Полиномиальные коды

Александра Игоревна Кононова

НИУ МИЭТ

20 декабря 2018 г.

Корректирующий код

Минимальная единица передачи по каналу связи — **символ** (элемент некоторого поля).

Каждый символ может быть искажён при передаче независимо от других.

При корректирующем кодировании в каждое **кодовое слово**, помимо **информационных** символов, вводят **проверочные**, или корректирующие.

Полиномиальные коды

Информационный полином (k символов)
$a(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1}$.

Порождающий полином $g(x)$ степени $m-1$ (m символов).

Полиномиальный код есть множество всех многочленов степени $m+k-2$ или меньше, делящихся на $g(x)$, т. е. $C(x) = g(x) \cdot A(x)$

Получаем $C(x) + err(x) = C'(x) = g(x) \cdot p(x) + r(x)$,
$r(x) = err(x) \bmod g(x)$ — **синдром**; $r(x) \neq 0$ — сбой.

Систематические и несистематические коды

Кодовое слово C ($n = k + m - 1$ символов) делится на $g(x)$:

несистематический код $C(x) = a(x) \cdot g(x)$;

систематический код (k информационных и $m - 1$ проверочных символов):
$C(x) = a(x) \cdot x^{m-1} - r(x)$,
где $r(x) = a(x) \cdot x^{m-1} \bmod g(x)$

Циклические коды

Циклическая перестановка символов в кодовом слове дает другое допустимое слово того же кода.

$C_1 = (c_0, c_1, \ldots c_{n-1})$
$C_2 = (c_{n-1}, c_0, c_1, \ldots c_{n-2})$
Таким образом, $C_2 = x \cdot C_1 - c_{n-1} \cdot (x^n - 1)$.

Необходимо, чтобы $x^n - 1$ делился на $g(x)$.
Проверочный многочлен h: $g(x)h(x) = 0 \mod x^n - 1$
$C(x)h(x) = a(x)g(x)h(x) = 0 \mod x^n - 1$

Двоичные циклические коды

Символы двоичных кодов — элементы $\mathrm{GF}(2)$.

Циклическая перестановка:
$C_2 = x \cdot C_1 - c_{n-1} \cdot (x^n - 1)$

Для символов из $\mathrm{GF}(2)$
либо $C_2 = x \cdot C_1$,
либо $C_2 = x \cdot C_1 - (x^n - 1)$, что эквивалентно
$C_2 = x \cdot C_1 + (x^n + 1)$;

$x^n + 1 = g(x) \cdot h(x)$, $h(x)$ — проверочный многочлен.

Бит чётности

Символ — бит: $a_i \in \mathrm{GF}(2)$

Порождающий полином $g(x) = x + 1$.

Бит чётности — циклический двоичный код.

Циклические коды Хэмминга над $\mathrm{GF}(2)$

Циклический n–код

$g(x)$ – произвольный, $\deg g < n$

↓

$g(x)$ – делитель $x^n - 1$

↓

$n = 2^M - 1$, $g(x)$ – примитивный, $\deg g = M$

Код Хэмминга

n	$g(x)$
1	1
3	?
7	$x^3 + x + 1$ $x^3 + x^2 + 1$

Циклические коды Хэмминга над $\mathrm{GF}(2)$

Циклический n–код

$g(x)$ – *произвольный*, $\deg g < n$

$\downarrow$

$g(x)$ – *делитель* $x^n - 1$

$\downarrow$

$n = 2^M - 1$, $g(x)$ – *примитивный*, $\deg g = M$

Код Хэмминга

n	$g(x)$
1	1
3	$x^2 + x + 1$
7	$x^3 + x + 1$
	$x^3 + x^2 + 1$

Порождающий полином

Корни порождающего полинома лежат в том же поле, над каким и строится код

Пусть β — элемент поля $\mathrm{GF}(q)$ порядка n (обычно выбирается примитивный элемент).

Тогда порождающий полином кода Рида—Соломона:

$$g(x) = (x - \beta^{l_0})(x - \beta^{l_0+1}) \ldots (x - \beta^{l_0+d-1})$$

где l_0 — некоторое целое число. Обычно $l_0 = 1$.

$\deg(g(x)) = d - 1$.

Длина кода

Длина полученного кода n,
минимальное расстояние m,
проверочных символов $\mu = m - 1 = \deg(g(x))$,
информационных символов $k = n - \mu = n - m + 1$.

Если β — примитивный элемент $\mathrm{GF}(q)$, то $n = q - 1$.
Количество проверочных μ однозначно определяет $g(x)$.
Исправляется до $\mu/2$ ошибок.

Декодирование систематического кода Рида-Соломона

Локатор ошибки — $X_i = \beta^\ell$ для x^ℓ. Многочлен локаторов $L(x) = (1 - xX_1)(1 - xX_2)...(1 - xX_u)$

- Остаток $e(x) = C(x) \mod g(x)$.
- Синдром $S(x) : s_i = e(\beta^{i+1}) = C(\beta^{i+1})$.
- Многочлен ошибок $W(x)$ — степень не превышает $u - 1$, где u — количество ошибок ($u \leqslant \mu/2$), причём $L(x) \cdot S(x) = W(x) \mod x^\mu$.
  Метод Берлекампа-Месси.
- Значения ошибок $Y_i = \frac{W(X_i^{-1})}{L'(X_i^{-1})}$.

Спасибо за внимание!

НИУ МИЭТ
http://miet.ru/

Александра Игоревна Кононова
illinc@mail.ru