НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Модуль 3. Циклические коды

Важнейший класс циклических кодов. Коды БЧХ. Алгоритм Горенстейна-Петерсона-Цирлера.

Иванов Ф. И.

к.ф.-м.н., доцент

Национальный исследовательский университет «Высшая школа экономики»

12 июня 2020 г.

Определение кода БЧХ

Определение

Кодом Боуза—Чоудхури—Хоквингема (БЧХ) над $GF(q)$ *называется такой циклический код, порождающий многочлен* $g(x)$ *которого имеет своими корнями последовательность идущих подряд степеней некоторого произвольного элемента* $\alpha \in GF(q^m)$*:*

$$\alpha^b, \alpha^{b+1}, ..., \alpha^{b+\delta-2},$$

где b *любое целое число и* $\delta \geq 2$*. Последовательность может содержать также только один элемент* α^b*.*

Длина кода БЧХ

Теорема

Либо длина n кода БЧХ равна порядку элемента α^b, если $\delta - 2 = 0$, либо порядку элемента α в противном случае, т.е. когда $\delta > 2$.

Доказательство

При $\delta - 2 = 0$ утверждение тривиально. Пусть $\delta > 2$. Докажем, что Н.О.К порядков корней равно в точности порядку элемента α. Действительно, пусть α порождает циклическую группу G порядка n. Именно к ней принадлежат все последовательные корни. Предположим противное. Пусть найдется такая подгруппа $G' \subset G$, которой принадлежат корни. Тогда все они являются степенями одного элемента α^h, т.е. имеют вид $\alpha^h j$, где h есть делитель n. Рассмотрим два соседних элемента α^{b+i} и α^{b+i+1}. По предположению $b + i = hj_0, b + i + 1 = hj_1$. Это значит, что $b + i + 1 - (b + i) = hj_1 - hj_0 = h(j_1 - j_0) = 1$, что возможно только при $h = 1$ для любых соседних целых чисел $b + i = hj_0, b + i + 1 = hj_1$. Доказанное означает, что порядки элементов α^{b+i}, $i = 0, 1, ..., \delta 2$ не являются делителями порядка никакой истинной подгруппы $G' \subset G$. Это значит, что они являются делителями только порядка n группы G, т.е. делителями порядка элемента α.

Граница БЧХ

Теорема

Минимальное расстояние кода БЧХ с корнями $\alpha^b, \alpha^{b+1}, ..., \alpha^{b+\delta-2}$ *порождающего многочлена* $g(x)$ *равно по меньшей мере* δ.

Доказательство

Проверочная матрица кода БЧХ:

$$H = \begin{bmatrix} 1 & \alpha^b & (\alpha^b)^2 & \dots & (\alpha^b)^{n-1} \\ 1 & \alpha^{b+1} & (\alpha^{b+1})^2 & \dots & (\alpha^{b+1})^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha^{b+\delta-2} & (\alpha^{b+\delta-2})^2 & \dots & (\alpha^{b+\delta-2})^{n-1} \end{bmatrix}$$

Доказательство - продолжение

Возьмем произвольный $\delta - 1$ столбец из **H**:

$$D = \begin{vmatrix} (\alpha^b)^{j_1} & (\alpha^b)^{j_2} & \dots & (\alpha^b)^{j_{\delta-1}} \\ (\alpha^{b+1})^{j_1} & (\alpha^{b+1})^{j_2} & \dots & (\alpha^{b+1})^{j_{\delta-1}} \\ \dots & \dots & \dots & \dots \\ (\alpha^{b+\delta-2})^{j_1} & (\alpha^{b+\delta-2})^{j_2} & \dots & (\alpha^{b+\delta-2})^{j_{\delta-1}} \end{vmatrix}$$

или:

$$D = \alpha^{b(j_1+j_2+\ldots+j_{d-1})} \begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha^{j_1} & \alpha^{j_2} & \dots & \alpha^{j_{\delta-1}} \\ \dots & \dots & \dots & \dots \\ (\alpha^{j_1})^{\delta-2} & (\alpha^{j_2})^{\delta-2} & \dots & (\alpha^{j_{\delta-1}})^{\delta-2} \end{vmatrix}.$$

Пусть $\alpha^{b(j_1+j_2+\ldots+j_{\delta-1})} = C$, $\alpha^{j_i} = a_i$.

Доказательство - окончание

$$D = C \begin{vmatrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_{\delta-1} \\ \dots & \dots & \dots & \dots \\ a_1^{\delta-2} & a_2^{\delta-2} & \dots & a_{\delta-1}^{\delta-2} \end{vmatrix}.$$

В этом равенстве справа легко узнать определитель Вандермонда. Известно, что он отличен от нуля тогда и только тогда, когда все a_i различны и принадлежат области целостности: $D \neq 0$.
Тем самым доказано, что любые $\delta - 1$ столбцов проверочной матрицы **H** кода БЧХ линейно независимы, а значит $d \geq \delta$

Алгоритм построения $g(x)$

- Выбирается длина n кода БЧХ как $q^m - 1$ или некоторый делитель этого числа
- Определяем, сколько t ошибок требуется исправить кодом и рассчитывам $\delta = 2t + 1$.
- Выбираем подходящее b и строим последовательность $\alpha^b, \alpha^{b+1}, ..., \alpha^{b+\delta-2}$
- Для каждого элемента последовательности находим минимальную функцию $m_{\alpha^{b+i}}(x)$ над $GF(q)$
- Строим порождающий многочлен $g(x)$ как НОК минимальных функций

$$g(x) = [m_{\alpha^b}(x), m_{\alpha^{b+1}}(x), \ldots, m_{\alpha^{b+\delta-2}}(x)]$$

Пример построения

Рассмотрим циклический код с корнями $g(x)$: $\alpha, \alpha^3, \alpha^5 \in GF(2^4)$. На самом деле получим последовательность:

$$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{12},$$

которая автоматически получается из первоначальной добавлением к ней сопряженных элементов. Получилось, что подряд идущих степеней элемента α ровно шесть. Это значит, что $\delta - 1 = 6$, и код заведомо исправляет любую комбинацию из трех и менее независимых ошибок. На самом деле здесь $d = \delta$.

Параметры кодов БЧХ

- Поле элементов: $GF(q)$ - выбирается заранее
- Поле корней $g(x)$: $GF(q^m)$ - выбирается заранее
- Длина n: делитель $q^m - 1$ - выбирается заранее
- Число исправляемых ошибок: t - выбирается заранее
- Число информационных символов:

$$k \geq n - 2tm(1 - 1/q)$$

Лучшая оценка:

$$k \geq n - tm$$

достигается для двоичных кодов БЧХ

Декодирование кодов БЧХ - вычисление синдрома

Пусть по каналу связи отправлен кодовый вектор

$$\mathbf{u} = (u_0, u_1, ..., u_{n-1})$$

кода БЧХ, и в канале произошла ошибка, изображаемая вектором

$$\mathbf{e} = (e_0, e_1, ..., e_{n-1})$$

На приёмном конце принят вектор

$$\mathbf{v} = \mathbf{u} + \mathbf{e}$$

И декодер вычисляет

$$\mathbf{S} = \mathbf{v}\mathbf{H}^T = \mathbf{e}\mathbf{H}^T$$

Вычисление синдрома

Так как i-ая строка матрицы $\mathbf{H}$ имеет вид:

$$\left(1\ \alpha^{b+i}\ (\alpha^{b+i})^2\ (\alpha^{b+i})^3 \ldots (\alpha^{b+i})^{n-1}\right)$$

то если $\mathbf{S} = (S_0, S_1, \ldots, S_{d-1})$, то:

$$S_i = \left(\left(1\ \alpha^{b+i}\ (\alpha^{b+i})^2\ (\alpha^{b+i})^3 \ldots (\alpha^{b+i})^{n-1}\right), (v_0, v_1, \ldots, v_{n-1})\right)$$

или

$$S_i = v_0 + v_1\alpha^{b+i} + v_2(\alpha^{b+i})^2 + \ldots + v_{n-1}(\alpha^{b+i})^{n-1}$$

$$S_i = v\left(\alpha^{b+i}\right) = e\left(\alpha^{b+i}\right)$$

Декодирование кодов БЧХ: $q = 2$, $t = 2$

Пусть $t = 2$, $d = 5$, $b = 1$. Последовательность корней: $\alpha, \alpha^2, \alpha^3, \alpha^4$. В векторе ошибки **e** отличны от нуля 2 компоненты с неизвестными номерами j_1, j_2, тогда:

$$S_1 = \alpha^{j_1} + \alpha^{j_2}$$

$$S_2 = (\alpha^2)^{j_1} + (\alpha^2)^{j_2} = S_1^2$$

$$S_3 = (\alpha^3)^{j_1} + (\alpha^3)^{j_2}$$

Положим для удобства $\alpha^{j_1} = X_1$, $\alpha^{j_2} = X_2$ и составим уравнение, корнями которого являются искомые величины:

$$(X - X_1)(X - X_2) = X^2 + (X_1 + X_2)X + X_1 X_2 = 0.$$

Решение уравнения

$$(X - X_1)(X - X_2) = X^2 + (X_1 + X_2)X + X_1X_2 = 0.$$

Выразим коэффициенты через компоненты синдрома:

$$X_1 + X_2 = S_1,$$

$$S_3 = X_1^3 + X_2^3 = (X_1 + X_2)(X_1^2 + X_1X_2 + X_2^2) = S_1(X_1X_2 + S_1^2),$$

откуда

$$X_1X_2 = S_1^2 + S_3/S_1$$

Окончательно имеем:

$$X^2 + S_1X + S_1^2 + S_3/S_1 = 0$$

решив которое (перебором) найдем X_1 и X_2.

Задача

Поле $GF(2^4)$ построено по модулю многочлена $p(x) = x^4 + x^3 + 1$. Корнями порождающего многочлена кода БЧХ являются α и α^3. Длина кода n $= 15$.
В принятом векторе

$$\mathbf{v} = (000101011001000)$$

найти искаженные символы в терминах α^i, исправить ошибку и убедиться, что получившийся после исправления вектор принадлежит коду.

Решение

В многочленной форме принятый вектор имеет вид:

$$v(x) = x^3 + x^5 + x^7 + x^8 + x^{11}.$$

Проводя операции в поле $GF(2^4)$, построенном по модулю многочлена $p(x) = x^4 + x^3 + 1$, легко вычислить:

$$S_1 = v(\alpha) = \alpha^3 + \alpha^5 + \alpha^7 + \alpha^8 + \alpha^{11} = \alpha^7,$$

$$S_3 = v(\alpha^3) = \alpha^3 + \alpha^9 + \alpha^{15} + \alpha^6 + \alpha^9 = \alpha^{13}.$$

После подстановки найденных элементов $S_1 = \alpha^7$, $S_3 =^{13}$ синдрома в квадратное уравнение оно станет таким:

$$x^2 + \alpha^7 x + \alpha^{12} = 0.$$

Корни: $X_1 = \alpha^4$, $X_2 = \alpha^8$ то есть ошибки на 5 и 9 позициях.

Проверка

$$\mathbf{e} = (000010001000000)$$

$$\mathbf{u} = \mathbf{v} + \mathbf{e} = (000111010001000)$$

$$u(x) = x^3 + x^4 + x^5 + x^7 + x^{11}$$

$$u(\alpha) = \alpha^3 + \alpha^4 + \alpha^5 + \alpha^7 + \alpha^{11} = 0$$

$$u(\alpha^3) = \alpha^9 + \alpha^{12} + \alpha^{15} + \alpha^6 + \alpha^3 = 0$$

$$\mathbf{S} = \mathbf{0}$$

то есть вектор (000111010001000) является кодовым словом кода БЧХ.

Общий случай декодирования двоичных кодов БЧХ

Пусть $b = 1$, нужно найти t компонент

$$e_{j_1}, e_{j_2}, ..., e_{j_t}.$$

вектора ошибок $\mathbf{e}$.
Пусть $\alpha^{j_i} = X_i$, $d = 2t + 1$. Тогда компоненты синдрома находятся как:

$$S_1 = X_1 + X_2 + ... + X_t,$$

$$S_2 = X_1^2 + X_2^2 + ... + X_t^2,$$

$$...$$

$$S_{2t} = X_1^{2t} + X_2^{2t} + ... + X_t^{2t}.$$

Цель: зная S_i решить систему нелинейных уравнений, то есть найти X_i — локаторы ошибок

Многочлен локаторов ошибок

Составим многочлен (локаторов ошибок)

$$\sigma(z) = (1 - X_1 z)(1 - X_2 z)...(1 - X_t z) = \sigma_0 + \sigma_1 z + \sigma_2 z^2 + ... + \sigma_t z^t,$$

где

$$\sigma_0 = 1,$$

$$\sigma_1 = (X_1 + X_2 + ... + X_t),$$

$$\sigma_2 = X_1 X_2 + X_1 X_3 + ... + X_{t-1} X_t,$$

$$..................$$

$$\sigma_t = (-1)^t X_1 X_2 ... X_t.$$

Задача: зная S_i, найти σ_i.

Тождества Ньютона

$$\sigma'(z) = -\sum_i X_i \prod_{j\neq i}(1 - X_j z)$$

тогда, если не ограничивать степень:

$$-\frac{z\sigma'(z)}{\sigma(z)} = \frac{X_1 z}{1 - X_1 z} + \frac{X_2 z}{1 - X_2 z} + \ldots + \frac{X_t z}{1 - X_t z},$$

воспользуемся суммой бесконечно убывающей геометрической прогрессии:

$$-\frac{z\sigma'(z)}{\sigma(z)} = X_1 z + (X_1 z)^2 + \ldots + X_2 z + (X_2 z)^2 + \ldots + X_t z + (X_t z)^2 + \ldots$$

$$-\frac{z\sigma'(z)}{\sigma(z)} = z(X_1 + X_2 + \ldots) + z^2(X_1^2 + X_2^2 + \ldots) + \ldots + z^i(X_1^i + X_2^i + \ldots) + \ldots$$

$$-\frac{z\sigma'(z)}{\sigma(z)} = S(z)$$

Тождества Ньютона

$$z\sigma'(z) = S(z)\sigma(z)$$

или

$$(1+\sigma_1 z+\sigma_2 z^2+\ldots)(S_1 z+S_2 z^2+S_3 z^3+\ldots) = z(\sigma_1+2\sigma_2 z+3\sigma_3 z^2+\ldots)$$

Приравнивая коэффициенты при одинаковых степенях z, получим:

$$S_1+\sigma_1=0$$

$$S_2+S_1\sigma_1+2\sigma_2=0,$$
$$S_3+S_2\sigma_1+S_1\sigma_2+3\sigma_3=0,$$
$$S_4+S_3\sigma_1+S_2\sigma_2+S_1\sigma_3+4\sigma_4=0,$$
$$S_5+S_4\sigma_1+S_3\sigma_2+S_2\sigma_3+S_1\sigma_4+5\sigma_5=0,$$

....

Это и есть тождества Ньютона. Берем их через одно и приводим коэффициенты по модулю 2.

Ключевая система

$$\begin{bmatrix} 1 & 0 & 0 & 0 & \dots & 0 \\ S_2 & S_1 & 1 & 0 & \dots & 0 \\ S_4 & S_3 & S_2 & S_1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots \\ S_{2t-4} & S_{2t-5} & S_{2t-6} & S_{2t-7} & \dots & S_{t-3} \\ S_{2t-2} & S_{2t-3} & S_{2t-4} & S_{2t-5} & \dots & S_{t-1} \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \sigma_3 \\ \vdots \\ \sigma_{t-1} \\ \sigma_t \end{bmatrix} = \begin{bmatrix} S_1 \\ S_3 \\ S_5 \\ \vdots \\ S_{2t-3} \\ S_{2t-1} \end{bmatrix}.$$

В дальнейшем матрицу коэффициентов системы будем обозначать символом $\mathbf{M}_t$.
Решением системы является набор коэффициентов $\sigma_1, \sigma_2, \ldots, \sigma_t$ многочлена локаторов ошибок. Далее локаторы ищутся подбором.

Основная теорема о разрешимости системы

Теорема

Матрица $\mathbf{M}_t$ *невырождена, и система имеет единственное решение тогда и только тогда, когда произошло* t *или* $t-1$ *ошибок. Матрица* $\mathbf{M}_t$ *вырождена тогда и только тогда, когда произошло менее, чем* $t-1$ *ошибок.*

Схема декодера

1. По принятому из канала слову **v** составляется вектор синдромов
2. По составленному вектору синдромов составляется матрица $\mathbf{M}_t$
3. Вычисляется $|\mathbf{M}_t|$. Если $|\mathbf{M}_t| \neq 0$, то решается система и находятся $\sigma_1, \sigma_2, \ldots, \sigma_t$
4. По $\sigma_1, \sigma_2, \ldots, \sigma_t$ составляется многочлен локаторов ошибок. Последовательной подстановкой в него всех ненулевых злементов поля $GF(2^m)$ получаются корни многочлена, как величины, обратные локаторам ошибок.
5. Компоненты вектора v, отвечающие локаторам, заменяются на противоположные.
6. Если $|\mathbf{M}_t| = 0$, то это означает, что произошло менее, чем $t-1$ ошибок.
7. В матрице $\mathbf{M}_t$ удаляются два последних столбца и две последних строки.
8. Процесс повторяется i раз до тех пор, пока матрица $\mathbf{M}t - 2i$ не станет невырожденной. Решается система $t-2i$ линейных уравнений.

Пример 1

Пусть передавался вектор $\mathbf{u} = (110100011000100)$ кода БЧХ длины $n = 15$ (поле по модулю $1 + x + x^4$) из рассмотренного ранее примера. Последовательность корней порождающего многочлена:

$$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \ d = 7, t = 3.$$

Произошло 3 ошибки и принят вектор:

$$\mathbf{v}_1 = (011101101000100).$$

Вычисляем компоненты синдрома:

$$S_1 = \alpha + \alpha^2 + \alpha^3 + \alpha^5 + \alpha^6 + \alpha^8 + \alpha^{12} = \alpha^{11}, S_3 = \alpha^3 + \alpha^6 + \alpha^9 + 1 + \alpha^3 + \alpha^9 +$$

$$S_5 = \alpha^5 + \alpha^{10} + 1 + \alpha^{10} + 1 + \alpha^{10} + 1 = 0,$$

$$S_2 = S_1^2 = \alpha^7, S_4 = S_2^2 = \alpha^{14}, S_6 = 1.$$

Пример 1 - продолжение

$$\mathbf{M}_3 = \begin{pmatrix} 1 & 0 & 0 \\ \alpha^7 & \alpha^{11} & 1 \\ \alpha^{14} & 1 & \alpha^7 \end{pmatrix},$$

$|\mathbf{M}_3| = 1 + \alpha^{18} = \alpha^{14} \neq 0$
Система линейных уравнений:

$$\begin{cases} \sigma_1 = S_1 = \alpha^{11}, \\ \alpha^7\sigma_1 + \alpha^{11}\sigma_2 + \sigma_3 = S_3 = 1, \\ \alpha^{14}\sigma_1 + \sigma_2 + \alpha^7\sigma_3 = S_5 = 0. \end{cases}$$

имеет решение: $\sigma_1 = \alpha^{11}$,$\sigma_2 = \alpha^8$,$\sigma_3 = \alpha^9$. Тогда многочлен локаторов ошибок имеет вид:

$$\sigma(z) = 1 + \alpha^{11}z + \alpha^8z^2 + \alpha^9z^3$$

Его корни как величины, обратные локаторам ошибок:
$z_1 = \alpha^8$,$z_2 = \alpha^{13}$,$z_3 = \alpha^0$, а значит сами локаторы: $X_1 = \alpha^7$, $X_2 = \alpha^2$, $X_3 = \alpha^0$, а значит исказились 1,3,8 позиции.

Пример 2

Произошла одна ошибка и принят вектор $\mathbf{v} = (110101101000100)$. Находим компоненты синдрома:

$$\begin{aligned}
&S_1 = 1 + \alpha + \alpha^3 + \alpha^5 + \alpha^6 + \alpha^8 + \alpha^{12} = \alpha^7,\\
&S_3 = 1 + \alpha^3 + \alpha^9 + 1 + \alpha^3 + \alpha^9\alpha^6 = \alpha^6,\\
&S_5 = 1 + \alpha^5 + 1 + \alpha^{10} + 1 + \alpha^{10} + 1 = 1\alpha^5\\
&S_2 = S_1^2 = \alpha^{14},\ S_4 = S_{14}^2 = \alpha^{13},\ S_6 = \alpha^{12}.
\end{aligned}$$

$$\mathbf{M}_3 = \begin{pmatrix} 1 & 0 & 0 \\ \alpha^{14} & \alpha^7 & 1 \\ \alpha^3 & \alpha^6 & \alpha^{14} \end{pmatrix},$$

$|\mathbf{M}_3| = 0$, тогда вычеркнем в $\mathbf{M}_3$ две последние строки и два столбца и получим матрицу $\mathbf{M}_1 = [1]$. Откуда $\sigma_1 = S_1 = \alpha^7, \sigma_2 = 0, \sigma_3 = 0$. Многочлен локаторов ошибок:

$$\sigma(z) = 1 + \alpha^7 z$$

Его корень $z_1 = \alpha^8$, Локатор: α^7, исказился 8 символ слова.

Общий случай декодирования недвоичных БЧХ кодов

Нужно искать не только позиции, но и значения ошибок из поля $GF(q)$!
Вектор ошибки содержит t ненулевых компонент:

$$e_{j_1}, e_{j_2}, ..., e_{j_t} \in GF(q).$$

Вектор ошибки:

$$e(x) = e_{i_1} x^{i_1} + e_{i_2} x^{i_2} + ... + e_{i_t} x^{i_t}.$$

Компоненты синдрома имеют вид: $S_i = e(\alpha^i)$.
Полагаем $e_{j_i} = Y_i, ^{j_i} = X_i$.

Основная система

$$S_1 = Y_1X_1 + Y_2X_2 + ... + Y_tX_t,$$

$$S_2 = Y_1X_1^2 + Y_2X_2^2 + ... + Y_tX_t^2,$$

$$...$$

$$S_{2t} = Y_1X_1^{2t} + Y_2X_2^{2t} + ... + Y_tX_t^{2t}.$$

$Y_i \in GF(q)$, $X_i \in GF(q^m)$.

Система линейна относительно Y_i. Если произошло t ошибок, то все X_i, $i = 1, 2, ..., t$, различны и отличны от нуля. В этих условиях определитель первых t уравнений системы отличен от нуля (???). Следовательно, первые t уравнений системы линейно независимы, и они разрешимы относительно неизвестных Y_i

Нахождение локаторов ошибок

$$\sigma(z) = \sigma_0 + \sigma_1 z + \sigma_2 z^2 + ... + \sigma_t z^t = \prod_{i=1}^{t}(1 - X_i z)$$

Подставим $z = X_i^{-1}$:

$$\sigma(X_i^{-1}) = 1 + \sigma_1 X_i^{-1} + \sigma_2 X_i^{-2} + ... + \sigma_t X_i^{-t} = 0,$$

Затем помножим тождество на $Y_i X_i^{j+t}$:

$$Y_i(X_i^{j+t} + \sigma_1 X_i^{j+t-1} + \sigma_2{}_i^{Xj+t-2} + ... + \sigma_t X_i^j) = 0.$$

При фиксированном j просуммируем все тождества по $i = 1, 2, ..., t$:

$$\sum_{i=1}^{t} Y_i(X_i^{j+t} + \sigma_1 X_i^{j+t-1} + \sigma_2{}_i^{Xj+t-2} + ... + \sigma_t X_i^j) = 0.$$

Раскроем скобки и меняем порядок суммирования.

Нахождение локаторов ошибок

$$\sum_{i=1}^{t} Y_i X_i^{j+t} + \sigma_1 \sum_{i=1}^{t} Y_i X_i^{j+t-1} + \sigma_2 \sum_{i=1}^{t} Y_i X_i^{j+t-2} + \ldots + \sigma_t \sum_{i=1}^{t} Y_i X_i^{j} = 0$$

но

$$\sum_{i=1}^{t} Y_i X_i^{j+t-l} = S_{j+t-l}, l = 0,1,\ldots,t$$

Поэтому для фиксированного j имеем:

$$S_{j+t} + \sigma_1 S_{j+t-1} + \ldots + \sigma_t S_j = 0,\ j = 1, 2, \ldots, t.$$

Таких уравнений будет t штук, и вместе они составляют систему

$$\begin{cases} \sigma_1 S_t + \sigma_2 S_{t-1} + \ldots + \sigma_t S_1 = -S_{t+1}, \\ \sigma_1 S_{t+1} + \sigma_2 S_t + \ldots + \sigma_t S_2 = -S_{t+2}, \\ \ldots \\ \sigma_1 S_{2t-1} + \sigma_2 S_{2t-2} + \ldots + \sigma_t S_t = -S_{2t} \end{cases}$$

Матричное представление

$$\begin{bmatrix} S_t & S_{t-1} & \dots & S_2 & S_1 \\ S_{t+1} & S_t & \dots & S_3 & S_2 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ S_{2t-1} & S_{2t-2} & \dots & S_{t+1} & S_t \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_t \end{bmatrix} = \begin{bmatrix} -S_{t+1} \\ -S_{t+2} \\ \vdots \\ -S_{2t} \end{bmatrix}$$

Обозначим матрицу системы символом $\mathbf{M}_t$.

Теорема

Система уравнений имеет единственное решение тогда и только тогда, когда произошло t ошибок.

Нахождение значений ошибок

- Найти значения $\sigma_0 = 1$, $\sigma_1, \ldots, \sigma_t$, решив систему уравнений
- Найти корни многочлена $\sigma(z) = \sigma_0 + \sigma_1 z + \sigma_2 z^2 + \ldots + \sigma_t z^t$
- Найти локаторы $X_1, \ldots, X_t$

Вернемся к системе уравнений на Y_i. Ее определитель:

$$\begin{vmatrix} X_1 & X_2 & \ldots & X_t \\ X_1^2 & X_2^2 & \ldots & X_t^2 \\ \vdots & \vdots & \vdots & \vdots \\ X_1^t & X_2^t & \ldots & X_t^t \end{vmatrix} = X_1 X_2 \ldots X_t \begin{vmatrix} 1 & 1 & \ldots & 1 \\ X_1 & X_2 & \ldots & X_t \\ \vdots & \vdots & \vdots & \vdots \\ X_1^{t-1} & X_2^{t-1} & \ldots & X_t^{t-1} \end{vmatrix}$$

Справа находится определитель Вандермонда. При наличии t ошибок локаторы X_i различны, и определитель отличен от нуля. Система имеет единственное решение.

Алгоритм

1. Подставляя в принятый вектор **v** корни порождающего многочлена, вычисляют элементы S_i синдрома. Если все они равны нулю, то считается, что ошибок нет, и процедура окончена.
2. В противном случае из элементов синдрома составляется система уравнений $\mathbf{M}_t$. Если ее матрица $\mathbf{M}_t$ в формул не вырождена, вычисляются коэффициенты $\sigma_1, \sigma_2, ...\sigma_t$ многочлена локаторов ошибок.
3. Отыскиваются t корней многочлена локаторов ошибок последовательной подстановкой в него элементов поля $GF(q^m)$. Величины, обратные корням, есть локаторы ошибок.
4. Составляется система уравнений на Y_i, которая имеет единственное решение, так как ее матрица не вырождена. Решением системы являются значения ошибок.
5. В соответствии с каждой ненулевой парой (X_i, Y_i) из i-го символа вектора **v** вычитается величина Y_i. Восстановлен передававшийся вектор **u**. Процедура закончена.
6. Если матрица $\mathbf{M}_t$ вырождена, система не разрешима. Это означает, что произошло не более, чем $t-1$ ошибок. Из матрицы $\mathbf{M}_t$ в следует удалить последние строку и столбец, положить $\sigma_t = 0$, а из системы — последнее уравнение. Вся процедура выполняется снова после замены t на $t-1$.