Столярова М.И., Бобрышева Г.В., Звозникова Г.О. Анализ ошибкообнаруживающих свойств циклических кодов. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей XVII Междунар. научно-техн. конф. – Пенза: ПДЗ, 2017. – С. 105-108.

УДК 621.391

АНАЛИЗ ОШИБКООБНАРУЖИВАЮЩИХ СВОЙСТВ ЦИКЛИЧЕСКИХ КОДОВ

М.И. Столярова, Г.В. Бобрышева, Г.О. Звозникова

ANALYSIS OF THE ERROR-DETECTING PROPERTIES OF CYCLIC CODES

M.I. Stolyarova, G.V. Bobrysheva, G.O. Zvoznikova

Аннотация. Циклические коды нашли широкую популярность при построении каскадных систем помехоустойчивого кодирования для вычислительных систем и сетей, что объясняется их достаточно высокой ошибкообнаруживающей и исправляющей способностью. На основе кода Боуза-Чоудхури-Хоквингема (БЧХ-код) описан алгоритм нахождения порождающего полинома и приведен пример его построения.

Ключевые слова: кодирование информации, циклические коды, обнаружение ошибок, исправление ошибок.

Abstract. Cyclic codes have found wide popularity in the construction of cascading systems of noise-immune encoding for computer systems and networks, which isexplained by their rather high error-detecting and correcting ability. Based on the Bose-Chowdhury-Hocquinghamcode (BCH-code), an algorithm for finding the generating polynomial is described and an example of its construction is given.

Keywords: information coding, cyclic codes, error detection, error correction.

Линейные циклические коды обладают тем свойством, что вместе с каждым словом $c = (c_0, c_1, \ldots, c_{n-1})$ в циклический код входят слова, полученные из с циклическим сдвигом на любое количество разрядов вправо или влево, т.е. $c_1 = (c_1,\ldots, c_{n-1},c_0)$, $c_2 = (c_2, \ldots, c_{n-1}, c_0, c_1)$ и т.д. Для описания и анализа циклических кодов используют специальную алгебраическую технику – технику полиномов (многочленов) над конечными полями.

Линейный (n, k)-код C над полем GF(q) называется циклическим, если каждое слово $c \in C$, будучи циклически сдвинуто, также является словом этого кода.

Циклические коды привлекательны по двум причинам. Во-первых, легко можно реализовать кодирование и вычисление, используя простые регистры сдвига с обратной связью. Во-вторых, этим кодам присуща алгебраическая структура, поэтому можно найти различные простые и эффективные способы их декодирования.

Свойства циклических кодов определяются выбранным порождающим (образующим) многочленом g(x) [1]:

1. Циклический код находит все одиночные ошибки, в том случае если порождающий многочлен g(x) содержит более одного члена. При представлении циклического кода многочленами одиночная ошибка описывается одночленом $E(x) = x^i$, где i указывает номер искаженного разряда $0 \le i \le n-1$. Ошибка будет обнаружена, т.к. одночлен не делится на многочлен без остатка.

2. Циклический код с порождающим многочленом $g(x) = x + 1$ находит все нечетные ошибки. Для многочлена $g(x) = x + 1$ проверочная матрица представляет вид $H^T = |111\ldots1|$. При такой проверочной матрице остаток определяется

суммой по модулю 2 всех элементов принятой кодовой комбинации, т.е. выполняется проверка на четность. Поэтому ошибки будут обнаружены на нечетном количестве позиций.

3. Циклический код находит все одиночные и двукратные ошибки в том случае, когда разрядность кода n не больше длины цикла l_c, под длиной цикла многочлена понимают минимальный показатель степени двучлена $x^n + 1$, при котором данный двучлен делится без остатка на образующий многочлен g(x).

4. Циклический код с порождающим многочленомg(x) степени k находит все групповые ошибки длительностью в k разрядов и менее. Любая групповая ошибка в k разрядов описывается многочленом степени k-1, т.е. $E(x) = x^i(x^{k-1} + x^{k-2} + \dots + 1)$. Данный вид ошибок обнаруживается, т.к. многочлен степени k-1 на многочлен степени k не делится.

5. Циклический код с порождающим многочленом g(x) степени k не обнаруживает $\frac{1}{2^{k-1}}$ часть ошибок кратности k + 1.

6. Циклический код с порождающим многочленом g(x) степени k не обнаруживает $\frac{1}{2^k}$ часть ошибок более кратности k+1.

Анализируя перечисленные свойства циклического кода, можно сделать вывод о том, что способности кода по обнаружению и исправлению ошибок определяются выбранным многочленом g(x).

При обнаружении ошибок стандартные многочлены имеют вид: $g(x) = x^8 + x^2 + x + 1$, d = 4 при длине кодовой комбинации $n \le 2^7$, или $g(x) = x^{16} + x^{15} + x^{13} + x^{11} + x^5 + x^3 + x + 1$, d = 6 при длине кодовой комбинации $n \le 2^7$.

Хотелось бы отметить, что разработан ряд методик по выбору порождающего многочлена g(x). В литературе коды называют по фамилиям ученых, предложивших ту или иную методику. Так получили свое название коды Боуза-Чоудхури-Хоквингема (БЧХ), коды Рида-Соломона, коды Файра и др. [2].

Особое внимание хотелось бы уделить кодам Боуза-Чоудхури-Хоквингема (БЧХ-коды) − это широкий класс циклических кодов, применяемых для защиты информации от ошибок.

Данный подход отличается возможностью построения кода с заранее определёнными корректирующими свойствами, выраженными минимальным кодовым расстоянием.

Частным случаем БЧХ-кодов является код Рида-Соломона.

Для нахождения порождающего полинома необходимо выполнить несколько этапов:

- выбрать поле $GF(q)$, над которым будет построен код;

- выбрать длину n кода из условия $n = (q^m - 1) / s$, где m, s – целые положительные числа;

- задать величину d конструктивного расстояния;

- построить циклотомические классы элемента $\beta = \alpha^s$ поля $GF(q^m)$ над полем $GF(q)$, где α − примитивный элемент $GF(q^m)$;

- поскольку каждому такому циклотомическому классу соответствует неприводимый полином над $GF(q)$, корнями которого являются элементы этого и только этого класса со степенью равной количеству элементов в классе, то выбрать $\beta^{i_0}, \beta^{i_0+1}, \dots, \beta^{i_0+d-2}$ таким образом, чтобы суммарная длина циклотомических классов была минимальна;

- вычислить порождающий полином $g(x) = f_1(x)f_2(x) \dots f_n(x)$, где $f_i(x)$ – полином, соответствующий i-ому циклотомическому классу.

Рассмотрим пример построения БЧХ-кода с длиной кодовых слов n = 15 и минимальным расстоянием между кодовыми словами d = 5.

Степень примитивного многочлена равна $q = \log_2(n+1) = 4$, следовательно, $q = x^4 + x^3 + 1$. Пусть α – его корень, тогда α^2 и α^4 – также его корни. Минимальным многочленом для α^3 будет $x^4 + x^3 + x^2 + x + 1$. Следовательно, $g(x) = НОК(x^4 + x^3 + 1, x^4 + x^3 + x^2 + x + 1) = (x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1) = x^8 + x^4 + x^2 + x + 1$.

Степень полученного многочлена равна 8, следовательно, построенный БЧХ-код будет (7, 15)-кодом.

Слово 1000100 или $\alpha(x) = x^4 + 1$ будет закодировано кодовым словом $\alpha(x)g(x) = x^{12} + x^6 + x^5 + x^2 + x + 1$ или 111001100000100.

В настоящее время циклический код широко используется при кодировании и декодировании передаваемой информации. Особое распространение данный код получил в сфере телекоммуникаций. На практике, как правило, применяются циклические коды, корректирующие ошибки невысокой кратности, это обусловлено высокими аппаратурными и временными затратами на схемы коррекции, которые резко возрастают при увеличении кратности исправляемых ошибок.

Библиографический список

1. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации: учебник для вузов / Бройдо О.П., Ильина В.Л. СПб.: Питер, 2011. 560 с.

2. Золотарев В.В., Овечкин Г.В. Помехоустойчивое кодирование. Методы и алгоритмы: справочник / под. ред. чл.-кор. РАН Ю.Б. Зубарева. М.: Горячая линия – Телеком, 2004. 126 с.

Столярова Мария Игоревна
Пензенский государственный университет, г. Пенза, Россия

Stolyarova M.I.
Penza State University, Penza, Russia

Бобрышева Галина Владимировна
Пензенский государственный университет, г. Пенза, Россия
E-mail: g_bobr@mail.ru

Bobrysheva G.V.
Penza State University, Penza, Russia

Звозникова Галина Олеговна
Пензенский государственный университет, г. Пенза, Россия

Zvoznikova G.O.
Penza State University, Penza, Russia