СВОЙСТВА НЕ ПРИМИТИВНЫХ РЕВЕРСИВНЫХ КОДОВ

В.А. Липницкий, А.В.Кушнеров
Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
Белорусский национальный технический университет
пр. Независимости 4, г. Минск, 220000, Республика Беларусь

E-mail: valipnitski@yandex.rue, lysander180@mail.ru

Ключевые слова: помехоустойчивое кодирование, код Хемминга, БЧХ-код, реверсивный код, минимальное расстояние кода.

Помехоустойчивое кодирование служит для передачи и хранения информации. Цель кодирования – противостояние ошибкам, которые зачастую возникают в каналах с шумами. Под каналом следует понимать любую физическую среду передачи данных.

Основная задача кода – исправление ошибок и на практике все просто: чем больше ошибок код способен исправить – тем он лучше. Пусть минимальное расстояние кода равно $d = 2t + 1$, тогда код способен скорректировать до t ошибок. Таким образом, основным показателем корректирующих способностей кода является минимальное расстояние кода, то есть наименьшее расстояние между кодовыми словами в метрике Хемминга [1]. К сожалению, нахождение кода с приемлемым минимальным расстоянием — достаточно трудоемкая вычислительная и исследовательская работа.

БЧХ-коды – наиболее популярное на практике и наиболее исследованное семейство линейных помехоустойчивых кодов. Если быть точным, то сказанное относится к примитивным БЧХ-кодам. В докладе речь пойдет о не примитивных БЧХ-кодах, неоправданно обойденных теорией и практикой. Дело в том, что их свойства и поведение достаточно хаотично меняются при переходе от одной длины к другой. Белорусской школой помехоустойчивого кодирования ведется систематическое исследование и в некотором роде реабилитация не примитивных БЧХ-кодов [2, 3].

Аналогична ситуация с реверсивными кодами. Их можно отнести к семейству БЧХ-кодов. Однако не примитивные реверсивные коды остаются практически не исследованными. В данном докладе приводятся некоторые результаты о найденных свойствах не примитивных реверсивных кодов.

Всякий реверсивный код C_R определен над полем Галуа $GF(2^m)$ из 2^m элементов, $m > 2$, имеет нечетную длину m, являющуюся делителем числа $2^m - 1$, а также размерность $k = n - 2m$. Код C_R однозначно задается своей проверочной матрицей $H = (\beta^i, \beta^{-i})^T$, $0 \le i \le n-1$, $2m < n$, $\beta = \alpha^\tau$ для примитивного элемента α поля $GF(2^m)$, $\tau = (2^m - 1)/n$. При $n = 2^m - 1$ величина $\beta = \alpha$ и код C_R называется примитивным. Для каждого нечетного n, в силу теоретико-числовой теоремы Эйлера, существует свое поле определения, то есть поле $GF(2^m)$ с минимальным m, обеспечивающим делимость $(2^m - 1)$ на n. Однако при этом может оказаться, что $2m > n$. В таких редких случаях код C_R не существует. Для каждого нечетного n существует свое поле определения $GF(2^m)$, для каждого значения n это поле определения и условия существования приходится вычислять отдельно [1,2].

В процессе исследований доказана следующая

Теорема 1 *Для каждого натурального делителя $s > 1$ числа n в коде C_R найдется кодовое слово весом s.*

Минимальное расстояние d кода C_R находится в диапазоне от 3 до s^* , где s^* — наименьший из делителей $s > 1$ числа n. Если n делится на 3, то $d = 3$.

Из данного следствия вытекает известный факт, что $d = 3$ для всех примитивных кодов над полями определения $GF(2^m)$ с четным показателем m.

В каждом случае, кода $s^* > 3$, точное значение минимального расстояния d находится путем достаточно скрупулезных вычислений. Сложность вычислений зависит как от длины n, так и от величины m. В основном, приходилось комбинировать следующие четыре метода: вычисление таблицы весов кода C_R или начального фрагмента этой таблицы; комбинаторный метод, базирующийся на теореме о рангах систем столбцов проверочной матрицы [1]; метод синдромов; норменный метод [2]; метод G-орбит для подгруппы G группы автоморфизмов кода C_R, порожденной циклическими и циклотомическими подстановками [2].

Наиболее интересные результаты для кодов C_R из рассматриваемого диапазона представлены в нижеприведенной таблице. Приведенные в таблице не примитивные реверсивные коды имеют хорошие декодирующие возможности и эффективны для применения на практике.

Таблица 1 – Результаты исследования

Параметры кода	Размерность кода	Минимальное расстояние	Корректирующая способность
$n = 31$ $m = 5$	21	5	5
$n = 43$ $m = 14$	15	6	2
$n = 73$ $m = 9$	55	6	2
$n = 89$ $m = 11$	67	6	2
$n = 49$ $m = 21$	7	7	3
$n = 77$ $m = 30$	17	7	3
$n = 91$ $m = 12$	67	6	2
$n = 109$ $m = 36$	37	≥ 8	≥ 3

1. Мак-Вильямс Ф.Дж. Теория кодов, исправляющих ошибки / Ф.Дж. Мак-Вильямс, Слоэн Н.Дж.А. // М.: Радио и связь, 1979. — 744.
2. Липницкий В.А. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения / В.А. Липницкий, В.К. Конопелько // Мн.: БГУ, 2007. — 214.
3. Lipnitski V. Non-primitive Hamming Codes // p. 73 - 75. // Modeling and Simulation // MS'2012 / Proc. of the Intern. Conf., 2 — May 2012, Minsk, Belarus. — Minsk: Publ. Center of BSU, 2012. — 178 p.
4. Курилович А.В. Не примитивные коды Боуза-Чоудхури-Хоквигнгема и их основные параметры / А.В. Курилович, В.А. Липницкий, Л.В. Михайловская // Технологии информатизации и управления : Сб. науч. ст. Вып. 2 / редкол.: А.М. Кадан (отв. ред.) [и др.]. — Минск, БГУ, 2011. — 43-49.
5. Липницкий В.А. Теория норм синдромов / В.А.Липницкий // Мн.: БГУИР, 2010. — 108.