 20. Степени всех корней этого полинома как степени элемента β в силу формулы (4) составляют один циклотомический класс

$$C(1) = \{1,\ 2,\ 4,\ 8,\ 16,\ 32,\ 23,\ 5,\ 10,\ 20,\ 40,\ 39,\ 37,\ 33,\ 25,\ 9,\ 18,\ 36,\ 31,\ 21\}.$$

Как видим, $C(1) = Q.$ Это означает, в полном соответствии с доказательством первой части предложения 2, что рассматриваемый линейный КВ-код $C_{q(x)}$ длиной 41 совпадает с непримитивным кодом Хемминга, задаваемым проверочной матрицей $H = (\beta^i) = (1\ \beta\ \beta^2 \ldots \beta^{40})$. Точно так же устроены и все остальные КВ-коды с условием: $t = 1.$ Как отмечено выше, минимальное расстояние данного кода удовлетворяет неравенству: $d \geq \sqrt{41}$ и, следовательно, $d \geq 7.$ Вычисления показывают, что на самом деле здесь $d = 9.$

Рассмотрим КВ-код $C_{q(x)}$ минимальной длины с $t > 1.$ Это код длиной $p = 31.$ Здесь $m = 5,\ \frac{p-1}{2} = 15 = 3m$ и $Q = \{1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28\}$. Циклотомический класс $C(1) = \{1, 2, 4, 8, 16\}$ – составляет лишь треть множества $Q.$ Остальные две трети множества Q распределены по двум следующим смежным классам: $C(9) = \{9, 18, 5, 10, 20\} = C(5);\ \ C(25) = \{25, 19, 7, 14, 28\} = C(7).$ Эти вычисления показывают, что в данном случае $q(x) = Irr(\beta, X) \cdot Irr(\beta^5, X) \cdot Irr(\beta^7, X)$. Следовательно, данный КВ-код длиной 31 можно рассматривать как непримитивный обобщенный БЧХ-код с проверочной матрицей $H = (\beta^i, \beta^{5i}, \beta^{7i})^T$.

ЗАКЛЮЧЕНИЕ

Логика исследований семейства кодов Боуза – Чоудхури – Хоквингема приводит к необходимости рассмотрения обобщенных БЧХ-кодов. Жестко устроенный класс квадратично-вычетных кодов принадлежит семейству обобщенных БЧХ-кодов. Это факт открывает возможности исследования КВ-кодов с помощью теории полей Галуа,

к разработке перестановочных методов коррекции ошибок КВ-кодами на основе теории норм синдромов.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки: пер. с англ. М. : Связь, 1979.
2. Липницкий В. А., Конопелько В. К. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Минск : БГУ, 2007.
3. Липницкий В. А., Олексюк А. О. Теория норм синдромов и плюс-декодирование // Докл. БГУИР. 2014. № 8. С. 71–78.
4. Лидл Р., Нидеррайтер Г. Конечные поля : в 2 т.: пер. с англ. М. : Мир, 1988.
5. Липницкий В. А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа. 2-е изд. Минск : БГУИР, 2006.
6. Виноградов И. М. Основы теории чисел. М. : Наука, 1972.