Телекоммуникационные технологии

Канальное кодирование, исправляющее ошибки

Введение

Линейные коды

Циклические коды

Коды

Линейные коды $c = a\mathbb{G}$

Систематические коды $c = [m||k]$

Циклические коды $\mathbb{C} = \begin{bmatrix} c_1 & c_2 & c_3 & \dots & c_N \\ c_2 & c_3 & \dots & c_N & c_1 \\ & & \vdots & & \\ & \dots & & & \end{bmatrix}$

Кодовое расстояние

Theorem

Кодовое расстояние линейного кода равно минимальному весу ненулевого кодового слова.

Theorem

Мощность линейного (n, k) *- кода равна* 2^k.

Линейные коды

Пусть $V \in B^n$ - линейный (n, k) - код.
Линейный код - непустое множество двоичных слов длины n, называемых кодовыми словами, такое, что сумма двух кодовых слов является кодовым словом.
В любом линейном коде нулевое слово $0 = 0...0$ выполняет роль нуля.
В линейном двоичном коде каждое слово противоположно самому себе, так как $c \oplus c = 0...0$ для любого $c \in B_n$, где булево пространство B_n, $B = \{0, 1\}$, представляет собой множество двоичных векторов длины n.
V является подпространством линейного пространства B^n, для задания линейного кода достаточно задать его базис.

Порождающая матрица

$$c = a\mathbb{G}$$

$$\mathbb{G} = \begin{bmatrix} \mathbb{I} & | & \mathbb{P} \end{bmatrix}$$

код Хэмминга -линейный блочный систематический циклический бинарный код. Исправляет 1 ошибку.

Порождающая матрица $\mathbb{G}$

Линейный код задается как пространство строк порождающей матрицы.
Матрица $\mathbb{G}$, состоящая из всех базисных векторов линейного кода V, называется порождающей матрицей кода.
Строки $\mathbb{G}$ линейно независимы, и число k строк равно размерности кода.
Таким образом, порождающая матрица (n, k) - кода имеет размерность $k \times n$. .

Ортогональное дополнение

Поскольку линейный код V является подпространством, то для него существует ортогональное дополнение (или нулевое подпространство).
Ортогональное дополнение V' (n, k) - кода V состоит из всех векторов длины n, ортогональных к каждому вектору $v \in V$.
Ортогональное дополнение также является подпространством и является линейным кодом.
Ортогональное дополнение $V'(n, k)$ - кода V имеет размерность $(n - k)$; соответственно любой его базис состоит из $(n - k)$ векторов.

Проверочная матрица $\mathbb{H}$

Порождающая матрица ортогонального дополнения называется проверочной матрицей кода V.
Т. к. проверочная матрица состоит из базисных векторов ортогонального дополнения, то двоичный вектор c является кодовым словом, если и только если $c\mathbb{H}^T = 0$.

Таблица декодирования. Стандартное расположение

Пусть V - линейный код (n, k) - код, v - нулевой вектор и $v_1, v_2, ..., v_{m-1}$ - остальные кодовые вектора.
Стандартное расположение имеет вид:

$$\begin{bmatrix} v & v_1 & v_2 & \cdots & v_{m-1} \\ g_1 & v_1 \oplus g_1 & v_2 \oplus g_1 & \cdots & v_{m-1} \oplus g_1 \\ g_2 & v_1 \oplus g_2 & v_2 \oplus g_2 & \cdots & v_{m-1} \oplus g_2 \\ \cdots & & & & \\ g_t & v_1 \oplus g_t & v_2 \oplus g_t & \cdots & v_{m-1} \oplus g_t \end{bmatrix}$$

$$m = 2^k, t = 2^{(n-k)-1}$$

Так как линейный код V является подгруппой группы $(B_n, +)$ это разложение группы B_n по подгруппе V.

Таблица декодирования. Стандартное расположение

Строки таблицы являются смежными классами, а векторы в первом столбце - образующими смежных классов. Принятый двоичный вектор декодируется в кодовый вектор, находящийся в **первой строке** столбца, в котором находится принятый вектор.

Theorem

Если в качестве таблицы декодирования используется стандартное расположение, то ошибка будет исправлена тогда и только тогда, когда вектор ошибки совпадает с образующим смежного класса.

Theorem

Если стандартное расположение используется в качестве таблицы декодирования, то ошибка будет исправлена с наибольшей вероятностью, если и только если в качестве представителя смежного класса выбирается вектор с минимальным весом в данном классе.

Theorem

Все векторы из одного смежного класса стандартного расположения имеют одинаковый синдром $s = u\mathbb{H}^T$, присущий только этому смежному классу.

Циклический код

Пространство V наборов длины n называется циклическим подпространством или циклическим кодом, если для любого вектора $v = (a_{n-1}, a_{n-2}, ..., a_0)$ из пространства V вектор $v' = (a_0, a_{n-1}, a_{n-2}, ..., a_1)$, получаемый в результате циклического сдвига компонент вектора v на единицу вправо, также принадлежит подпространству V.
Всякий циклический код является линейным, и может быть описан посредством порождающей и/или проверочной матрицы.
Однако циклические коды можно описать с помощью многочленов, по степеням формальной переменной x.

Классы вычетов многочленов степени n над полем $\mathrm{GF(2^n)}$

Каждому двоичному набору длины n можно поставить в соответствие многочлен с коэффициентами из простого поля Галуа $\mathrm{GF}_2 = \{0, 1\}$.
Каждому двоичному набору $(r_{n-1}, r_{n-2}, ..., r_0)$ длины n соответствует многочлен $r(x) = r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + ... + r_0x^0$,из множества многочленов с коэффициентами из $\mathrm{GF}_2 = \{0, 1\}$ (класс вычетов), остаток от деления которых на многочлен $f(x)$ равен $r(x)$.

Порождающий многочлен циклического кода

В алгебре классов вычетов по модулю многочлена x^{n+1} подпространство V является циклическим тогда и только тогда, когда V содержит все классы вычетов, представители которых кратны некоторому многочлену $g(x)$. Более того, многочлен $g(x)$ является делителем многочлена $x^n + 1$.

Кодирование циклическим кодом

Пусть циклический $(n, n-k)$-код порождается многочленом $g(x)$, который является делителем многочлена $x^n + 1$, и степень $g(x)$ равна $k < n$.

$$a = (a_{n-k-1}, a_{n-k-2}, \dots, a_0)$$

в виде многочлена

$$a_{n-k-1}x^{n-k-1} + a_{n-k-2}x^{n-k-2} + \dots + a_0$$

и умножить данный многочлен на $g(x)$.

Пример

Пусть $(7,4)$-код порожден многочленом $g(x) = x_3 + x_2 + 1$ и принято слово 1110111. По принятому слову строится многочлен $x_6 + x_5 + x_4 + x_2 + x + 1$, который делится на $g(x)$.
Поэтому можно сделать заключение, что при передаче ошибок не было, и переданное информационное слово есть вектор коэффициентов частного $x3 + x + 1$ от деления многочлена $x6 + x5 + x4 + x2 + x + 1$ на $g(x)$, т. е. вектор 1011.