Федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский университет
«Высшая школа экономики»

Факультет математики

Беребердина Наталья Александровна

Вычетно-квадратичные коды

Курсовая работа студента 3 курса

образовательной программы бакалавриата «Математика»

Научный руководитель:

Гриценко Валерий Алексеевич
Профессор: Факультет математики
Доктор физико-математических наук

Москва 2023

Содержание

1 Введение

1.1 Описание работы

В этой работе мы поговорим о вычетно-квадратичных кодах над полями $GF(l)$ для простых l и над кольцами ($\mathbb{Z}_{2^n}$. В частности опишем для этих кодов порождающие идемпотенты, порождающие и проверочные матрицы.

2 Вычетно-квадратичные коды над полями $GF(l)$

2.1 Общие сведения об устройстве циклических кодов над $GF(l)$

В этом разделе мы поговорим о некоторых важных свойствах циклических кодов и введем определение вычетно-квадратичного кода над полем.

Рассмотрим простое конечное поле F и $F[x]$ — кольцо всех многочленов от переменной x с коэффициентами из поля F. Тогда $F[x]/(x^n - 1)$ - фактор-множество классов вычетов по модулю $x^n - 1$ является кольцом, но не является полем при $n > 1$, так как $(x-1)|(x^n-1)$.

Сопоставив каждому многочлену кодовое слово с помощью изоморфизма

$$c(x) = c_0 + c_1x + c_2x^2 + ... + c_{n-1}x^{n-1} \leftrightarrow c = (c_0, c_1, c_2, ..., c_{n-1})$$

мы можем сформулировать следующую теорему.

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

Кроме того мы знаем что если F поле, то кольцо многочленов $F[x]$ является кольцом главных идеалов. Докажем следующую лемму.

Лемма 1. Если кольцо многочленов $F[x]$ является кольцом главных идеалов, то подпространство кольца $F[x]/(x^n - 1)$ также является кольцом главных идеалов.

Доказательство. Для начала заметим, что $F[x]/(x^n - 1)$ замкнуто по умножению, так как $(x^n - 1)F[x]$ является двусторонним идеалом и замкнуто по сложению, так как является фактор-группой по сложению. Таким образом $F[x]/(x^n - 1)$ действительно кольцо. Теперь рассмотрим в нем произвольный идеал I. Тогда для любого элемента фактор-кольца f выполнено $fi \in I, \forall i \in I$. Тогда для любых $f + k_1x^{n-1}, i + k_2 * x^{n-1} \in F[x]$ выполнено:

$$(f + k_1x^{n-1}) * (i + k_2 * x^{n-1}) = fi + x^{n-1} * (k_1i + k_2f + k_1k_2 * x^{n-1})$$

Таким образом мы получили, что если I - идеал $F[x]/(x^n - 1)$, то $\mathcal{I}$ - праобраз I в кольце $F[x]$ тоже идеал, но тогда $\mathcal{I}$ порождается элементом α, а значит и I порождается элементом α. Таким образом, I - главный идеал, а $F[x]/(x^n - 1)$ - кольцо главных идеалов.

Теперь мы можем рассмотреть два способа задания циклического кода многочленом: с помощью нормированного порождающего многочлена наименьшей степени и идемпотентного многочлена.

Лемма 2. Циклический код содержит единственный ненулевой нормированный многочлен наименьшей степени.

Доказательство. Пусть существуют два нормированных многочлена $f(x)$ и $g(x)$ наименьшей степени r. Тогда многочлен $f(x) - g(x)$, принадлежащий коду, имеет степень меньше r, что приводит к противоречию.

Сформулируем ниже две теоремы, позволяющие нам задавать код C его порождающим многочленом, т.е. многочленом $g(x)$ таким, что $c \in C$ тогда и только тогда, когда $c = f(x)g(x)$ для некоторого $f(x) \in F[x]/(x^n - 1)$.

Теорема 2. Циклический код состоит из всех многочленов вида $f(x)g(x)$, где $g(x)$ — ненулевой нормированный многочлен наименьшей степени.

Пусть есть $s(x) \in C$. Поделим его с остатком на $g(x)$, например алгоритмом Евклида. Получим

$$s(x) = f(x)g(x) + r(x),$$

где $deg(r(x)) < deg(g(x))$. В силу линейности кода $r(x) = s(x) - f(x)g(x) \in C$, но в коде C не может быть ненулевых многочленов степени меньше $deg(g(x))$, значит $r(x) = 0$ и $s(x) = f(x)g(x)$

Теорема 3. Циклический код длины n с порождающим многочленом g(x) существует тогда и только тогда, когда $g(x)$ делит $x^n - 1$.

Таким образом получаем, что циклический код C состоящий из элементов вида $g(x)f(x)$ является главным идеалом в кольце $F[x]/(x^n-1)$ и наоборот, любой идеал $F[x]/(x^n-1)$ порожденный элементом $g(x)$ является циклическим кодом, порожденным этим же многочленом. Получим теперь оценку размерности циклического кода.

Лемма 3. Если $g(x)$ — ненулевой нормированный многочлен наименьшей степени r кода C длины n, то размерность C равна $n-r$.

Доказательство. Произведения $g(x)$ на все многочлены степени, меньшей чем $n-r$, принадлежат C, причем среди них есть линейно независимые $1, x, x^2, ...x^{n-r-1}$. Значит размерность кода не менее $n-r$.

Покажем, что любой кодовый многочлен $s(x)$ представим в виде линейной комбинации $g(x)x^i$, $i < n-r$. Пусть это не так, тогда $t(x)$ многочлен наименьшей степени, такой что $s(x) = g(x)t(x)$ и при этом степень $t(x)$ больше $n-r-1$ равна z. Заметим, что по теореме 3: $g(x)|x^n-1 \Rightarrow g(x)|(x^{r+z} - x^{r+z-n+1})$. Тогда рассмотрим

$$t'(x) = t(x) - (x^{r+z} - x^{r+z-n+1})/g(x).$$

$t'(x)$ будет иметь меньшую степень при этом

$$g(x)t'(x) = g(x)(t(x) - (x^{r+z} - x^{r+z-n+1}/g(x)) = g(x)t(x) + (x^{n-1}-1)x^{r+z-1} = s(x)$$

Тогда $t(x)$ многочлен не наименьшей степени. Получили противоречие, значит лемма доказана.

Но многочлен порождающий код, как и элемент порождающий идеал, не единственен. Один из вариантов такого многочлена - ненулевой нормированный многочлен наименьшей степени. Однако могут быть и другие.

Теорема 4. Если (x) не вводит никаких новых нулей, т. е. если $(i) \neq 0$ для всех $i : g(i) \neq 0$, то многочлены $g(x)$ и $p(x)g(x)$ порождают один и тот же код.

Один из удобных вариантов задать код многочленом - идемпотентный многочлен, то есть многочлен $E(x)$, такой что $E(x) = E^2(x)$. Сформулируем следующие утверждение о $E(x) \in C$:

Теорема 5. Циклический код С, или идеал порожденный $g(x)$, содержит единственный идемпотент $E(x)$ такой, что $E(x)$ порождает С. Кроме того, $E(x) = p(x)g(x)$ для некоторого многочлена $p(x)$, причем $E(a) = 0$ тогда и только тогда, когда $g(a) = 0$.

Для проверки этого утверждения достаточно рассмотреть $p(x)$ такое, что

$$p(x)g(x) + q(x)h(x) = 1,$$

где $h(x)$ такой взаимопростой с $g(x)$ многочлен, что $x^n - 1 = g(x)h(x)$. Тогда если положим $E(x) = p(x)g(x)$, можно проверить, что $E(x)$ — идемпотент и $p(x)$ не вводит новых корней, а значит согласно лемме выше, $E(x)$ порождает тот же код что и $g(x)$.

Тогда если для некоторого $c(x)$ верно, что $c(x) = E(x)c(x)$, то $E(x)c(x) \in C \Rightarrow c(x) \in C$.

При этом, если $c(x) = E(x)c(x)$, то верно

$$(x)E(x) = r(x)E(x)E(x) = r(x)E(x) = c(x).$$

Таким образом получили критерий, если $E(x)$ - порождающий идемпотент кода C, то

$$E(x)c(x) \in C \iff c(x) \in C$$

.

2.2 Вычетно-квадратичные коды как частный случай циклических кодов

Обсудим один из способов изучения вычетного-квадратичного кода над полем $GF(l)$ длины q - его задание с помощью идемпотентного многочлена. Сперва введем определение.

Вычетно-квадратичными кодами длины p над полем $GF(L)$, где l - квадратичный вычет по модулю p, называются коды $L, \overline{L}, N, \overline{N}$, порожденные многочленами $q(x),\ \ q(x)(x-1),\ \ n(x),\ \ n(x)(x-1)$ соответственно, где если Q_p - множество всех квадратичных вычетов по модулю p, N_p - множество невычетов, а a - примитивный корень из единицы в некотором поле содержащем $GF(l)$, то $q(x),\ \ n(x)$ задаются формулами:

$$q(x) = \prod_{r \in Q_p} (x - a^r),$$

$$n(x) = \prod_{n \in N_p} (x - a^n).$$

Заметим, что многочлены описанные в определении являются нормированный порождающими многочленами наименьшей степени. Докажем это для $\overline{L}$, для остальных кодов все будет аналогично. Пусть есть код $s(x) \neq q(x)(x-1)$, порождающий $\overline{L}$. Тогда по теореме 4

$$q(x)(x-1) = s(x)p(x),$$

где $p(x)|q(x)(x-1)$ не имеет корней отличных от корней $s(x)$. Но при этом у $q(x)(x-1)$ нет кратных корней, значит у $p(x)$ нет корней. Но так как $q(x)(x-1)$ раскладывается в произведение многочленов первой степени, $p(x)$ тоже является произведением многочленов первой степени, а значит имеет корни. Получили противоречие.

Теперь по лемме 3 мы можем определить размерность наших кодов. Мы знаем, что для простого p $|Q_p| = |N_p| = \frac{p-1}{2}$, а значит знаем степень многочленов $q(x),\ \ q(x)(x-1),\ \ n(x),\ \ n(x)(x-1)$. Таким образом размерность вычетно-квадратичных кодов: $\frac{p+1}{2}$ для L, N и $\frac{p-1}{2}$ для $\overline{L}, \overline{N}$.

2.3 Идемпотенты вычетно-квадратичных кодов

Порождающие идемпотенты этих кодов описываются тремя следующими теоремами.

Теорема 6. Если $l = 2$ $p = 4k-1$, то a можно выбрать так, что порождающие идемпотенты вычетно-квадратичных кодов $L, \overline{L}, N, \overline{N}$ будут соответственно равны:

$$E_q(x) = \sum_{r \in Q_p} x^r$$

$$F_q(x) = \sum_{n \in N_p} x^n + 1$$

$$E_n(x) = \sum_{n \in N_p} x^n$$

$$F_n(x) = \sum_{r \in Q_p} x^r + 1$$

Теорема 7. Если $l = 2$ $p = 4k+1$, то a можно выбрать так, что порождающие идемпотенты вычетно-квадратичных кодов $L, \overline{L}, N, \overline{N}$ будут соответственно равны:

$$E_q(x) = \sum_{r \in Q_p} x^r + 1$$

$$F_q(x) = \sum_{n\in N_p} x^n$$

$$E_n(x) = \sum_{n\in N_p} x^n + 1$$

$$F_n(x) = \sum_{r\in Q_p} x^r$$

Теорема 8. Если $l > 2$ и $p = 4k \pm 1$ то коды $L, \overline{L}, N, \overline{N}$ порождаются соответственно идемпотентами:

$$E_q(x) = \frac{1}{2}(1+\frac{1}{p}) + \frac{1}{2}(\frac{1}{p} - \frac{1}{\theta})\sum_{r\in Q_p} x^r + \frac{1}{2}(\frac{1}{p} + \frac{1}{\theta})\sum_{n\in N_p} x^n$$

$$F_q(x) = \frac{1}{2}(1-\frac{1}{p}) - \frac{1}{2}(\frac{1}{p} + \frac{1}{\theta})\sum_{r\in Q_p} x^r - \frac{1}{2}(\frac{1}{p} - \frac{1}{\theta})\sum_{n\in N_p} x^n$$

$$E_n(x) = \frac{1}{2}(1+\frac{1}{p}) + \frac{1}{2}(\frac{1}{p} + \frac{1}{\theta})\sum_{r\in Q_p} x^r + \frac{1}{2}(\frac{1}{p} - \frac{1}{\theta})\sum_{n\in N_p} x^n$$

$$F_n(x) = \frac{1}{2}(1-\frac{1}{p}) - \frac{1}{2}(\frac{1}{p} - \frac{1}{\theta})\sum_{r\in Q_p} x^r - \frac{1}{2}(\frac{1}{p} + \frac{1}{\theta})\sum_{n\in N_p} x^n$$

где $\theta = \sum_{i=1}^{p-i}\chi(i)\alpha^i$, $\chi(i)$ - символ Лежандра i по модулю p.

2.4 Описание порождающих и проверочных матриц

Сперва вернемся к циклическим кодам. Пусть у нас есть код C порожденный многочленом $g(x)$. Тогда мы знаем что $\exists h(x) : x^n - 1 = g(x)h(x)$. Такой многочлен будем называть проверочным. Действительно, если $c(x) \in C$, то

$$c(x)h(x) = k(x)g(x)h(x) = k(x)(x^n - 1) = 0.$$

Тогда мы можем сформулировать следующие утверждения о порождающей и проверочной матрицах:

Теорема 9. Порождающая матрица циклического кода длины n с порождающим многочленом $g(x) = g_0 + g_1x + ... + g_rx^r$ имеет вид:

$$G = \begin{pmatrix} g_0 & g_1 & \dots & g_r & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_r & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \dots & 0 & g_0 & g_1 & \dots & g_r \end{pmatrix}$$

Теорема 10. Проверочная матрица циклического кода длины n с проверочным многочленом $h(x) = h_0 + h_1x + ... + h_kx^k$ имеет вид

$$H = \begin{pmatrix} 0 & 0 & \dots & 0 & h_k & h_{k-1} & \dots & h_0 \\ 0 & \dots & 0 & h_k & h_{k-1} & \dots & h_0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \\ h_k & h_{k-1} & \dots & h_0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

Обе эти матрицы состоят из n столбцов, $n-r$ и $n-k=r$ столбцов соответственно, и имеют ранг $n-r$ и порождает, являющийся идеалом порожденным $g(x)$. Теперь с помощью этих утверждении можем описать дуальный код.

Лемма 4. Дуальный код $C^{\perp}$ является циклическим кодом с порождающим многочленом

$$g(x) = x^{deg(h(x)}h(x^{-1}),$$

где $h(x)$ - проверочный многочлен кода C.

Доказательство. Порождающая матрица кода $C^{\perp}$ является проверочной матрицей кода C. Проверочная матрица кода C:

$$H = \begin{pmatrix} 0 & 0 & \dots & 0 & h_k & h_{k-1} & \dots & h_0 \\ 0 & \dots & 0 & h_k & h_{k-1} & \dots & h_0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \\ h_k & h_{k-1} & \dots & h_0 & 0 & 0 & \dots & 0 \end{pmatrix} \sim \begin{matrix} x^{deg(h(x))}h(x^{-1}) \\ x^{deg(h(x))+1}h(x^{-1}) \\ \vdots \\ x^n h(x^{-1}) \end{matrix}$$

Но по теореме 10 матрица порождающая код $C^{\perp}$

$$G = H \sim \begin{matrix} g(x) \\ xg(x) \\ \vdots \\ x^{-deg(g(x))}g(x) \end{matrix}$$

Таким образом $g(x) = x^{deg(h(x)}h(x^{-1})$.

2.5 Порождающие и проверочные матрицы вычетно-квадратичных кодов

Используя теоремы выше можно записать порождающие матрицы вычетно-квадратичных кодов используя многочлены $q(x)$, $q(x)(x-1)$, $n(x)$, $n(x)(x-1)$. А чтобы записать проверочную матрицу надо найти проверочные многочлены кодов. Для этого выпишем тождество:

$$x^p - 1 = \prod_{i=0}^{p-1}(x-\alpha^i) = q(x)n(x)(x-1)$$

Заметим, что многочлены бьются на пары порождающий-проверочный. Обозначим коэффициенты многочленов $q(x), n(x)$:

$$q(x) = q_0 + q_1 x + ... + q_{\frac{p-1}{2}} x^{\frac{p-1}{2}}$$

$$q(x) = n_0 + n_1 x + ... + n_{\frac{p-1}{2}} x^{\frac{p-1}{2}}$$

Таким образом коэффициенты других двух многочленов:

$$q(x)(x-1) = -q_0 + (q_0 - q_1)x + ... + (q_{\frac{p-3}{2}} - q_{\frac{p-1}{2}})x^{\frac{p-1}{2}} + q_{\frac{p-1}{2}} x^{\frac{p-1}{2}}$$

$$n(x)(x-1) = -n_0 + (n_0 - n_1)x + ... + (n_{\frac{p-3}{2}} - n_{\frac{p-1}{2}})x^{\frac{p-1}{2}} + n_{\frac{p-1}{2}} x^{\frac{p-1}{2}}$$

Тогда проверочные и порождающие матрицы можно записать следующим образом:

$$G_L = \begin{pmatrix} q_0 & q_1 & \dots & q_{\frac{p-1}{2}} & 0 & 0 & \dots & 0 \\ 0 & q_0 & q_1 & \dots & q_{\frac{p-1}{2}} & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \dots & 0 & q_0 & q_1 & \dots & q_{\frac{p-1}{2}} \end{pmatrix}$$

$$H_L = \begin{pmatrix} 0 & 0 & \dots & 0 & -n_0 & n_0-n_1 & \dots & n_{\frac{p-1}{2}} \\ 0 & \dots & 0 & -n_0 & n_0-n_1 & \dots & n_{\frac{p-1}{2}} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \\ -n_0 & n_0-n_1 & \dots & n_{\frac{p-1}{2}} & 0 & 0 & \dots & 0 \end{pmatrix}$$

$$G_{\overline{L}} = \begin{pmatrix} -q_0 & (q_0-q_1) & \dots & q_{\frac{p-1}{2}} & 0 & 0 & \dots & 0 \\ 0 & -q_0 & (q_0-q_1) & \dots & q_{\frac{p-1}{2}} & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \dots & 0 & -q_0 & (q_0-q_1) & \dots & q_{\frac{p-1}{2}} \end{pmatrix}$$

$$H_{\overline{L}} = \begin{pmatrix} 0 & 0 & \dots & 0 & n_0 & n_1 & \dots & n_{\frac{p-1}{2}} \\ 0 & \dots & 0 & n_0 & n_1 & \dots & n_{\frac{p-1}{2}} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \\ n_0 & n_1 & \dots & n_{\frac{p-1}{2}} & 0 & 0 & \dots & 0 \end{pmatrix}$$

Порождающие и проверочные матриц также можно задать с помощью идемпотент. Для этого сперва определим вид дуальных кодов.

Теорема 11. Для вычетно-квадратичных кодов $L, \overline{L}, N, \overline{N}$:
1)$L^{\perp} = \overline{L}$, $N^{\perp} = \overline{N}$, если $p = 4k-1$
2)$L^{\perp} = \overline{N}$, $N^{\perp} = \overline{L}$, если $p = 4k+1$

Теперь найдем порождающую матрицу вычетно-квадратичных кодов над полем с помощью идемпотент. Согласно теоремам 7, 8, 9:

$$E_q = F_q + \frac{1}{p}\sum_{i=0}^{p-1} x^i$$

$$E_n = F_n + \frac{1}{p}\sum_{i=0}^{p-1} x^i$$

Тогда если $F_q = \sum_{i=0}^{p-1} f_i x^i$ - порождающий идемпотент кода $\overline{L}$, то порождающая матрица G кода $\overline{L}$ является циркулянтной матрицей вида:

$$\widetilde{G_{\overline{L}}} = \begin{pmatrix} f_0 & f_1 & \dots & f_{p-1} \\ f_{p-1} & f_0 & \dots & f_{p-2} \\ \vdots & \vdots & \ddots & \vdots \\ f_1 & f_2 & \dots & f_0 \end{pmatrix}$$

А порождающая матрица кода L:

$$\widetilde{G_L} = \begin{pmatrix} f_0 & f_1 & \dots & f_n \\ f_n & f_0 & \dots & f_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ f_1 & f_2 & \dots & f_0 \\ 1 & 1 & \dots & 1 \end{pmatrix}$$

Аналогичные матрицы можно записать для N и $\overline{N}$. Осталось понять как будет выглядеть проверочная матрица. Зная, что порождающая матрица дуального кода является проверочной для исходного кода, мы можем задать проверочную матрицу используя теорему 8.

Для $p = 4k - 1$:
$$\widetilde{H_L} = \widetilde{G_{\overline{L}}},\ \ \widetilde{H_{\overline{L}}} = \widetilde{G_L},\ \ \widetilde{H_N} = \widetilde{G_{\overline{N}}},\ \ \widetilde{H_{\overline{N}}} = \widetilde{G_N}.$$
Для $p = 4k + 1$:
$$\widetilde{H_L} = \widetilde{G_{\overline{N}}},\ \ \widetilde{H_{\overline{L}}} = \widetilde{G_N},\ \ \widetilde{H_N} = \widetilde{G_{\overline{L}}},\ \ \widetilde{H_{\overline{N}}} = \widetilde{G_L}.$$

3 Вычетно-квадратичные коды над кольцами

3.1 Отличие кодов над кольцами от кодов над полями

Аналогично случаю с полем знаем, что если R - кольцо, то фактор-множество классов вычетов по модулю $x^n - 1$ $R[x]/(x^n - 1)$ является кольцом. Так как дальше речь будет идти о кольцах вычетов, то здесь и далее будем по умолчанию считать, что произвольное рассматриваемое кольцо R на самом деле конечное коммутативное кольцо с единицей. Тогда будем рассматривать циклический код длины n над кольцом R как подмножество фактор-кольца $R[x]/(x^n - 1)$.

Теорема 12. Подпространство кольца $R[x]/(x^n-1)$ является циклическим кодом тогда и только тогда, когда оно образует идеал.

Однако, в отличие от случая с полями, идеал кольца $R[x]/(x^n-1)$ может не быть главным, то есть циклический код над кольцом не обязательно порождается одним элементом. Тем не менее, лемма 2 теряет смысл, так как в кольце мы не всегда можем определить нормирование многочлена так, чтобы после нормировки многочлен оставался в идеале. Немного изменим лемму:

Лемма 5. Циклический код над кольцом содержит не более одного ненулевого многочлен наименьшей степени с заданным старшим коэффициентом.

Доказательство. Пусть существуют два многочлена $f(x)$ и $g(x)$ наименьшей степени r с одинаковыми старшими коэффициентами. Тогда многочлен $f(x)-g(x)$, принадлежащий коду, имеет степень меньше r, что приводит к противоречию.

В такой формулировке лемма остается верной. Тогда если мы умеем сравнивать элементы в кольце, можно выбрать единственный ненулевой многочлен наименьшей степени с наименьшим старшим коэффициентом, но будет ли он порождать код?

Оказывается теорема 3 не будет верна в случае колец, так как в ее доказательстве мы пользовались тем, что при делении многочлена $s(x) \in F[x]/(x^n - 1)$ на многочлен $g(x) \in F[x]/(x^n-1)$ для полученного остатка $r(x)$ верно: $deg(r(x)) < deg(g(x)$, однако для $s(x), g(x) \in F[x]/(x^n - 1)$ это утверждение неверно. Также не будет верна теорема 4 (в ее доказательстве возникают аналогичные проблемы). Тем не менее, мы можем точно сказать, что идеал циклического кода над кольцом является конечнопорожденным идеалом, а значит можно найти набор его линейно независимых порождающих.

3.2 Описание идемпотент вычетно-квадратичных кодов

Для начала сформулируем определение вычетно-квадратичного кода над кольцом $\mathbb{Z}_{2^n}$. При $n = 1$ определение дается аналогично определению над полем. Достаточно заметить, что 2 является квадратичным вычетом по модулю $p \equiv \pm 1 \pmod 8$ (здесь и далее будем рассматривать только такие простые числа).

Тогда, если обозначить

$$f_{Q_p} = \prod_{r \in Q_p} (x - a^r), \quad f_{N_p} = \prod_{r \in N_p} (x - a^r),$$

где a — первообразный корень n-й степени из единицы в кольце $\mathbb{Z}_p$, то вычетно-квадратичные коды над кольцом $\mathbb{Z}_{2^n}$ можно определить как коды, порождаемые многочленами

$$f_{Q_{2^m}}(x), \quad f_{N_{2^m}}(x), \quad (x-1)f_{Q_{2^m}}(x), \quad (x-1)f_{N_{2^m}}(x),$$

где $f_{Q_{2^m}}(x)$ - поднятие Гензеля многочлена $f_{Q_2}(x)$, а $f_{N_{2^m}}(x)$ - поднятие Гензеля многочлена $f_{N_2}(x)$.

Таким образом, мы получаем циклические коды являющиеся главными идеалами. Тогда к ним будут применимы многие факты из прошлого раздела, в частности верен следующий аналог теоремы 6.

Теорема 13. Пусть C - циклический код над $\mathbb{Z}_{2^n}$ нечетной длины n. Если C порождается многочленом $f(x)$, где $f(x)g(x) = x^n - 1$ для некоторого $g(x)$, такого, что $f(x)$ и $g(x)$ взаимно просты, то C имеет идемпотентный генератор в R_n. Более того, идемпотентный генератор циклического кода уникален.

Интересно также описать дуальные коды с помощью идемпотент, аналогично лемме 8.

Теорема 14. Если циклический код C над $\mathbb{Z}/p^m\mathbb{Z}$ имеет порождающую идемпотенту $e(x)$, то $C^\perp$ имеет порождающую идемпотенту $1 - e(x^{-1})$.

Также надо заметить, что если C_1 и C_2 являются Z_{2m}-циклическими кодами с порождающими идемпотентами $e_1(x)$ и $e_2(x)$ соответственно, то $C_1 \cap C_2$ порождается идемпотентой $e_1(x)e_2(x)$, а $C_1 \cup C_2$ порождается идемпотентой $e_1(x) + e_2(x) - e_1(x)e_2(x)$.

Далее за e_1 и e_2 обозначим соответственно многочлены

$$\sum_{i \in Q} x^i, \quad \sum_{i \in N} x^i.$$

Заметим что согласно теоремам 7 и 8 они будут являться порождающими идемпотентами для кодов $\overline{L}, \overline{N}$, если $p \equiv -1 \pmod 8$ и порождающими идемпотентами для кодов L, N, если $p \equiv 1 \pmod 8$. Оказывается идемпотенты вычетно-квадратичных кодов над $\mathbb{Z}/2^m\mathbb{Z}$ связываются с e_1 и e_2 следующей теоремой.

Теорема 15. Идемпотент $\alpha + \beta e_1 + \gamma e_2$ вычетно-квадратичного кода над $\mathbb{Z}/2^m\mathbb{Z}$ удовлетворяет тождеству: $2\alpha - (\beta + \gamma) \equiv 1 (\bmod \quad 2^m)$.

3.3 Описание порождающих матриц вычетно-квадратичных кодов над кольцами ($\mathbb{Z}_{2^n}$)

Заметим, что теоремы 10 и 11 остаются верны и в случае колец, если код является главным идеалом. В случае вычетно-квадратичных кодов это так, а значит порождающие матрицы вида описанного в теоремах 10 и 11 в случае колец строятся аналогично.

Теперь найдем порождающую матрицу заданную с помощью идемпотентов вычетно-квадратичных кодов над ($\mathbb{Z}_{2^n}$). Пусть $F = \sum_{i=0}^{l} f_i x^i$, где $n = \frac{p-1}{2}$ порождающий идемпотент кода $\overline{L}$. Тогда порождающая матрица G кода $\overline{L}$ является циркулянтной матрицей вида:

$$\overline{G} = \begin{pmatrix} f_0 & f_1 & \dots & f_n \\ f_n & f_0 & \dots & f_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ f_1 & f_2 & \dots & f_0 \end{pmatrix}$$

А порождающая матрица кода L:

$$G = \begin{pmatrix} f_0 & f_1 & \dots & f_n \\ f_n & f_0 & \dots & f_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ f_1 & f_2 & \dots & f_0 \\ 1 & 1 & \dots & 1 \end{pmatrix}$$

Аналогичные матрицы можно записать для N и $\overline{N}$. Тогда согласно теореме 6 можем выразить матрицу G следующим образом, если $p = 8k + 1$:

$$G = \alpha\widetilde{G_L} + \beta\widetilde{G_N} + \gamma E,$$

если $p = 8k - 1$

$$G = \alpha\widetilde{G_{\overline{L}}} + \beta\widetilde{G_{\overline{N}}} + \gamma E,$$

где α, β, γ таковы, что $2\alpha - (\beta + \gamma) \equiv 1 (\mathrm{mod} \quad 2^m)$.

Аналогичные тождества можно получить для порождающих матриц остальных вычетно-квадратичных кодов.

Список литературы

[1] Дж. Мак-Вильямс, Н. Дж. А. Слоэн "Теория кодов, исправляющих ошибки", *Москва "СВЯЗЬ"*, (1979)

[2] Xiongqing Tan "A family of Quadratic Resident Codes over Z_{2^m}", *arXiv*, (2011)

[3] Mei Hui Chiu, Stephen S.-T., Yung Yu "$\mathbb{Z}_8$-Cyclic Codes and Quadratic Residue Codes", *idealibrary*, (2000)

[4] Ф. И. Соловьева, "Введение в теорию кодирования", *Редакционно-издательский центр НГУ*, (2006)