Практическая 6

Теория информации

Циклические коды

I. Линейный код длины n называется *циклическим*, если для любого кодового слова $(x_1, x_2, \ldots, x_n)$ слово $(x_2, \ldots, x_n, x_1)$ также является кодовым. Подкольцо I кольца $F[x]/(x^n - 1)$ называется *идеалом*, если для любых многочленов $u(x) \in F[x]/(x^n - 1)$ и $c(x) \in I$ многочлен $u(x) \cdot c(x)$ принадлежит I.

Теорема. *Подпространство кольца $F[x]/(x^n - 1)$ является циклическим кодом тогда и только тогда, когда оно образует идеал.*

Приведенный многочлен наименьшей степени, принадлежащий циклическому коду, называется *порождающим* многочленом кода.

II. Код длины n размерности k называется *систематическим*, если после вычеркивания некоторых $(n - k)$ столбцов из его кодовой матрицы остаются в точности все различные векторы длины k.

III. *Минимальным многочленом* элемента β над полем $GF(p)$ называется приведенный многочлен $M(x)$ наименьшей степени такой, что $M(\beta) = 0$.

Свойства минимального многочлена $M(x)$ элемента β из $GF(p^m)$.

1. Многочлен $M(x)$ неприводим.
2. Если $f(x)$ – некоторый многочлен такой, что $f(\beta) = 0$, то $M(x)$ делит $f(x)$.
3. Многочлен $M(x)$ делит $x^{p^m} - x$.
4. Степень многочлена $M(x)$ не превосходит m.
5. Многочлен $M(x)$ минимальный для элементов β и β^p.

Цикломатические классы

Множество целых чисел по модулю $p^m - 1$ следующим образом распадается на подмножества, называемые *циклотомическими классами по модулю* $p^m - 1$: циклотомический класс, содержащий s, имеет вид $C_s = \{s, ps, p^2 s, p^3 s, \ldots, p^{m_s - 1} s\}$, где m_s – наименьшее положительное целое число такое, что $p^{m_s} \cdot s \equiv s (\mathrm{mod}(p^m - 1))$. Пусть $M^{(i)}(x)$ – минимальный многочлен элемента α^i из $GF(p^m)$, где α – примитивный элемент поля.

Цикломатические классы

6. Если i лежит в классе C_s, то справедливо $M^{(i)}(x) = \prod_{j \in C_s} (x - \alpha^j)$.

Из теоремы Ферма следует равенство

$$x^{p^m-1} - 1 = \prod_s M^{(s)}(x),$$

где s пробегает все множество представителей циклотомических классов по модулю $p^m - 1$.

- *Характеристической функцией* кода C называется булева функция $f : E^n \to \{0,1\}$ такая, что $f(x_1, \ldots, x_n) = 1$ тогда и только тогда, когда вектор $(x_1, \ldots, x_n)$ принадлежит коду C. Пусть $A(n,d)$ обозначает мощность максимального двоичного кода длины n с расстоянием d.

Циклический код

- *Циклический код* – такой групповой код, все базовые комбинации которого могут быть получены из одной путем циклического сдвига ее элементов.
- *Циклический сдвиг кодовой комбинации* – перемещение ее элементов справа налево без нарушения порядка их следования, так что крайний левый элемент занимает место крайнего правого.

Кодовые комбинации

- В теории циклических кодов принято записывать кодовые комбинации в виде полинома некоторой фиктивной переменной ***x***:

$$C_1 a_1 \oplus C_2 a_2 \oplus C_3 a_3 \oplus \ldots \oplus C_i a_i \oplus \ldots \oplus C_q a_q \neq 0$$

- где $\boldsymbol{a}^i$ – значение символа кодовой комбинации на позиции ***i*** при нумерации справа налево;
  $\boldsymbol{x}^i - 1$ – фиктивная переменная в степени номера позиции ***i*** без единицы.

Пример

- Представить в виде полинома кодовую комбинацию ***a*** ≈ 1011101.

$$a(x) = a^7x^{7-1} + a^6x^{6-1} + a^5x^{5-1} + a^4x^{4-1} + a^3x^{3-1} + a^2x^{2-1} + a^1x^{1-1} =$$

$$= a^7x^6 + a^6x^5 + a^5x^4 + a^4x^3 + a^3x^2 + a^2x + a^1 =$$

$$= 1 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 1 =$$

$$= x^6 + x^4 + x^3 + x^2 + 1.$$

Задание

Задание 1.

а) Представить в виде полинома кодовую комбинацию $\boldsymbol{\alpha} \approx 1001001$.

б) Представить в виде полинома кодовую комбинацию $\boldsymbol{\alpha} \approx 1101101$.

в) Представить в виде полинома кодовую комбинацию $\boldsymbol{\alpha} \approx 1010111$.

Порождающий полином

- Неприводимым называется многочлен, который не может быть представлен в виде произведения многочленов низших степеней, т. е. такой многочлен делится только на самого себя или на единицу и не делится ни на какой другой многочлен. На такой многочлен делится без остатка двучлен $x^n + 1$. Неприводимые многочлены в теории циклических кодов играют роль образующих полиномов.

Порождающая матрица

Можно записать порождающую матрицу циклического кода в следующем виде:

$$V = \begin{matrix} p(x) \\ p(x) \cdot x - C_2\,(x^n - 1) \\ p(x) \cdot x^2 - C_3\,(x^n - 1) \\ \dots \\ p(x) \cdot x^{m-1} - C_m\,(x^n - 1)\,, \end{matrix}$$

где $p(x)$ — исходная кодовая комбинация, на базе которой получены все остальные $(m - 1)$ базовые комбинации, $C_i = 0$ или $C_i = 1$ («0», если результирующая степень полинома $p(x) \cdot x^i$ не превосходит $(n - 1)$, «1», если превосходит).

Порождающий полином

Комбинация $p(x)$ называется порождающей (генераторной) комбинацией.

Для построения циклического кода достаточно верно выбрать $p(x)$. Затем все остальные кодовые комбинации получаются такими же, как и в групповом коде.

Порождающий полином должен удовлетворять следующим требованиям:

1. $p(x)$ должен быть ненулевым;
2. вес $p(x)$ не должен быть меньше минимального кодового расстояния: $v(p(x)) \geq d_{min}$;
3. $p(x)$ должен иметь максимальную степень k (k — число избыточных элементов в коде);
4. $p(x)$ должен быть делителем полинома $(x^n - 1)$.

Степень порождающего полинома

- Выполнение условия 4 приводит к тому, что все рабочие кодовые комбинации циклического кода приобретают свойство делимости на p(x) без остатка. Циклический код — код, все рабочие комбинации которого делятся на порождающий без остатка.
- Для определения степени порождающего полинома можно воспользоваться выражением $r \geq \log_2(n+1)$, где n — размер передаваемого пакета за раз, т. е. длина строящегося циклического кода.

Примеры порождающих полиномов

***r*,** **степень полинома**	***P*(*x*),** **порождающий полином**
2	111
3	1011
4	10011
5	100101, 111101, 110111
6	1000011, 1100111
7	10001001, 10001111, 10011101
8	111100111, 100011101, 101100011

Разрешенные кодовые комбинации

- Пусть задан полином $P(x) = a^{r-1} x^r + a^{r-2} x^{r-1} + \ldots + 1$, определяющий корректирующую способность кода и число проверочных разрядов r, а также исходная комбинация простого k-элементного кода в виде многочлена $A_{k-1}(x)$.
- Требуется определить разрешенную кодовую комбинацию циклического кода (n, k).

Алгоритм

1. Умножаем многочлен исходной кодовой комбинации на x^r: $A_{k-1}(x) \cdot x^r$
2. Определяем проверочные разряды, дополняющие исходную информационную комбинацию до разрешенной, как остаток от деления полученного в предыдущем пункте произведения на порождающий полином: $A_{k-1}(x) \cdot x^r / P_r(x) \Rightarrow R(x)$
3. Окончательно разрешенная кодовая комбинация циклического кода определится так: $A_{n-1}(x) = A_{k-1}(x) \cdot x^r + R(x)$
4. Для обнаружения ошибок в принятой кодовой комбинации достаточно поделить ее на производящий полином. Если принятая комбинация — разрешенная, то остаток от деления будет нулевым. Ненулевой остаток свидетельствует о том, что принятая комбинация содержит ошибки. По виду остатка (синдрома) можно в некоторых случаях также сделать вывод о характере ошибки, ее местоположении и исправить ошибку.

Пример

Закодировать комбинацию вида 1101, что соответствует $A(x) = x^3 + x^2 + 1$.

1. Определяем число контрольных символов $r = 3$. Из таблицы возьмем многочлен $P(x) = x^3 + x + 1$, т. е. 1011.
2. Умножим $A(x)$ на x^r:
3. $A(x) \cdot x^r = (x^3 + x^2 + 1) \cdot x^3 = x^6 + x^5 + x^3 \Rightarrow 11010000$
4. Разделим полученное произведение на образующий полином $g(x)$:
5. $A(x) \cdot x^r / P(x) = (x^6 + x^5 + x^3) / (x^3 + x + 1) = x^3 + x^2 + x + 1 + 1 / (x^3 + x + 1) \Rightarrow 1111 + 001 / 1011$
6. При делении необходимо учитывать, что вычитание производится по модулю 2. Остаток суммируем с $h(x) \cdot x^r$. В результате получим закодированное сообщение:
7. $F(x) = (x^3 + x^2 + 1) \cdot (x^3 + x + 1) = (x^3 + x^2 + 1) \cdot x^3 + 1 \Rightarrow 1101001$
8. В полученной кодовой комбинации циклического кода информационные символы $A(x) = 1101$, а контрольные $R(x) = 001$. Закодированное сообщение делится на образующий полином без остатка.

Задание2

а) Закодировать комбинацию вида 110.

б) Закодировать комбинацию вида 11010.

в) Закодировать комбинацию вида 1010.

г) Закодировать комбинацию вида 10111.

Определение ошибки

- Пусть имеем n-элементные комбинации ($n = k + r$) тогда:
- Получаем остаток от деления $E(x)$ соответствующего ошибке в старшем разряде [1000000000], на порождающий полином $P_r(x)$: $E_1(x) / P_r(x) = R_0(x)$
- Делим полученный полином $H(x)$ на $P_r(x)$ и получаем текущий остаток $R(x)$.
- Сравниваем $R_0(x)$ и $R(x)$.
  - Если они равны, то ошибка произошла в старшем разряде.
  - Если нет, то увеличиваем степень принятого полинома на x и снова проводим деления: $H(x) \cdot x / P_r(x) = R(x)$

Определение ошибки

- Опять сравниваем полученный остаток с $R_0(x)$.
  - Если они равны, то ошибки во втором разряде.
  - Если нет, то умножаем $H(x) \cdot x^2$ и повторяем эти операции до тех пор, пока $R(x)$ не будет равен $R_0(x)$.
- Ошибка будет в разряде, соответствующем числу, на которое повышена степень $H(x)$, плюс один.
- Например: $H(x) \cdot x^3 \,/\, P_r(x) = R_0(x)$

Пример

- Полином $g(x) = 1 + x^2 + x^3$ генерирует бинарный (7,4)-циклический код, $d_{min} = 3$ (т.е. 1-ошибку исправляет). Рассмотрим кодовое слово $1 + x + x^5 = (1 + x + x^2)\, g(x)$. Пусть после передачи многочлен $R(x) = 1 + x + x^5 + x^6$ был получен.
- Декодируем его. Разделим $R(x)$ на $g(x)$ для нахождения синдрома, $R(x) = (x^3 + 1)g(x) + (x + x^2)$,
- так $S(x) = x + x^2$.Так как вес $S(x) > 1$ (= t), вычислим синдром $s_1(x) * x^r(x)$. Так как $S(x) = 2 = n - k - 1$, умножаем $S(x)$ на x и делим на $g(x)$, что дает $s_1(x) = 1$.
- Поскольку вес 1, маска ошибки $e(x) = x^{7-1}(s_1,0) = x^6(1000000) = x^6$.
- Так как n = 7 все ошибки веса 1 имеют циклический сдвиг на шесть 0's и 6 > k = 4

Задание 3

- Принятая кодовая комбинация ЦК(7,4) имеет вид Bi'(X)=1101110. Определить и исправить ошибку в B i' (X),если она имеется.

Задание 4

- Выполнить кодирование чисел(даны в 10-й с.с.) циклическим кодом с заданным порождающим полиномом(дан в 8-й с.с.)

по вариантам

Задания по вариантам

№ варианта	Порождающий полином	Числа для кодирования
1	23	15
2	31	17
3	37	22
4	41	25
5	53	34
6	65	99
7	117	78
8	135	45
9	171	120
10	213	111
11	321	63
12	347	123
13	427	127
14	673	113

Учебные материалы

- http://yourtutor.narod.ru/cyclic/CyclicCodes.htm
- http://informkod.narod.ru/5_5item.htm
- http://peredacha-informacii.ru/ustrojstva-rekurrentnyh-kodov.htmlhttp://peredacha-informacii.ru/ustrojstva-rekurrentnyh-kodov.html
- http://estohard.narod.ru/InfoTeory/1/15/153.htm

Конец

- Если вы выполнили все задания, вы получаете 10 баллов