О СФЕРИЧЕСКИХ КОДАХ И МЕТОДАХ ИХ ПОСТРОЕНИЯ

Белов С.В.
Оренбургский государственный университет, г. Оренбург

Пусть S^{n-1} означает сферу радиуса *1* с центром в начале координат евклидова пространства R^n. Конечное число точек $X \subset S^{n-1}$ будем называть сферическим кодом с параметрами n, ρ, M (и обозначим $X:(n,\rho,M)$). Размерность n – это размерность пространства над R, натянутого на точки X Параметр ρ обозначает квадрат минимального евклидова расстояния между точками X.

$$p = \rho(X) = \min\{\rho(x,y) : x \neq y, x, y \in X\}, \tag{1}$$

где $\rho(x,y) = \sum_{i=1}^{n}(x_i - y_i)^2, x = (x_1,\ldots,x_n), y = (y_1,\ldots,y_n)$.

Параметр M обозначает мощность кода, или просто число кодовых точек $M = |X|$.

Сферические коды связаны с проблемой упаковки шаров, имеющей приложения в различных областях, таких как теория чисел, алгебры Ли, численное вычисление интегралов, геометрия, физика, цифровая связь, проектирование антенн, статический анализ, химия, биологии.

Особую роль играют практические и теоретические приложения к задачам цифровой связи. В частности, сферические коды находят свое применение в проектировании сигналов по каналу с шумом. В связи с этим актуальным является вопрос построения сферических кодов.

В литературе рассматриваются различные методы построения сферических кодов. Ещё в 1971 году в работе [1] Лич и Слоэн привели примеры построения сферических кодов на основе двоичных блоковых кодов. В фундаментальной работе Дж. Конвея и Н. Слоэна, посвященной различным аспектам проблемы упаковки шаров, также рассматриваются вопросы получения сферических кодов. Существует ряд работ, посвященных конструкциям кодов. Так, в работе [2] представлены конструкции, позволяющие улучшить нижние оценки мощности сферических кодов с $p < 1$ для размерностей $n \leq 64$. Статья [3] содержит описание конструкции для сферических кодов конечной размерности *n*, основанной на двух семействах двоичных кодов: кодах постоянного веса и обычных блоковых кодах.

Анализ публикаций, посвященных алгоритмам построения сферических кодов, позволяет выделить некоторые группы методов, основанных на общих принципах и идеях их построения. Первую группу объединяет общая идея, основанная на перестановках.

Перестановочная модуляция – один из старых методов построения сферических кодов. Метод очень прост и имеет два варианта выполнения.

Возьмем произвольный вектор $x_0 = (x_{01}, x_{02}, \ldots, x_{0N})$ с вещественными значениями и единичной нормой и построим все возможные перестановки этого вектора. Множество векторов, построенных таким образом, является сферическим кодом. Такая конструкция известна как перестановочная модуляция первого типа. Если в дополнение также допускаются все возможные изменения знаков, то такая конструкция называется перестановочной модуляцией второго типа. Оба типа производят коды со свойствами, которые легко описываются, легко исследуются и легко реализуются а, главное, для них декодирование методом максимального правдоподобия выполняется при помощи простого алгоритма. Следует отметить, что эффективность данных кодов быстро ухудшается с ростом размерности. Для размерностей больше 6 хорошие коды не производятся. Исключением являются симплекс и биортогональные коды, которые всегда строятся как частные случаи.

К следующей группе можно отнести коды, которые получаются из объединения двух и более кодов. Иногда таким образом можно построить хорошие коды даже из кодов, которые по отдельности не очень хороши. Чтобы оценить параметры сферического кода, построенного как объединение двух или более известных кодов, необходима подходящая оценка минимального расстояния между составляющими кодами.

Ещё одна группа методов имеет название «расширение кодов». Применение алгоритмов, основанных на идее расширения, позволяет довольно часто получать хорошие коды. Его также иногда называют «расширенное объединение».

Пусть $Y = \{y_1, y_2, \ldots, y_m\}$ будет сферическим кодом с размерностью n_2. Предположим, что для каждого кодового слова $y_i \in Y$ мы имеем сферические коды X_i, каждый из которых имеет размерность n_1. Расширение Y кода с добавлением кода $X_i, i = 1,2,\ldots,m$ это следующий код

$$Z = \bigcup_{i=1}^{m} (X_i \sin\theta_i, y_i \cos\theta_i), \tag{2}$$

где θ_i – параметры, которые должны быть оптимизированы. Термин «расширение» обусловлен тем, что это простая модификация объединения. Можно рассматривать код Y как средство увеличения расстояния между подкодами путем добавления идентификационного окончания для каждого подкода. Разумеется, у такого увеличения расстояния есть и обратная сторона, размерность результирующего кода увеличивается с n_1 до $n_1 + n_2$ и энергия кодов X_i должна быть уменьшена, с неизбежным следствием в виде уменьшения соответствующего минимального расстояния. Тем не менее, этот метод производит хорошие коды.

Частным случаем сферического кода является равновесный код. Равновесными принято называть коды, каждая комбинация которых содержит одно и то же число r отличных от нуля символов. Простейшие из них, так называемые двоичные биортогональные коды, имеют вид

$$x_1, x_2, \ldots, x_m, x_1 + 1, x_2 + 1, \ldots, x_m + 1 \quad (3)$$

(к каждой комбинации безызбыточного кода дописывается комбинация, отличающаяся от нее точно в m позициях). Видно, что любая комбинация содержит точно m единиц, а $d = 2$. В биортогональных кодах обнаруживаются все ошибки, кроме ошибок, приводящих одновременно к трансформации одинакового числа нулей и единиц.

Максимальное число m-значных комбинаций веса r равно

$$M_r = (b-1) r C_m^r. \quad (4)$$

Такие множества также представляют собой равновесные коды. В бинарном случае $b = 2$ их комбинации отличаются не менее чем в двух позициях, а для $b \geq 3$ кодовое расстояние равно 1.

Равновесный код применяется при передаче данных внутри устройств машины и по каналам связи. Особенностью равновесного кода является то, что в нем каждая информационная комбинация содержит фиксированное число единиц и нулей. Отличаются комбинации только позициями единиц.

Этот код получается путем добавления пятого разряда к тетраде, изображающей десятичную цифру. Код имеет высокую корректирующую способность при обнаружении асимметричных ошибок, т.е. когда происходит инверсия только единиц или только нулей. Ошибка не сможет быть обнаружена, если количество переходов нулей в единицу будет равно количеству переходов единиц в нули. Другими словами, признаком ошибки здесь является изменение количества единиц в комбинации. Избыточность равновесного кода «2 из 5» выше, чем у обычного двоично-десятичного кода. Добавление пятого разряда увеличивает число возможных комбинаций ($2^5 = 32$), однако для изображения цифр используется только 10, которые выбираются так, чтобы минимальное кодовое расстояние было равно 2. Поскольку для отображения информации используется меньше половины всех возможных комбинаций, корректирующая способность рассматриваемого кода выше, чем у обычного кода с проверкой на четность. Код «2 из 5» обнаруживает одиночные и групповые асимметричные ошибки. В некоторых машинах были попытки применить равновесный код «2 из 7». Однако резкое увеличение избыточности не повышает корректирующую способность этого кода, так как его минимальное кодовое расстояние остается тем же, т. е. равным 2. В то же время увеличение количества знаков в коде приводит к увеличению вероятности появления не обнаруживаемых симметричных ошибок.

Список литературы

1. Leech John, Sloane N.J.A. Sphere Packingsandl Error-Correcting Codes // Canadian J. Mathematics. 1971. V. 23. N4 . P. 718-745 .

2. Зиновьев В. А., Эриксон Т. Новые упаковки на евклидовой сфере для конечных размерностей //Проблемы передачи информации. – 1992. – Т. 28. – №. 2. – С. 47-53.

3. Додунеков С. М., Зиновьев В. А., Эриксон Т. Каскадный метод построения сферических кодов в n-размерном евклидовом пространстве //Проблемы передачи информации. – 1991. – Т. 27. – №. 4. – С. 34-38.

4. Зиновьев В. А., Эриксон Т. Новые нижние оценки на контактное число для небольших размерностей //Проблемы передачи информации. – 1999. – Т. 35. – №. 4. – С. 3-11.

5. Конвей Дж. Слоэн Н.. Упаковки шаров, решетки и группы. – Мир, 1990.

6. Юдин Н. Арифметический минимум квадратичной формы и сферические коды. – 1998.

7. Бородин Л. Ф. Введение в теорию помехоустойчивого кодирования. – 1968.