Національний Університет
«Києво-Могилянська Академія»
Кафедра математики

# Курсова робота на тему:
# «Надлишкове кодування на еліптичних кривих»

**Виконав:**
Михайло Михайлович Трояновський,
студент ІСПР–1

**Науковий керівник:**
Юрій Вікторович Боднарчук

Київ–2010

# Зміст

# 1 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 порівняти 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.

## 2 Постановка задачі

Мета даної курсової роботи – описати наявні способи надлишкового кодування з використанням еліптичних кривих, а також їхні переваги у порівнянні з іншими кодами.

## 3 Основні поняття

### 3.1 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.

### 3.2 Алгебраїчні криві

Гладенька 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 гладенькість 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.

### 3.3 Функціональні поля

### 3.4 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 $\mathbb{D}$, формує Абелеву групу із законом додавання:

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

Ступінь $D$ — це цілочисельна сума його коефіцієнтів:

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

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

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

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

## 4 Алгебро-геометричні коди

### 4.1 Коди Гоппи

Алгебро-геометричні коди — це клас лінійних кодів, які вперше були описані Валерієм Денисовичем Гоппою, тому їх часто називають кодами Гоппи. 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.

### 4.2 Приклад кодів Гоппи

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. Код лишків визначають як

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

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:

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

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 Curve
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]
```

### 4.3 Кількість раціональних точок на алгебраїчній кривій

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

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

Можна перевірити, що Ермітові криві (зокрема еліптичі), а також кватрики Клейна досягають верхньої межі, тобто мають найбільшу із можливих кількість раціональних точок. Оскільки ця величина визначає довжину відповідного алгебро-геометричного коду, доцільно застосовувати саме вказані криві.

## Література


[1] *Гоппа В. Д.* Алгебраико-геометрические коды // *Изв. АН СССР. Сер. матем.* — 1982. — Vol. 46, no. 4. — Pp. 762–781.

[2] *Гоппа В. Д.* Коды, ассоциированные с дивизорами // *Пробл. передачи информ.* — 1977. — Vol. 13, no. 1. — Pp. 33–39.

[3] *Hao Chen.* Algebraic geometric codes with applications // *Frontiers of Mathematics in China.* — 2007. — Vol. 2, no. 1. — Pp. 1–11.

[4] *Цфасман М. А.* Коды Гоппы, лежащие выше границы Варшамова–Гилберта // *Пробл. передачи информ.* — 1982. — Vol. 18, no. 3. — Pp. 3–6.

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

[6] *Cheng Qi.* Hard problems of algebraic geometry codes.

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

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

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

[10] *Goldschmidt D. M.* Algebraic functions and projective curves. — Springer, 2002.

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

[12] *Coblitz N.* Algebraic Aspects of Cryptography. — Springer, 2002.