1 Preliminaries

Нехай m — степінь простого числа. Тоді над полем $\mathbb{F}_{m^2}$ крива, яка визначається рівнянням $H_m = x^{m+1} + y^m z + y z^m$, називається ермітовою кривою. Ця крива має $m^3 + 1$ $\mathbb{F}_{m^2}$-раціональних точок, серед них є одна нескінченно віддалена, $Q = (0 : 1 : 0)$. Рід цієї кривої можна обчислити як $g = \frac{m(m-1)}{2}$.

Нерівність Серра дає оцінку максимальної кількості точок N на кривій роду g над полем $\mathbb{F}_q$:

$$N \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor$$

Підставивши параметри ермітової кривої у цю нерівність, отримаємо:

$$N \leq m^2 + 1 + \frac{m(m-1)}{2}\lfloor 2\sqrt{m^2} \rfloor = m^2 + 1 + m(m-1)m =$$

$$= m^2 + 1 + m^3 - m^2 = m^3 + 1$$

Звідси зрозуміло, що ермітова крива є максимальною.

Для ермітової кривої базис простору $L(aQ)$ має особливий вигляд та може бути досить тривіально обчислений:

$$L(aQ) = span\left\{ \frac{x^i y^j}{z^{i+j}} \middle| im + j(m+1) \leq a, i \leq m \right\}$$

2 Алгоритм

Нехай $\mathcal{P}$ — множина усіх $\mathbb{F}_{m^2}$-раціональних точок H_m, окрім Q, тоді алгеброгеометричний код $C_{H_m,a} = (H_m, \mathcal{P}, aQ)_\Omega$ називатимемо ермітовим кодом з параметрами (m, a). Параметри цього лінійного коду: $[m^3, m^3 - a + \frac{m(m-1)}{2} - 1, a - m(m-1) + 2]_{\mathbb{F}_{m^2}}$ за умови, що $a > m(m-1) - 2$.

2.1 Кодування

2.1.1 Попередня підготовка

Обчислимо базис $L(aQ)$, за теоремою Рімана-Роха кількість його елементів дорівнюватиме: $\ell_{aQ} = a + 1 - \frac{m(m-1)}{2}$:

$$basis(L(aQ)) = \left\{ \frac{x^i y^j}{z^{i+j}} \middle| im + j(m+1) \leq a, i \leq m \right\}$$

Обчислимо множину раціональних точок $\mathcal{P}$.

Обчислимо перевірочну матрицю H:

$$H = \begin{pmatrix} f_1(P_1) & \cdots & f_1(P_{m^3}) \\ \vdots & \ddots & \vdots \\ f_{\ell_{aQ}}(P_1) & \cdots & f_{\ell_{aQ}}(P_{m^3}) \end{pmatrix}, P_i \in \mathcal{P}, f_j \in basis(L(aQ))$$

Обчислимо породжуючу матрицю G:

$$G = \begin{pmatrix} G_1 \\ \vdots \\ G_k \end{pmatrix}, G_i \in basis(kernel(H^T))$$

Зауваження: $(H_m, \mathcal{P}, aQ)^{\perp}_{\Omega} = (H_m, \mathcal{P}, (m^3 + m^2 - m - a - 2)Q)_L$, з цих міркувань можна обчислювати матриці H і G як матриці G' та H' відповідного дуального коду.

2.1.2 Кодування вхідного слова

Для вхідного слова $v, v \in \mathbb{F}_{m^2}^k$ обчислимо кодове слово $c, c \in \mathbb{F}_{m^2}^n$:

$$c = v \cdot G$$

2.2 Декодування алгоритмом Скоробогатова-Вледуца

2.2.1 Попередня підготовка

Кількість помилок, які може виправити алгоритм: $t = \left\lfloor \frac{a - \frac{3m(m-1)}{2} + 1}{2} \right\rfloor$

Обчислимо базис $\{g_j\}$ простору $L((t+g)Q)$ та обчислимо базис $\{h_k\}$ простору $L((a-t-g)Q)$.

Обчислимо матрицю синдромів S:

$$S = \begin{pmatrix} g_1 \\ \vdots \\ g_{\ell((t+g)Q)} \end{pmatrix} \cdot \begin{pmatrix} h_1 & \cdots & h_{\ell((a-t-g)Q)} \end{pmatrix}$$

2.2.2 Декодування вхідного слова

Для вхідного слова $v, v = c + e, v \in \mathbb{F}_{m^2}^n$ обчислимо матрицю синдромів слова:

$$S_v = \begin{pmatrix} g_1 f_1 \cdot v & g_2 f_1 \cdot v & \dots \\ g_1 f_2 \cdot v & g_2 f_2 \cdot v & \dots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

Тут $\phi \cdot v = (\phi(P_1), \dots, \phi(P_{m^3})) \cdot v$

Якщо отримана матриця складається із нулів, тоді вектор e є нульовим, а слово v — кодовим.

Знайдемо ядро S_v, якщо базис відповідного простору складається не з одного вектора, алгоритм не може декодувати слово v. Нехай $(s_1, \dots, s_{\ell((t+g)Q)})$ — вектор відповідного базису. Обчислимо скалярний добуток:

$$\theta = (s_1, \dots, s_{\ell((t+g)Q)}) \cdot (g_1, \dots, g_{\ell((t+g)Q)})$$

Знайдемо координати i_e, у яких відбулися помилки: перебором $P_{i_e} \in \mathcal{P}$ знаходимо такі точки, для яких $\theta(P_{i_e}) = 0$.

Вирішуємо систему рівнянь:

$$\begin{pmatrix} f_1(P_{i_{e_1}}) & \dots & f_1(P_{i_{e_t}}) \\ \vdots & \ddots & \vdots \\ f_{\ell(aQ)}(P_{i_{e_1}}) & \dots & f_{\ell(aQ)}(P_{i_{e_t}}) \end{pmatrix} \cdot \begin{pmatrix} e_1 \\ \vdots \\ e_t \end{pmatrix} = \begin{pmatrix} f_1 \cdot v \\ \vdots \\ f_{\ell(aQ)} \cdot v \end{pmatrix}, f_i \in L(aQ)$$

Отримавши значення e_{i_e}, відновимо вхідний вектор: $c = v - e$.

Декодоване слово w отримаємо із співвідношення $w \cdot G = c$.

3 Приклад

Для прикладу візьмемо ермітовий код з параметрами $(2, 6)$. Відповідна крива H_2 задається рівнянням $x^3 + y^2z + yz^2$ над полем $\mathbb{F}_4$. Окрім нескінченно віддаленої точки $Q = (0 : 1 : 0)$ у неї 8 раціональних точок:

$\mathcal{P} = \{(0 : 0 : 1), (0 : 1 : 1), (1 : w : 1), (1 : w + 1 : 1), (w : w : 1),$
$(w : w + 1 : 1), (w + 1 : w : 1), (w + 1 : w + 1 : 1)\}$

Ця крива має рід 1 (більше того, це еліптична крива), отже параметри лінійного коду $[8, 2, 6]_{\mathbb{F}_4}$, кількість помилок, які може виправити алгоритм Скоробогатова-Вледуца $t = 2$.

$$L(6Q) = span\left\{1, y/z, y^2/z^2, x/z, xy/z^2, x^2/z^2\right\}$$

Породжуюча матриця може бути обчислена як перевірочна відповідного дуального коду:

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & w & w & w+1 & w+1 \end{pmatrix}$$

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & w+1 & 0 & w \\ 0 & 1 & 0 & 0 & 0 & w+1 & 0 & w \\ 0 & 0 & 1 & 0 & 0 & w & 0 & w+1 \\ 0 & 0 & 0 & 1 & 0 & w & 0 & w+1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Нехай вхідне повідомлення $(0, 1)$, тоді кодове слово:

$$c = (0, 0, 1, 1, w, w, w + 1, w + 1)$$

Нехай при передачі відбулись помилки у другій та восьмій позиціях і приймальна сторона отримала слово:

$$v = (0, 1, 1, 1, w, w, w + 1, 0)$$

Матриця синдромів для коду має вигляд:

$$S = \begin{pmatrix} 1 & y/z & x/z \\ y/z & y^2/z^2 & xy/z^2 \\ x/z & xy/z^2 & x^2/z^2 \end{pmatrix}$$

Для отриманого вектора v вона набуде вигляду:

$$S_v = \begin{pmatrix} w & w+1 & w \\ w+1 & 0 & 1 \\ w & 1 & 1 \end{pmatrix}$$

Локатор помилок:

$$\theta = \frac{((w+1) * x + y + z)}{z}$$

4 Аналіз складності

Через те, що параметр m накладає певні обмеження на параметр a ермітового коду, складність алгоритмту можна виразити лише через параметр m.

При побудові коду, а також при декодуванні необхідно обчислювати базиси трьох просторів Рімана-Роха: $L(aQ), L((t+g)Q), L((a-t-g)Q)$. Для того, аби в теоремі Рімана-Роха досягалась рівність, необхідно накласти такі обмеження на параметри (для спрощення обчислень у виразі параметру t буде прибрано округлення вниз, це може вплинути на точність оцінки при малих m):

$$\begin{cases} a > 2g-2 \\ t+g > 2g-2 \\ a-t-g > 2g-2 \end{cases}, \begin{cases} t > g-2 \\ a > 3g+t-2 \end{cases}, \begin{cases} \frac{a-3g+1}{2} > g-2 \\ a > 3g + \frac{a-3g+1}{2} - 2 \end{cases},$$

$$\begin{cases} a-3g+1 > 2g-4 \\ 2a > 6g+a-3g+1-4 \end{cases}, \begin{cases} a > 5g-5 \\ a > 3g-3 \end{cases}, a > 5\frac{m(m-1)}{2} - 5$$

З іншого боку має виконуватись нерівність $0 < k < n$, тобто $0 < m^3 - a -$

$\frac{m(m-1)}{2} - 1 < m^3$, яка накладає обмеження:

$$\begin{cases} a > \frac{m(m-1)}{2} - 1 \\ a < m^3 + \frac{m(m-1)}{2} - 1 \end{cases}$$

Підсумовуючи наведені нерівності, можна сказати, що a має лежати у такому проміжку:

$$5\frac{m(m-1)}{2} - 5 < a < m^3 + \frac{m(m-1)}{2} - 1,$$

тобто асимптотично a має зростати швидше, ніж m^2, але повільніше, ніж m^3, тому далі можна вважати, що $a = O(m^3)$ і $a = \Omega(m^2)$.

Більшість етапів алгоритму використовує операції із матрицями над скінченним полем, тому відповідні оцінки складності будуть прив'язані до складності операцій в полі. При використанні представлення елементів $\mathbb{F}_{m^2}$ у вигляді лишків незвідного полінома операції множення та ділення потребуватимуть $O(\ln^2 m^2) = O(\ln^2 m)$ операцій, піднесення елемента поля до додатнього степеню N потребуватиме $O(\ln N \ln^2 m)$ операцій. Додавання двох елементів поля потребуватиме $O(\ln m)$ операцій. Використання представлення елементів поля у вигляді степенів породжуючого елемента зведе операції множення та ділення до додавання та віднімання показників степенів за модулем $m^2 - 1$, складність такої операції дорівнюватиме $O(\ln(m))$. Проте така форма представлення незручна для додавання та віднімання елементів, тому необхідно попередньо створити таблицю відповідностей двох форм запису, це потребуватиме $O(m^2 \ln^2 m)$ операцій та $O(m^2)$ пам'яті.

Для ермітової кривої процедуру знаходження базису $L(aQ)$ можна зводиться до знаходження пар (i, j), для яких виконується співвідношення $im + j(m+1) \leq n$ у циклах, пробігаючи $0 \leq j \leq \left\lfloor \frac{a}{m+1} \right\rfloor$ та $0 \leq i \leq m$. Тобто усього $O(a)$ операцій вартістю порядку $O(\ln a)$ кожна, загалом $O(a \ln a)$.

Для побудови перевірочної матриці H необхідно знайти базис $L(aQ)$, це займе $O(a \ln a) = O(m^3 \ln m)$ операцій. Перебірна реалізація знаходження раціональних точок (підстановка усіх $x, y \in \mathbb{F}_{m^2}$ у рівняння кривої, найдорожча

арифметична операція — піднесення елемента поля до m-го степеня) займе $O(m^2 m^2 m \ln^2 m) = O(m^5 \ln^2 m)$. Отже, у матриці H $\ell_{aQ} = a + 1 - \frac{m(m-1)}{2}$ рядків та m^3 стовпчиків, тому загальну кількість її елементів можна оцінити як $O(m^3 m^3) = O(m^6)$. Для обчислення кожного з її елементів найдорожчою арифметичною операцією буде піднесення до степеню (в найгіршому випадку $\frac{a}{m+1} = O(m^2)$), складність операції $O(\ln m^2 \ln^2 m) = O(\ln^3 m)$. Тому загальна складність обчислення всіх елементів H буде $O(m^6 \ln^3 m)$, як бачимо це і буде найдорожчою операцією у побудові H. Із властивості самодуальності ермітового коду вважатимемо, що складність побудови матриці G не перевищуватиме складності побудови H.

Кодування полягає у множенні вектора довжини k на матрицю $k \times n$: для цього необхідно обчислити kn результатів множення елементів поля: складність $kn \ln^2 m = O(m^3 m^3 \ln^2 m) = O(m^6 \ln^2 m)$.

При декодуванні найдорожчою операцією буде обчислення матриці S_v, кількість її елементів можна оцінити як $O(m^6)$, обчислення кожного її елементу полягає в обчисленні скалярного добутку двох векторів довжиною m^3. Отже, загальна складність знаходження S_v дорівнюватиме $O(m^9 \ln^2 m)$.

Вартість розв'язку систем лінійних рівнянь, яка виникає при декодуванні має аналогічну складність (матриця розміром $m^3 \times m^3$): метод Гаусса виглядатиме так: i-тий рядок ділимо на елемент $a_{i,i}$, для кожного іншого k-го рядка віднімаємо даний, поділений на $a_{k,i}$: це буде три вкладені цикли по m^3 кроків у кожному із вартістю внутрішньої операції $O(\ln^2 m)$. Загальна складність методу: $O(m^9 \ln^2 m)$.

Наведена складність алгоритму Скоробогатова-Вледуца збігається із оцінкою, яка дається у літературі: $O(n^3)$ операцій в скінченному полі. Якщо врахувати, що для ермітового коду $n = m^3$, а вартість множення $O(\ln^2 m)$, ми отримуємо оцінку $O(m^9 \ln^2 m)$.