7 Циклические коды. Минимальный многочлен

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.

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.

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

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 $p^m - 1$.

7.1 Найти разложение многочлена $x^8 - x$ в произведение минимальных многочленов.

а) Какие элементы поля $GF(2^3)$, построенного с помощью неприводимого многочлена $x^3 + x + 1$, им отвечают?

б) Сколько двоичных циклических кодов длины 7 можно построить?

в) Найти порождающие и проверочные матрицы этих кодов.

7.2 Найти проверочный многочлен кода Хэмминга с порождающим многочленом $g(x) = x^4 + x + 1$.

7.3 Найти два систематических кодера для кода длины 7 с порождающим многочленом $g(x) = x^3 + x + 1$. С помощью второго систематического кодера закодировать вектор (1101).

7.4 Найти разложение многочлена $x^{10} - x$ на неприводимые многочлены над $GF(2)$.

7.5 Доказать, что для произвольного элемента β из $GF(p^m)$ минимальный многочлен $M_\beta(x)$ существует и единствен.

7.6 Пусть β — произвольный элемент поля $GF(p^m)$. Доказать, что если для некоторого многочлена $f(x) \in F[x]$ выполнено $f(\beta) = 0$, то минимальный многочлен $M_\beta(x)$ делит $f(x)$.

7.7 Доказать, что минимальный многочлен $M_\beta(x)$ произвольного элемента β из $GF(p^m)$ делит многочлен $x^{p^m-1} - 1$.

7.8 Доказать, что степень минимального многочлена любого элемента поля $GF(p^m)$ не превосходит m.

7.9 Доказать, что степень минимального многочлена примитивного элемента поля $GF(p^m)$ равна m.

Теория к Семинару 8 "Циклические коды (продолжение). Нелинейные коды".

I. Декодирование циклических кодов. Циклическое представление кода Хэмминга. Теорема о границе БЧХ. Определение кодов БЧХ.

II. Повторить свойства кода исправлять и обнаруживть ошибки, границы объемов кодов из семинара 3.