

ОПРЕДЕЛЕНИЕ НОРМ СИНДРОМА БЧХ-КОДА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Пригон А.Н.

Конопельно В.К. – к.т.н., доцент, профессор

В современных инфокоммуникационных системах используется помехоустойчивое кодирование для уменьшения влияния ошибок на передаваемую информацию. Развитие элементной базы открывает возможность реализовывать сложные, недоступные ранее алгоритмы декодирования, имеющие более качественные параметры. Вычислительный эксперимент показывает, что примерно треть исследуемых кодов обладает корректирующими возможностями, большими конструктивными, и перспективна для применения. Они становятся востребованными в системах передачи информации, требующих высокой надежности передачи информации.

Коды Боуза-Чоудхури-Хоквингема являются результатом обобщения кодов Хэмминга, которые позволяют исправлять множественные ошибки. Они составляют класс циклических кодов, который обеспечивает достаточную свободу выбора длины блока, скорости кода и возможностей коррекции ошибок. Коды БЧХ превосходят своими качествами все другие блочные коды с той же длиной блока и степенью кодирования. В наиболее часто применяемых кодах БЧХ используется двоичный алфавит и блок кодового слова длиной $n = 2m - 1$, где $m = 3, 4, \dots$. Относительно широкий максимум эффективности кодирования, в зависимости от степени кодирования при фиксированном n , для этих кодов находится между скоростью кодирования $1/3$ и $3/4$.

Норменное декодирование базируется на систематической классификации векторов ошибок в блочных кодах, анализе спектров синдромов ошибок и норм синдромов примитивных и непримитивных БЧХ-кодов. В основу классификации ошибок положено группа Γ циклических сдвигов, принадлежащая группе автоморфизмов многих линейных кодов. Благодаря этому векторы ошибок, переходящие друг друга посредством циклических сдвигов, образуют один класс эквивалентности – Γ -орбиту. Понятие нормы синдрома N введено для произвольных БЧХ-кодов, как примитивных, так и непримитивных, являющейся константой для кодов (в узком смысле) с минимальным расстоянием $d=5$ и вектором при $d \geq 7$. Γ -орбиты с попарно различными нормами содержат ошибки с непересекающимися спектрами синдромов и можно подобрать набор Γ -орбит, исчерпывающий весь спектр синдромов и, следовательно, декодировать любую ошибку из этого набора. Это позволяет при заданном d исправлять существенно большее число ошибок, не корректируемых известными методами, на основе одних и тех же достаточно простых декодеров.

Основное свойство норм синдромов отражает то, что для всякого вектора ошибок \bar{e} и его синдрома $S(\bar{e})$ в БЧХ-коде C справедливо равенство $\bar{N}(S(\sigma(\bar{e}))) = \bar{N}(S(\bar{e}))$. Это же равенство справедливо и для реверсивных кодов C_R^{2r+1} . Все векторы каждой Γ -орбиты имеют одинаковую норму синдрома, то есть норма синдрома инвариантна относительно группы Γ циклических сдвигов. Нормой $N(J)$ Γ -орбиты J векторов-ошибок в любом БЧХ-коде, а так же и в реверсивном коде, называется норма синдрома любого вектора-ошибки из этой Γ -орбиты.

Норма Γ -орбиты является ее однозначной характеристикой, то есть идентификатором этой орбиты и спектры синдромов таких Γ -орбит не пересекаются. I и J – две Γ -орбиты векторов-ошибок с одинаковыми нормами в примитивном двоичном БЧХ-коде C_{2r+1} (в реверсивном коде C_R^{2r+1}). Пусть I – полная Γ -орбита с полным спектром синдромов. Тогда для всякого вектора $\bar{f} \in J$ найдется вектор $\bar{e} \in I$, такой, что $S(\bar{e}) = S(\bar{f})$.

Множество Γ -орбит всех векторов-ошибок весом 1-3 имеет в примитивном двоичном БЧХ-коде C_7 попарно различные нормы. Множество Γ -орбит всех векторов-ошибок весом 1-2 имеет в примитивном двоичном БЧХ-коде C_5 попарно различные нормы.

Основные свойства нормы синдрома:

- у всех векторов-ошибок отдельно взятой Γ -орбиты норма синдрома одна и та же; норма синдрома является характерным признаком, меткой каждой Γ -орбиты;
- если у двух полных Γ -орбит совпадают нормы, то и множества синдромов векторов-ошибок этих орбит также совпадают;
- синдромы всех корректируемых векторов-ошибок попарно различны; следовательно, нормы синдромов Γ -орбит ошибок любой корректируемой совокупности имеют попарно различные нормы.

Список использованных источников:

1. Липницкий В. А., Олексюк А. О. Теория норм синдромов и плюс-декодирование // БГУИР. 2014. № 8. С. 71–78.
2. Липницкий В. А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа. 2-е изд. Минск : БГУИР, 2006.
3. Конопельно В. К. Норменное декодирование помехоустойчивых кодов. Минск : БГУ, 2007.
4. Лидл Р., Нидеррайтер Г. Конечные поля : в 2 т.: пер. с англ. М. : Мир, 2004.