Міністерство освіти і науки України
Національний Університет
«Києво-Могилянська Академія»
Кафедра математики факультету інформатики

# Надлишкове кодування на алгебраїчних кривих

**Науковий керівник:**
проф. Боднарчук Ю. В.
**Виконав:**
Трояновський М. М.

Київ 2011

# Зміст

# Вступ

Надлишкове кодування відіграє значну роль у боротьбі з помилками, які виникають при передачі даних через зашумлені телекомунікаційне середовище. Загалом для надійної передачі інформації через ненадійні канали застосовують дві стратегії: виявлення та виправлення помилок. У першому випадку до блоку даних додають контрольну інформацію, за допомогою якої одержувач має змогу зрозуміти, що під час зв'язку відбулося пошкодження відповідного блоку, тому необхідно зробити запит на повторну передачу. Найпростішим прикладом такої контрольної інформації є біт парності, який додається до блоку бінарних даних таким чином, аби загальна кількість одиниць у блоці була парною. Це дає можливість одержувачу виявити помилку в одному біті переданого блоку, проте якщо помилок було більше, вони можуть скасувати одна одну; втім подібний метод можна досить просто узагальнити для виявлення будь-якої непарної кількості помилок.

Проте існують застосування, у яких одного виявлення факту помилки при передачі інформації замало, оскільки повторна передача блоку даних може бути занадто витратною: так при зв'язку із об'єктами у космосі, що віддалені від Землі на велику відстань існує значна затримка, яка буде лише збільшуватися при ретрансмісії; при односторонній передачі даних (наприклад, у телемовленні) ретрансмісія взагалі технічно неможлива. У таких випадках необхідно намагатися виправляти помилки наперед, додаючи до блоку даних надлишкову інформацію, яка дозволятиме одержувачу відновити блок навіть за наявності помилок передачі. Простим прикладом даного підходу може бути таке бінарне кодування: кожен біт передається тричі підряд, одержувач аналізує триплети та декодує їх у той біт, якого кількісно більше у триплеті. Зрозуміло, що такий спосіб дозволяє виправити одну помилку в окремому триплеті, але ціна такої можливості досить велика: дані за такого підходу будуть передаватися втричі повільніше.

Природнім є бажання знайти способи надлишкового кодування, які з одного боку дозволятимуть виправляти значну кількість помилок, а з іншого боку не призводить до сповільнення передачі. Розвиненою в цьому аспекті є теорія лінійних кодів, де були встановлені нерівності, які дають можливість порів-

няти різні кодування між собою, а також обирати для практичного використання коду із граничними характеристиками. Зокрема, важливою є границя Сінглтона, яка стверджує, що для лінійного $(n, k, d)$-коду справжується нерівність: $d \leq n - k + 1$. Код який досягає відповідної рівності, називають кодом із максимально досяжною мінімальною відстанню, нетривіальним прикладом такого випадку слугують коди Ріда-Соломона.

Однак у теорії лінійних кодів також є проблемні місця. Так, у загальному випадку алгоритм декодування, а також визначення мінімальної дистанції лінійного коду є NP-складними. Тому для практичного використання необхідно використовувати коди зі специфічними властивостями, які дозволятимуть їх ефективно декодувати. У цій роботі описано алгебро-геометричні коди, для яких з одного боку відомий швидкий алгоритм декодування, а з іншого боку була доведена можливість перевершення цими кодами границі Варшамова-Гілберта.

# 1 Постановка задачі

Мета даної курсової роботи – описати наявні способи надлишкового кодування з використанням еліптичних кривих, характеристики отриманих кодів, базові алгоритми кодування та декодування, а також їхні переваги у порівнянні з іншими кодами, попередньо визначивши основні теоретичні поняття.

# 2 Основні поняття

## 2.1 Лінійні коди

Лінійний код — векторний підпростір $C$ розмірності $k$ векторного простору $\mathbb{F}_q^n$ розмірності $n$, де $\mathbb{F}_q$ — скінченне поле із $q$ елементів. $d$ — мінімальна відстань за Хемінгом між кодовими словами. Максимальна кількість помилок, які може виправити код: $r = \left\lfloor \frac{d-1}{2} \right\rfloor$. Підсумовуючи ці основні характеристики, часто кажуть про лінійний код як про $(n, k, d)_q$-код.

Нерівність Сінглтона: для $(n, k, d)$-коду виконується: $d \leq n - k + 1$, коди для яких виконується рівність $d = n-k+1$ називають кодами із максимально досяжною мінімальною відстанню (maximum distance separable), вони є у певному сенсі найкращими. З цієї нерівності можна побачити, що, за фіксованого $n$, $k$ та $d$ не можуть бути одночасно великими.

Нерівність Варшамова-Гілберта: якщо виконується співвідношення

$$\sum_{i=1}^{d-1} C_{n-1}^{i}(q-1)^{i} < q^{n-k}$$

то існує лінійний $(n,k,d)_q$-код.

## 2.2 Алгебраїчні криві

$\mathbb{A}^n$ — $n$-вимірний афінний простір над полем $k$, точками якого будуть надори $P=(x_1,\ldots,x_n), x_i \in k$. $\mathbb{P}^n$ — $n$-вимірний проективний простір над $k$, точками якого є набори $Q=(y_0:y_1:\ldots:y_n), y_i \in k$, де не всі $y_i$ дорівнюють нулю, при чому набори $(y_0:y_1:\ldots:y_n)$ та $(\lambda y_0:\lambda y_1:\ldots:\lambda y_n)$ при $\lambda \in k, \lambda \neq 0$ визначають одну й ту саму точку. При цьому простір $\mathbb{A}^n$ передбачає природнє вкладення у $\mathbb{P}^n$, яке задається формулою $P=(x_1,\ldots,x_n) \mapsto (1:y_1:\ldots:y_n)$.

Гладка проективна алгебраїчна крива $C$ у $N$-вимірному проективному просторі $P^N$ над полем $\mathbb{F}$ — це одновимірний многовид без особливостей, тобто сукупність розв'язків системи однорідних алгебраїчних рівнянь від $(N+1)$ змінної із коефіцієнтами із $\mathbb{F}$ таких, що матриця похідних у кожній точці задає рівняння прямої; розв'язки загалом потрібно розглядати з координатами у замиканні $\bar{\mathbb{F}}$ основного поля. Інтуїтивно гладкість означає відсутність точок повернення та самоперетину, одновимірність — єдиність дотичного напрямку у кожній точці.

З кривою $C$ пов'язують поле $\mathbb{F}(C)$ раціональних функцій на ній, тобто відношень однорідних многочленів рівного степеню з точністю до рівнянь з $C$. Функція є регулярною в точці, якщо вона набуває у ній скінченного значення.

## 2.3 Дивізори

Дивізор алгебраїчної кривої $C$ — це формальна сума її точок, взятих із певною кратністю:

$$D = \sum_{P \in C} n_P P, n_P \in \mathbb{Z},$$

де тільки скінченна кількість цілих чисел $n_P$ відмінна від нуля.

Множина усіх дивізорів, позначена як $Div$, формує Абелеву групу із за-

коном додавання:

$$\sum_{P\in C} n_P P + \sum_{P\in C} m_P P = \sum_{P\in C} (n_P + m_P) P$$

Степінь $D$ — це цілочисельна сума його коефіцієнтів:

$$deg(D) = \sum_{P\in C} n_P$$

$\forall D_1, D_2 \in Div : deg(D_1) + deg(D_2) = deg(D_1 + D_2)$, тому відображення $deg : Div \to \mathbb{Z}$ є гомоморфізмом. Множина $Div^0$ дивізорів ступеню 0 є підгрупою $Div$, а також ядром гомоморфізму $deg$.

Порядок $D$ у точці $P$ — це цілий коефіцієнт при $P$: $ord_P(D) = n_P$.

Носій дивізора — $supp(D) = \{P | n_P \neq 0\}$.

Якщо у дивізора всі $n_P$ — невід'ємні, такий дивізор називається ефективним. Поняття ефективності дозволяє задати відношення порядку на множині дивізорів.

Довільну ненульову раціональну функцію $f \in \mathbb{K}(X)$ можна пов'язати із дивізором $(f) = \sum ord_P(f) P$. Таке визначення є коректним, бо у такої функції на $X$ є скінченна кількість нулів та полюсів, тому $ord_P(f) \neq 0$ для скінченного числа точок $P$.

Нехай $X$ — гладка проективна крива роду $g$ та канонічного класу $K$. Теорема Рімана-Роха стверджує, що для будь-якого дивізора $D \in Div(X)$ виконується співвідношення

$$\ell(D) - \ell(K - D) = degD - g + 1$$

тут $\ell(D)$ — розмірність простору раціональних функцій на кривій, полюси яких у кожній точці не гірші, ніж відповідні коефіцієнти $D$. Зазначене співвідношення грає ключову роль для визначення конструктивних характеристик алгеброгеометричного коду.

# 3 Алгебро-геометричні коди

## 3.1 Означення

Алгебро-геометричні коди — це клас лінійних кодів, які вперше були описані Валерієм Денисовичем Гоппою, тому їх часто називають кодами Гоппи, проте це іноді може вносити неясність, оскільки такі коди не єдині, які називають на його честь. Його ідеєю було сконструювати код, за допомогою обчислення функцій із простору Рімана-Роха на раціональних точках алгебраїчної кривої.

$L(D)$ — це $\mathbb{F}$-векторний простір для будь-якого раціонального дивізора кривої, визначеної над $\mathbb{F}$. Згадавши, що лінійний код — це просто векторний підпростір $\mathbb{F}^n$, виникає природне бажання побудувати код. Проте $L(D)$ є векторним простором функцій, тому він не зобов'язаний бути кодом; однак лінійна властивість просторів Рімана-Роха дозволяє сконструювати лінійний код. Окрім того, теорема Рімана-Роха дозволяє визначити характеристики коду.

## 3.2 Приклад алгебро-геометричного коду

Нехай ми маємо криву $C$ над скінченним полем $\mathbb{F}$, скінченну множину точок $\mathcal{P} = \{P_1, \ldots, P_n\}$ і дивізор $D$, відокремлений (disjoint) від $P_i$. Код Гоппи $GC = GC(\mathcal{P}, D, C)$ визначають як

$$GC = \{(\phi(P_1), \ldots, \phi(P_n)) | \phi \in L(D)\}$$

Зазначений запис є функціональним кодом ($L$-конструкція). Код лишків (residue code, $\Omega$-конструкція) визначають як

$$GC' = \{c \in \mathbb{F}^n | c \cdot (\phi(P_1), \ldots, \phi(P_n)) = 0, \forall \phi \in L(D)\}$$

Конструктивні характеристики коду можна оцінити такими співвідношеннями:

$$n = |\mathcal{P}|,\ k \geq n - a + g - 1,\ d \geq a - 2g + 2$$

Для прикладу нехай $C$ — еліптична крива, задана за допомогою $f = X^3 + Y^2Z + YZ^2$ над $\mathbb{F}_4$ ($w^2 + w + 1 = 0$). Це несингулярна крива роду 1 із дев'ятьма

раціональними точками, одна з яких, $Q = (0 : 1 : 0)$, — нескінченно віддалена точка. Утворимо множину $\mathcal{P}$ усіма точками, окрім $Q$, тоді

$$P_1 = (0 : 0 : 1);\ P_2 = (0 : 1 : 1);\ P_3 = (1 : w : 1);\ P_4 = (1 : w^2 : 1);$$

$$P_5 = (w : w : 1);\ P_6 = (w : w^2 : 1);\ P_7 = (w^2 : w : 1);\ P_8 = (w^2 : w^2 : 1)$$

Нехай дивізор $D = 5Q$, тоді $L(D)$ — п'ятивимірний простір із базисом $L(5Q) = \langle 1, x, y, x^2xy \rangle$.

У цьому випадку конструктивна мінімальна відстань коду дорівнює 5, тому код буде здатен виправити дві помилки. Перевірочна матриця виглядатиме таким чином:

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ x(P_1) & x(P_2) & \dots & x(P_8) \\ y(P_1) & y(P_2) & \dots & y(P_8) \\ x^2(P_1) & x^2(P_2) & \dots & x^2(P_8) \\ xy(P_1) & xy(P_2) & \dots & xy(P_8) \end{pmatrix}$$

Після обчислень:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & w & w & w^2 & w^2 \\ 0 & 1 & w & w^2 & w & w^2 & w & w^2 \\ 0 & 0 & 1 & 1 & w^2 & w^2 & w & w \\ 0 & 0 & w & w^2 & w^2 & 1 & 1 & w \end{pmatrix}$$

Програмний код, який реалізує описаний вище приклад у математичному середовищі Magma:

```
> A<x,y> := AffineSpace(FiniteField(4),2);
> f:=x^3+y^2+y;
> C:=Curve(A,f);
> P1:=Places(C,1);
> Div := DivisorGroup(C);
> P1;
[
    Place at (0 : 1 : 0),
```

```
    Place at (0 : 0 : 1),
    Place at (0 : 1 : 1),
    Place at ($.1 : $.1 : 1),
    Place at ($.1 : $.1^2 : 1),
    Place at ($.1^2 : $.1 : 1),
    Place at ($.1^2 : $.1^2 : 1),
    Place at (1 : $.1 : 1),
    Place at (1 : $.1^2 : 1)
]
> D:=5*P1[1];
> P2:=[P1[2],P1[3],P1[4],P1[5],P1[6],P1[7],P1[8],P1[9]];
> D0:=Div!D;
> D0;
Divisor on Curve over GF(2^2) defined by
$.1^3 + $.2^2*$.3 + $.2*$.3^2
> RiemannRochSpace(D0);
KModule of dimension 5 over GF(2^2)
Mapping from: KModule of dimension 5 over GF(2^2) to Function Field of C
over GF(2^2) defined by
$.1^3 + $.2^2*$.3 + $.2*$.3^2
> Basis(D0);
[
    1,
    x,
    x^2,
    y,
    x*y
]
> GC:=AlgebraicGeometricCode(P2,D0);
> GC;
[8, 5, 3] Linear Code over GF(2^2)
Generator matrix:
[    1     0     0     0     0 $.1^2 $.1^2     1]
```

```
[    0     1     0     0     0 $.1^2   $.1     0]
[    0     0     1     0     0   $.1     1   $.1]
[    0     0     0     1     0   $.1     0 $.1^2]
[    0     0     0     0     1     1     1     1]
```

### 3.3 Кількість раціональних точок на алгебраїчній кривій

Нерівність Серре дає оцінку кількості точок $N$ на кривій роду $g$, визначеної над $\mathbb{F}_q$:

$$|N - (q+1)| \leq g\lfloor 2\sqrt{g} \rfloor$$

Оскільки ця величина визначає довжину відповідного алгебро-геометричного коду, доцільно застосовувати криві із найбільшою кількістю раціональних точок.

### 3.4 Алгоритми декодування

Основний алгоритм декодування коду $C = (X, \mathcal{P}, D)_\Omega$ за допомогою допоміжного дивізора виглядає таким чином:

1. Обчислити базис $f_i$ простору $L(D)$, базис $g_j$ простору $L(D')$ і базис $h_k$ простору $L(D - D')$.

2. Для даного вектора $v \in \mathbb{F}_q^n$ обчислити синдроми $s(v, g_j, h_k)$ та $s(v, f_i)$.

3. Знайти розв'язок $y$ системи лінійних рівнянь

$$\sum_{i=1}^{\ell} s_{ij} x_i = 0$$

4. Знайти (за допомогою перебору точок $P_i$ ті $i$, для яких $g_y(P_i) = 0$.

5. Знайти розв'язок системи рівнянь

$$\sum_{i \in I_y} f_j(P_i) z_i = s(v, f_j)$$

# 4 Алгеброгеометричні коди на ермітових кривих

Нехай $m$ — степінь простого числа. Тоді над полем $\mathbb{F}_{m^2}$ крива, яка визначається рівнянням $H_m = x^{m+1} + y^m z + yz^m$ , 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:

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

## 4.1 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 $a > m(m-1) - 2$.

### 4.1.1 Попередня підготовка кодування

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.

### 4.1.2 Кодування вхідного слова

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

$$c = v \cdot G$$

### 4.1.3 Попередня підготовка декодування алгоритмом Скоробогатова-Вледуца

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 $S$:

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

### 4.1.4 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 $w \cdot G = c$.

## 4.2 Приклад

Для прикладу візьмемо ермітовий код з параметрами $(2, 6)$. Відповідна крива $H_2$ задається рівнянням $x^3 + y^2 z + y z^2$ 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:

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

### 4.3 Аналіз складності

Через те, що параметр $m$ накладає певні обмеження на параметр $a$ ермітового коду, складність алгоримтму 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 загаль-

на 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 $O(m^9 \ln^2 m)$.

## Висновки

Попри специфічні властивості алгеброгеометричні коди поки массово не застовують в індустрії, де знайшли використання коди Ріда-Соломона, які поступово витісняються LDPC-кодами. Проте теорія, яка є підгрунтям для побудови алгеброгеометричних кодів досі активно розвивається, тому є можливість виявлення нових, більш швидких алгоритмів кодування та декодування, а також покращення характеристик коду, зокрема можливість декодувати поза конструктивною відстанню. Окрім того, дослідження у даній галузі можуть дозволити зробити додаткові узагальнення у теорії кодування.

# Література


[1] С. Г. Влэдуц Д. Ю. Ногин, М. А. Цфасман. Алгеброгеометрические коды. Основные понятия / М. А. Цфасман С. Г. Влэдуц, Д. Ю. Ногин. — Издательство Московского центра непрерывного образования, 2003.

[2] Гоппа, В. Д. Алгебраико-геометрические коды / В. Д. Гоппа // Изв. АН СССР. Сер. матем. — 1982. — Vol. 46, № 4. — P. 762–781.

[3] Гоппа, В. Д. Коды, ассоциированные с дивизорами / В. Д. Гоппа // Пробл. передачи информ. — 1977. — Vol. 13, № 1. — P. 33–39.

[4] Hao, Chen. Algebraic geometric codes with applications / Chen Hao // Frontiers of Mathematics in China. — 2007. — Vol. 2, № 1. — P. 1–11.

[5] Цфасман, М. А. Коды Гоппы, лежащие выше границы Варшамова–Гилберта / М. А. Цфасман // Пробл. передачи информ. — 1982. — Vol. 18, № 3. — P. 3–6.

[6] А. М. Барг Г. Л. Кацман, М. А. Цфасман. Алгеброгеометрические коды по кривым малых родов / М. А. Цфасман А. М. Барг, Г. Л. Кацман // Пробл. передачи информ. — 1987. — Vol. 23, № 1. — P. 42–46.

[7] Cheng, Qi. Hard problems of algebraic geometry codes.

[8] Shokrollahi, M. Amin. Decoding algebraic-geometric codes beyond the error-correction bound / M. Amin Shokrollahi, Hal Wasserman // STOC '98: Proceedings of the thirtieth annual ACM symposium on Theory of computing. — New York, NY, USA: ACM, 1998. — P. 241–248.

[9] Dai, Zhuo Jia. — Algebraic Geometric Coding Theory. — Master's thesis, School of Mathematics and Statistics, University of Sydney, Australia, 2006.

[10] Goppa, V. D. Geometry and Codes / V. D. Goppa; Ed. by M. Hazewinkel. — New York: Springer-Verlag, 2002.

[11] Goldschmidt, D. M. Algebraic functions and projective curves / D. M. Goldschmidt. — Springer, 2002.

[12] А. Г. Ростовцев, Е. Б. Маковенко. Теоретическая криптография / Е. Б. Маковенко А. Г. Ростовцев. — АНО НПО «Професионал», 2004.

[13] Coblitz, N. Algebraic Aspects of Cryptography / N. Coblitz. — Springer, 2002.

[14] Pellikaan, Ruud. On a decoding algorithm for codes on maximal curves / Ruud Pellikaan // IEEE Transactions on Information Theory. — 1989. — Vol. 35, № 6. — P. 1228–1232.

[15] Porter, S. C. Decoding geometric goppa codes using an extra place / S. C. Porter, Ba-Zhong Shen, Ruud Pellikaan // IEEE Transactions on Information Theory. — 1992. — Vol. 38, № 6. — P. 1663–1676.

[16] Høholdt, Tom. On the decoding of algebraic-geometric codes / Tom Høholdt, Ruud Pellikaan // IEEE Transactions on Information Theory. — 1995. — Vol. 41, № 6. — P. 1589–1614.

[17] Fast decoding of algebraic-geometric codes up to the designed minimum distance / Shojiro Sakata, Jørn Justesen, Y. Madelung et al. // IEEE Transactions on Information Theory. — 1995. — Vol. 41, № 6. — P. 1672–1677.

[18] Duursma, Iwan M. Majority coset decoding / Iwan M. Duursma // IEEE Transactions on Information Theory. — 1993. — Vol. 39, № 3. — P. 1067–.

[19] Feng, Gui Liang. Decoding algebraic-geometric codes up to the designed minimum distance / Gui Liang Feng, Thammavarapu R. N. Rao // IEEE Transactions on Information Theory. — 1993. — Vol. 39, № 1. — P. 37–45.

[20] Wocjan, P. — The Brill–Noether Algorithm: Construction of Geometric Goppa Codes and Absolute Factorization. — Master's thesis, University of Kalsruhe, 1999. http://www.cs.caltech.edu/ wocjan/.

[21] Hess, Florian. Computing riemann-roch spaces in algebraic function fields and related topics / Florian Hess // J. Symb. Comput. — 2002. — Vol. 33, № 4. — P. 425–445.