清 华 大 学

综 合 论 文 训 练

题目：有限域上代数曲线在编码理论中的应用

系　　别：数学科学系

专　　业：数学与应用数学

姓　　名：侯贺冬

指导教师：马连荣　副教授

2021 年 6 月 24 日

关于学位论文使用授权的说明

本人完全了解清华大学有关保留、使用学位论文的规定，即：学校有权保留学位论文的复印件，允许该论文被查阅和借阅；学校可以公布该论文的全部或部分内容，可以采用影印、缩印或其他复制手段保存该论文。

(涉密的学位论文在解密后应遵守此规定)

签　名：侯贺冬　导师签名：马连荣　日　期：2024年6月9日

中文摘要

本篇文章首先回顾了椭圆曲线相关理论, 给出了其群结构和自同态环的清晰刻画, 并基于此复现了有限域上椭圆曲线的有理点估计定理, Hasse 定理. 文章进而提供了基于有限平面中的直线族设计的线性码和基于椭圆曲线族的线性码的建构过程和基本性质的分析. 我们进一步地通过数值计算研究了基于椭圆曲线族的线性码, 特别研究了两类情形: 包含素数个元素的有限域 $\mathbb{F}_p$ 和特征为 2 的有限域 $\mathbb{F}_{2^s}$. 我们给出了关于基于 $\mathbb{F}_p$ 设计的关联矩阵的秩, 基于 $\mathbb{F}_{2^s}$ 设计的关联矩阵的秩和对应线性码 $\mathcal{C}_{2^s}$ 的最小距离的猜想.

关键词：椭圆曲线；线性码；有限域；有限平面

ABSTRACT

In this thesis, we first review some fundamental theory on elliptic curves, especially on the group structure and their endomorphism rings. Based on these works, we show the estimation theorem of the number of rational points on elliptic curves over finite fields, so-called Hasse's theorem. In addition to this, we study two kinds of linear codes, which are based on finite planes and families of lines or elliptic curves, respectively. Some basic analysis is also provided. Furthermore, we propose a series of conjectures about linear codes constructed by elliptic curves over finite fields $\mathbb{F}_p$ and $\mathbb{F}_{2^s}$ through intensive numerical computation. They cover the rank of parity-check matrices, and the minimum distance of these codes.

Keywords: elliptic curves; linear codes; finite fields; finite planes

目　　录

主要符号对照表

$[n,k,d;q]$ 码	一个码长为 n, 维数是 k, 最小距离是 d 的 q 进制线性码
$\mathbb{A}^2(k)$	域 k 上的仿射平面
$\mathbb{F}_q$	元素个数为 q 的有限域
$\mathbb{F}_q^n$	有限域 $\mathbb{F}_q$ 上的 n 维线性空间
$\mathbb{P}^2(k)$	域 k 上的射影平面
$\mathbb{Z}/n$	商群 $\mathbb{Z}/n\mathbb{Z}$, 或记作 $\mathbb{Z}/(n)$
$\operatorname{card} A$	集合 A 的势
C_q	由 $\mathbb{F}_q$ 上椭圆曲线构造的线性码
$\operatorname{char} k$	域 k 的特征
$\operatorname{Div}(C)$	光滑曲线 C 的除子群
$\operatorname{End}(C)$	椭圆曲线 (C,O) 的自同态群
$\operatorname{Gal}(L/K)$	域扩张 L/K 的 Galois 群
$\operatorname{GL}(n,k)$	矩阵环 $M_n(k)$ 中可逆矩阵全体在矩阵乘法运算下构成的环
$\operatorname{Im}\phi$	映射 ϕ 的像
$\ker\phi$	映射 ϕ 的核
$\operatorname{LHS}(1)$	式 (1) 的左手侧项
$\operatorname{ord}(a)$	群中元素 a 的周期
$\overline{k}$	域 k 的代数闭包
ϕ_q	有限域 $\mathbb{F}_q$ 上椭圆曲线的 Frobenius 映射
$\operatorname{Pic}(C)$	光滑曲线 C 的 Picard 群
$\rho(A)$	矩阵 $A \in M_{m\times n}(\mathbb{F}_2)$ 作为 $\mathbb{F}_2$ 上矩阵的秩
$\operatorname{RHS}(1)$	式 (1) 的右手侧项
$A(i,j)$	矩阵 A 的第 i 行第 j 列元素
$A=(a_{ij})_{m\times n}$	第 i 行第 j 列元素是 a_{ij} 的 $m\times n$ 矩阵 A
A^T	矩阵 A 的转置
$c=(c_i)_{1\leqslant i\leqslant n}$	向量 $c=(c_1,c_2,\cdots,c_n)$
$d(C)$	码 C 的最小距离
H_q	由 $\mathbb{F}_q$ 上椭圆曲线构造的 $\mathbb{F}_2$ 矩阵
$i(P;C,D)$	光滑曲线 C,D 在 P 点的相交重数
I_n	尺寸为 n 阶的单位阵

$k(C)$	光滑曲线 C 在 k 上的函数域
$k[x_1, \cdots, x_n]_d$	域 k 上的 n 元多项式环中次数为 d 的全体多项式构成的集合
$k[x_1, \cdots, x_n]$	域 k 上的 n 元多项式环
k^*	域 k 的乘法群
$L_P(C)$	光滑曲线 C 在 P 点的切线
$M(A)$	矩阵 A 的行数
$M_n(R)$	交换环 R 上的 $n \times n$ 矩阵全体
$M_{m\times n}(R)$	交换环 R 上的 $m \times n$ 矩阵全体
$N(A)$	矩阵 A 的列数
$w(\mathbf{x})$	码字 $\mathbf{x}$ 的重量
$w_c(A; j)$	矩阵 A 的第 j 列列重
$w_r(A; i)$	矩阵 A 的第 i 行行重
$Z_F(k)$	射影平面 $\mathbb{P}^2(k)$ 中齐次多项式 F 的零点集
$Z_f(k)$	仿射平面 $\mathbb{A}^2(k)$ 中多项式 f 的零点集

第 1 章　研究简介

代数曲线是一门研究射影空间中齐次多项式零点, 或仿射平面中多项式零点构成的集合的学科 [1-2]. 它在编码理论中也有很多的应用, 比如由一条特定代数曲线构造的 Goppa 码, 和射影曲线

$$y^p - y = ax + \frac{1}{x}$$

上有理点个数相关的 Melas 码和 Zetterberg 码, 其中 p 是一个素数. 关于以上码的具体定义和相关性质, 读者可以参考 [3]. 此外, 还有和超奇异椭圆曲线相关的 Reed-Muller 码, 关于这类码的性质, 读者可以参考 [4]; 关于上述关系, 读者可以参考 [5].

我们由此进而考查一类由有限域上的代数曲线族通过构造关联矩阵 (incidence matrix) 并将关联矩阵作为校验矩阵 (parity-check matrix) 给出的线性码.

现今人们设计的这类线性码主要包括: 通过有限域上的直线族或一般 t 维超平面族构造的码和通过有限域上的椭圆曲线族构造的码. 这类码的构造方式陈述如下. 考查仿射空间或射影空间上的全体点和一些特定的代数曲线族, 而后在一定的限制下给出点和所取代数曲线族之间的关联矩阵, 并由此作为校验矩阵得到一个线性码. 注意到这类码的校验矩阵从构造角度而言并不复杂, 但其代数特征, 如秩, 对应码的最小距离等并不易获得. 这样的码由此获得了大家的普遍关注.

我们举直线族或超平面族得到的码为例, [6-7] 研究了有限域 $\mathbb{F}_q$ 的射影平面 $\mathbb{P}^2\left(\mathbb{F}_q\right)$ 上 1 维直线和点形成的关联矩阵的秩, [7] 还给出了由这类关联矩阵作为校验矩阵得到的码的最小距离. 更进一步地, [8-9] 分别给出了一般射影空间 $\mathbb{P}^d\left(\mathbb{F}_q\right)$ 中 $d-1$ 维超平面族和点形成的关联矩阵的秩. 特别地, [8] 还给出了在有限域 $\mathbb{F}_q$ 中 q 是一个素数的情况下, 一般的射影空间 $\mathbb{P}^d\left(\mathbb{F}_p\right)$ 中 $t(1 \leqslant t \leqslant d)$ 维超平面和点形成的关联矩阵的秩. 在这一问题上的集大成者是 [10], 这篇文章得到了任意有限域 $\mathbb{F}_q$ 上的射影空间 $\mathbb{P}^d\left(\mathbb{F}_q\right)$ 中 $t(1 \leqslant t \leqslant d)$ 维超平面和点形成的关联矩阵的秩.

相对应地, 我们只需要在对应的射影空间上去掉原点和所有过原点的对应曲线或平面就能获得仿射空间中此类关联矩阵. 对这类关联矩阵的研究始于 [8], 这篇文章给出了有限域 $\mathbb{F}_q$ 上 $d+1$ 维仿射空间 $\mathbb{A}^{d+1}\left(\mathbb{F}_q\right)$ 中 d 维超平面和点形成的关联矩阵的秩. 进一步地, [10] 给出了绝大多数一般有限域 $\mathbb{F}_q$ 上 $d+1$ 维仿射空间 $\mathbb{A}^{d+1}\left(\mathbb{F}_q\right)$ 中 $t(1 \leqslant t \leqslant d)$ 维超平面和点形成的关联矩阵的秩. 而 [11] 完全回答了

这一问题.

通过椭圆曲线族建构码的想法来源于 [12], 这篇文章给出了通过选取有限平面上特定的椭圆曲线族和所有点在椭圆曲线取逆意义下形成的等价类之间的关系, 构造了一类关联矩阵, 并以此作为校验矩阵定义了一类线性码. 这篇文章同时给出了关于这类码的校验矩阵的尺寸, 围长和密度等基本性质的分析.

我们的研究将以这篇文章中建构的线性码为基础, 将对这类码的校验矩阵的秩和这类码的最小距离进行深入分析. 我们的研究注意到, 基于 $\mathbb{F}_p$(p 是一个素数) 的仿射平面 $\mathbb{A}^2\left(\mathbb{F}_p\right)$ 上的椭圆曲线设计的关联矩阵应当是一个列满秩矩阵 (除 $p=3$). 而基于特征为 2 的有限域 $\mathbb{F}_{2^s}$ 的仿射平面 $\mathbb{A}^2\left(\mathbb{F}_{2^s}\right)$ 上的椭圆曲线设计的关联矩阵的秩应当是 3^s-1. 以此为校验矩阵设计的线性码的最小距离应当是 2^s+2 (除 $s=1,2$). 我们进行了大量的数值计算和相关程序设计, 提出了上述猜想.

我们的文章中对椭圆曲线上群结构中结合律的证明避免了一般教材中对 Cayley-Bacharach 定理的错误使用. 此外, 文章还结合 [13-14] 提出利用分块循环矩阵的方法证明有限域 $\mathbb{F}_{2^s}$ 的仿射平面 $\mathbb{A}^2\left(\mathbb{F}_{2^s}\right)$ 上直线族和点形成的关联矩阵的秩, 也值得读者关注.

文章分为 5 个部分. 第二部分回顾了一般域上的椭圆曲线的群结构和自同态环, 并证明了有限域上椭圆曲线的有理点估计, Hasse 定理. 第三部分提供了线性码的基本知识和基于有限平面中的直线族设计的线性码的相关分析. 第四部分先回顾了基于有限平面中的椭圆曲线族的线性码的建构过程和对关联矩阵的尺寸, 围长和密度等基本性质的分析. 最后基于数值计算结果, 我们提出了关于 $\mathbb{F}_p$ 和 $\mathbb{F}_{2^s}$ 的情况下关联矩阵的秩和对应线性码最小距离的猜想. 第五部分陈述了相关结论.

第 2 章　椭圆曲线

设 k 是一个域.

2.1　椭圆曲线的基本结构

2.1.1　仿射平面, 射影平面和代数曲线

我们在下文中关于仿射平面和射影平面中的讨论将遵循 [15-16].

定义 k 上的**仿射平面** $\mathbb{A}^2(k)$ 为

$$\mathbb{A}^2(k) := \left\{(x_1, x_2) \in k^2\right\}.$$

给定 $k^3 \setminus \{(0,0,0)\}$ 上的点的一个等价关系: $(x_1, x_2, x_3) \sim (x_1', x_2', x_3')$ 如果存在 $\lambda \in k^*$ 使得 $(x_1', x_2', x_3') = \lambda(x_1, x_2, x_3)$. 记点 (x_1, x_2, x_3) 在这个等价关系下所在的等价类为 $[x_1, x_2, x_3]$, 则 k 上的**射影平面** $\mathbb{P}^2(k)$ 定义为:

$$\mathbb{P}^2(k) := \left\{[x_1, x_2, x_3] | (x_1, x_2, x_3) \in k^3 \setminus \{(0,0,0\}\right\}.$$

我们称 $[x_1, x_2, x_3]$ 是 $\mathbb{P}^2(k)$ 中对应点的**齐次坐标**.

考查仿射平面到射影平面的嵌入 $\iota_i : \mathbb{A}^2(k) \to \mathbb{P}^2(k)(1 \leqslant i \leqslant 3)$, 其中 $\iota_1(y_1, y_2) = [1, y_1, y_2], \iota_2(y_1, y_2) = [y_1, 1, y_2], \iota_3(y_1, y_2) = [1, y_1, y_2]$. 定义

$$U_i = \{[x_1, x_2, x_3] \in \mathbb{P}^2(k) | x_i \neq 0\}, H_i = \{[x_1, x_2, x_3] \in \mathbb{P}^2(k) | x_i = 0\} (1 \leqslant i \leqslant 3).$$

注意到 ι_i 是从 $\mathbb{A}^2(k)$ 到 U_i 的双射, $\bigcup_{i=1}^3 U_i = \mathbb{P}^2(k)$, 因此每个 $\mathbb{P}^2(k)$ 上的点都可以通过 $\{(\mathbb{A}^2(k), \iota_i)\}_{1 \leqslant i \leqslant 3}$ 给出一个**仿射局部坐标**.

另外, 我们再考查 $\mathbb{P}^2(k)$ 上的**射影变换**, 即 $\mathrm{GL}(3, k)$ 在 $\mathbb{P}^2(k)$ 上的作用. 任取点 $[x, y, z] \in \mathbb{P}^2(k)$ 和 $\boldsymbol{\Phi} \in \mathrm{GL}(3, k)$, 记 $(x', y', z') = \boldsymbol{\Phi}(x, y, z)$, 则我们称 $\boldsymbol{\Phi}$ **作用**在点 $[x, y, z]$ 上得到点 $[x', y', z']$. 易见这个作用是良好定义的, 而且 $\mathrm{GL}(3, k)$ 在 $\mathbb{P}^2(k)$ 上的作用是可迁的, 因为 $\mathrm{GL}(3, k)$ 在 $k^3 \setminus \{(0,0,0)\}$ 上的作用是可迁的. 因此固定某个 $[x_0, y_0, z_0] \in \mathbb{P}^2(k)$ 时, 我们都可以选取某个 $\boldsymbol{\Phi} \in \mathrm{GL}(3, k)$ 使得 $\boldsymbol{\Phi}[x_0, y_0, z_0] = [0, 0, 1]$, 那么我们由此可以给出 $\mathbb{A}^2(k)$ 到 $\mathbb{P}^2(k)$ 的另一个嵌入 $\iota := \boldsymbol{\Phi}^{-1} \circ \iota_3 : \mathbb{A}^2(k) \to \mathbb{P}^2(k)$. 注意到 $\iota(0, 0) = [x_0, y_0, z_0]$.

我们称 C 是 k 上的一条 d **次 (代数平面射影) 曲线** ($d \in \mathbb{N}$), 如果存在 d 次齐

次多项式 $F \in k[x,y,z]_d$ 使得

$$\{[x,y,z] \in \mathbb{P}^2(k) | F(x,y,z) = 0\} =: Z_F(k) = C.$$

注意到由于 F 是一个齐次多项式, $Z_F(k)$ 在 $\mathbb{P}^2(k)$ 上总是良定义的. 1 次平面曲线可以简称**直线**. 我们称 C' 是 k 上的一条 **(平面) 仿射曲线**, 如果存在 $F \in k[x,y,z]_d$ 使得

$$C' = \{(x,y) \in \mathbb{A}^2(k) | F(\iota_3(x,y)) = 0\}.$$

在上下文不引发歧义时, 我们有时也称仿射曲线为曲线.

设 $C = Z_F(k)$ 是 k 上的一条平面曲线. 点 $[x_0,y_0,z_0] \in C$, 我们称点 $[x_0,y_0,z_0]$ 是**非奇异点**, 如果

$$\frac{\partial F}{\partial x}(x_0,y_0,z_0), \frac{\partial F}{\partial y}(x_0,y_0,z_0), \frac{\partial F}{\partial z}(x_0,y_0,z_0)$$

在 k 中不全为 0. 否则称 $[x_0,y_0,z_0]$ 是一个**奇点**. 我们称 $C = Z_F(k)$ 是**非奇异的** (或**光滑的**), 如果 $Z_F(\overline{k})$ 上每个点都是非奇异的, 否则称为**奇异的**, 其中 $\overline{k}$ 是 k 的代数闭包. 如果 $P \in C = Z_F(k)$ 是一个非奇异点, 定义多项式

$$G(x,y,z) = \frac{\partial F}{\partial x}(x_0,y_0,z_0)x + \frac{\partial F}{\partial y}(x_0,y_0,z_0)y + \frac{\partial F}{\partial z}(x_0,y_0,z_0)z \in k[x,y,z]_1$$

在 $\mathbb{P}^2(k)$ 中的零点集 $Z_G(k)$ 为 C 的**切线**, 记作 $L_P(C)$.

2.1.2 椭圆曲线的定义

通过 Weierstrass 标准型的定义 一个简单的定义椭圆曲线的方案来自 [16][42]:

定义 2.1: 在 $\mathbb{P}^2(k)$ 中形如

$$y^2z + a_1xyz + a_3yz = x^3 + a_2x^2z + a_4xz_2 + a_6z^3$$

的一条非奇异三次曲线称作**椭圆曲线**.

事实上, 满足一定条件的 $\mathbb{P}^2(k)$ 上的非奇异三次曲线都能够转化成为这种标准形式, 我们将在2.1.3中讨论这一过程.

通过曲线亏格的定义 一种使用更多代数几何语言的定义方式来自 [17][59]. 这则定义直接将椭圆曲线和它的群结构联系起来, 我们将在2.1.4中详细讨论椭圆曲线上的群结构. 在表述这个定义之前, 我们需要先引用曲线形式的 Riemann-Roch 定理, 关于下文内容, 读者可以参考 [15][章 1] 或 [17][章 1-2].

设 C 是一条光滑曲线, 记 $k(C)$ 是 k 上曲线 C 的函数域, $\mathrm{Div}(C)$ 是 C 的除子

群. 每个除子 $D \in \mathrm{Div}(C)$ 都可以写作形式和

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

其中 $n_P \in \mathbb{Z}$ 而且只有有限多个 n_P 非零. 我们称

$$\sum_{P \in C} n_P$$

为 D 的**度**, 记作 $\deg D$.

设 $P \in C$ 是一个非奇异点, $\overline{k}[C]_P$ 是曲线 C 在 P 点的局部环, $\mathfrak{m}_P$ 是 $\overline{k}[C]_P$ 的极大理想. 定义 $\overline{k}[C]_P$ 上的**赋值**映射 $v_P : \overline{k}[C]_P \to \mathbb{N}_0 \cup \{\infty\}$ 为

$$v_P(f) = \sup\{d \in \mathbb{Z} | f \in \mathfrak{m}_P^d\},$$

并通过 $v_P\left(\frac{f}{g}\right) = v_P(f) - v_P(g)$ 延拓至 $\overline{k}(C)$ 上. 我们称

$$\sum_{P \in C} v_P(f) P$$

为 f 的**除子**, 记作 (f). 注意到对于每个 f, 只有有限多个 $v_p(f)$ 取值不为 0, 所以它是良好定义的. 我们称一个除子 $D \in \mathrm{Div}(C)$ 是一个**主除子**, 如果存在某个 $f \in \overline{k}(C)^*$ 使得 $(f) = D$.

我们称两个除子 $D_1, D_2 \in \mathrm{Div}(C)$ 是**线性相关**的, 如果 $D_1 - D_2$ 是一个主除子. 不难验证这是一个等价关系. 称除子群 $\mathrm{Div}(C)$ 在这个等价关系下的商群为 **Picard 群** (或**除子类群**), 记作 $\mathrm{Pic}(C)$.

一种直接给出典范除子定义的方案来自于 [17]^{31}. 设 t 是 $\overline{k}(C)$ 在 P 点的一致化元 (uniformizer), 则对于任意 C 上的非零微分形式 ω, 都存在唯一的一个函数 $g \in \overline{k}(C)$ 使得 $\omega = g\,dt$, 记 $\frac{\omega}{dt} := g$. 我们称 $v_P\left(\frac{\omega}{dt}\right)$ 是 ω 在 P 点的**阶**, 记作 $v_P(\omega)$. 对于每个非零的微分形式 ω, 至多有有限个点 $P \in C$ 使得 $v_P(\omega) \neq 0$. 定义 ω 对应的除子 $(\omega) \in \mathrm{Div}(C)$ 为

$$(\omega) := \sum_{P \in C} v_P(\omega) P.$$

我们称一个除子 D 是一个**典范除子** (canonical divisor), 如果存在某个微分形式 ω 使得 D 和 (ω) 在 $\mathrm{Pic}(C)$ 中对应同一个元素. 详细的讨论请参考 [17]^{31}.

另一种定义典范除子的方式来源于 [15]^{295}, 需要使用更多的层论的语言. 考查 C 在 k 上的相对微分层 Ω_C, 由于 C 是一条一维曲线, 所以 Ω_C 是 C 上的可逆层, 因此等于 C 上的典则层 ω_C. 它对应的线性等价类中的每一个除子都称作一个**典范除子**.

我们称一个除子 $\sum_{P\in C} n_P P = D \in \mathrm{Div}(C)$ 是一个**有效除子**, 如果对每个 $P \in C$ 都有 $n_P \geqslant 0$. 我们记 $\mathscr{L}(D)$ 是

$$\mathscr{L}(D) := \{f \in \overline{k}(C)^* | (f) + D\text{是有效除子}\} \cup \{0\}.$$

已知 $\mathscr{L}(D)$ 是一个有限维 $\overline{k}$-线性空间, 关于此事实的证明请参考 [15]^{122}. 记 $\dim \mathscr{L}(D) = l(D)$, 我们有 Riemann-Roch 定理.

定理 2.1 (Riemann-Roch)： 设 C 是一条光滑曲线, K 是 C 上的一个典范除子, 那么, 存在一个整数 $g \geqslant 0$ 使得每个在 C 的除子群 $\mathrm{Div}(C)$ 中的元素 $D \in \mathrm{Div}(C)$ 都有

$$l(D) - l(K - D) = \deg D - g + 1.$$

其中 g 称作 C 的**亏格**.

证明： 请参考 [15]$^{295\text{-}296}$. □

在 Riemann-Roch 定理的保障下, 我们这样定义椭圆曲线:

定义 2.2： 设 C 是 k 上的一条亏格为 1 的非奇异曲线, $O \in C$, 我们就称序对 (C, O) 是 k 上的一条**椭圆曲线**.

2.1.3 Weierstrass 标准形式

我们这节讨论定义2.1的合理性, 也即建立满足一定条件的 $\mathbb{P}^2(k)$ 上非奇异三次曲线的 Weierstrass 标准形式.

我们先给出曲线和直线相交重数的概念.

设 $C = Z_F(k)$ 是 k 上的一条曲线, $L = Z_G(k)$ 是一条直线, $F \in k[x, y, z]_d, G \in k[x, y, z]_1$, 设 $P = [x_0, y_0, z_0] \in C \cap L$. 选取嵌入 $\iota : \mathbb{A}^2(k) \to \mathbb{P}^2(k)$ 使得 $\iota(0, 0) = [x_0, y_0, z_0]$. 记 $f(x, y) = F(\iota(x, y)), g(x, y) = G(\iota(x, y))$. 注意到此时 f, g 未必再是齐次多项式, 因此考查齐次分解 $f(x, y) = f_0(x, y) + f_1(x, y) + \cdots + f_d(x, y), g(x, y) = g_0(x, y) + g_1(x, y)$, 其中 $f_i(x, y), g_i(x, y) \in k[x, y]_i (1 \leqslant i \leqslant d)$. 但显然有 $f(0, 0) = g(0, 0) = 0$, 所以 $f_0(x, y) = g_0(x, y) = 0$.

记 $g_1(x, y) = ax + by$, 其中 $a, b \in k$ 且不全为 0, 则 $g(x, y) = 0$ 的零点集 $Z_g(k) \subset \mathbb{A}^2$ 有参数表示 $\phi : k \to Z_g(k)$

$$\phi(t) = \begin{bmatrix} -bt \\ at \end{bmatrix}.$$

从而考查

$$f(\phi(t)) = \sum_{i=1}^{d} f_i(-bt, at) = \sum_{i=1}^{d} t^i f_i(-b, a).$$

我们称 C 和 L 在 P 点的**相交重数** $i(P; C, L)$ 为

$$i(P; C, L) = \begin{cases} \min\{i \in \mathbb{N} | 1 \leqslant i \leqslant d, f_i(-b, a) \neq 0\} & \text{if } f(\phi(t)) \neq 0 \\ +\infty & \text{otherwise} \end{cases}.$$

为了方便, 我们也说 $i(P; C, L) = 0$, 如果 $P \notin C \cap L$. 线性代数知识表明: 容易证明 $i(P; C, L)$ 和所选取的局部仿射坐标系无关.

我们称 C 上的一个非奇异点 P 是一个**拐点**, 如果 P 对 C 的切线 $L_P(C)$ 和 C 在 P 点的相交重数 $i(P; C, L_P(C)) \geqslant 3$.

事实上, 相交重数也有一个使用更多代数几何语言的定义方式. 我们不对此引入更多的预备知识, 这一部分的内容请参考 [18]章 11 和 [15]53. 考虑分层环 $S = k[x, y, z] = \bigoplus_{d \in \mathbb{N}_0} S_d$, 其中 $S_d = k[x, y, z]_d$. 设 C_1, C_2 是 $\mathbb{P}^2(k)$ 上的两条曲线, 它们在 S 中生成的理想分别记作 I_{C_1}, I_{C_2}, 也即 $I_{C_i} = \{f \in S | f|_{C_i} = 0\}$. 设 $P \in C_1 \cap C_2$, $\mathfrak{p}$ 是 P 对应的 S 的齐次素理想. 设 M 是一个 S-模, 我们记 $\mathtt{l}_{\mathfrak{p}}(M)$ 是 $M_{\mathfrak{p}}$ 在 $S_{\mathfrak{p}}$ 中的 Krull 长度. 定义 C_1, C_2 在 $P \in C$ 点的**相交重数** $i(P; C_1, C_2)$ 为

$$i(P; C_1, C_2) = \mathtt{l}_{\mathfrak{p}}\left(S/(I_{C_1} + I_{C_2})\right).$$

我们来陈述本节主要命题.

命题 2.1： 设 k 是一个域, $\mathrm{char}(k) \neq 2$, $C = Z_F(k)$ 是 k 上的一条非奇异三次曲线, $[x_0, y_0, z_0]$ 是 C 的一个拐点, 则存在一个射影变换 $\Phi \in \mathrm{GL}(3, k)$ 使得 $Z_{F \circ \Phi^{-1}} = Z_{\mathcal{W}}$, 其中 $\mathcal{W} \in k[x, y, z]_3$ 且形如

$$\mathcal{W}[x, y, z] = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3, \quad a_i \in k (1 \leqslant i \leqslant 6). \tag{2.1}$$

我们称形式

$$\mathcal{W}[x, y, z] = 0$$

为 **Weierstrass 标准型**, 如果 $\mathcal{W}[x, y, z] \in k[x, y, z]_3$ 且形如式(2.1). 相应地, 我们称 $Z_{\mathcal{W}}(k)$ 在 U_3 中的限制给出的标准型

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.2}$$

为**仿射 Weierstrass 标准型**. 在上下文语义清楚时, 我们不做区分.

注释 2.1： Weierstrass 标准型事实上对于特征为 2 的域 k 也成立. 我们这里只是

为了介绍射影变换证明的方法.

通过射影变换的证明 我们首先给出使用较少代数几何语言的证明.

证明： 考查 $\mathbb{P}^2(k)$ 上三次曲线一般形式

$$\begin{aligned} F(x,y,z) = {} & ax^3 + bx^2y + cxy^2 + dy^3 + ex^2z \\ & + fxyz + gy^2z + hxz^2 + iyz^2 + jz^3 = 0. \end{aligned}$$

证明分成以下几步.

Step 1 设 C 的拐点是 $O := [0,1,0]$. 否则考虑射影变换 $\boldsymbol{\Phi}_1 \in \mathrm{GL}(3,k)$ 使得 $\boldsymbol{\Phi}_1[x_0,y_0,z_0] = [0,1,0]$. 由于 $i(P,C,L_P(C))$ 与所选局部仿射坐标系无关, 我们知道 $[0,1,0]$ 是 $Z_{F\circ\boldsymbol{\Phi}_1^{-1}}$ 的拐点. 因此有 $d=0$. 同时注意到 $[0,1,0]$ 是一个非奇异点,

$$\frac{\partial F}{\partial x}(0,1,0) = c, \quad \frac{\partial F}{\partial y}(0,1,0) = 0, \quad \frac{\partial F}{\partial z}(0,1,0) = g,$$

所以有 $c \neq 0$ 或 $g \neq 0$. 这一步需要 $\mathrm{char}(k) \neq 2$.

Step 2 我们进一步假设 $L_O(C) = H_3 = \{[x,y,z] \in \mathbb{P}^2(k) | z = 0\}$. 否则, 假设 $L_O(C)$ 对应的形式是 $\mathfrak{L}(x,y,z) = cx + gz = 0$. 根据线性代数, 找到矩阵 $M = (m_{ij})_{2\times 2} \in \mathrm{GL}(2,k)$ 满足

$$cm_{11} + gm_{21} = 0.$$

则考查 $\boldsymbol{\Phi}_2 \in \mathrm{GL}(3,k)$ 使得

$$\boldsymbol{\Phi}_2^{-1} = \begin{bmatrix} m_{11} & 0 & m_{12} \\ 0 & 1 & 0 \\ m_{21} & 0 & m_{22} \end{bmatrix}.$$

注意到 $Z_{\mathfrak{L}\circ\boldsymbol{\Phi}_2^{-1}} = H_3$, 而且 $Z_{F\circ\boldsymbol{\Phi}_1^{-1}\circ\boldsymbol{\Phi}_2^{-1}}$ 以 $[0,1,0]$ 为拐点, 切线即是 H_3. 从而我们总可以假设 $c=0, g\neq 0$.

Step 3 注意到条件 $i(O;Z,F) \geqslant 3$ 给出 $b=0, Z \nmid F$, 其中 $Z \in k[x,y,z]_1$, 定义 $Z(x,y,z) = z$. 特别地, 有 $a \neq 0$.

进一步考查 $\boldsymbol{\Phi}_3 \in \mathrm{GL}(3,k)$ 使得

$$\boldsymbol{\Phi}_3 = \begin{bmatrix} -\frac{a}{g} & & \\ & -\frac{a}{g} & \\ & & 1 \end{bmatrix}.$$

记 $\boldsymbol{\Phi} = \boldsymbol{\Phi}_3 \circ \boldsymbol{\Phi}_2 \circ \boldsymbol{\Phi}_1 \in \mathrm{GL}(3, k)$, 则有

$$F \circ \boldsymbol{\Phi}(x, y, z) = \frac{g^3}{a^2}(y^2 z - x^3) + (\text{Other Terms}).$$

我们即证明了所要的结论.

□

通过 Riemann-Roch 定理的证明 详细的证明需要较多理论上的准备, 囿于篇幅所限, 请参考 [17]$^{61\text{-}62}$. 注意这个证明对于域 k 的特征没有限制.

Weierstrass 简化标准型 在域特征 $\mathrm{char}\, k \neq 2$ 的时候, 考查坐标变换

$$x' = x, \quad y' = y + \frac{1}{2}(a_1 + a_3),$$

式(2.2)可变化为

$$(y')^2 = f(x') = (x')^3 + a(x')^2 + bx' + c, \tag{2.3}$$

其中 $a, b, c \in k$, 此时非奇异的条件是 $f(x')$ 无重根, 即在 k 中判别式 $\Delta = a^2 b^2 - a^3 c - b^3 \neq 0$. 在域特征 $\mathrm{char}\, k \neq 2, 3$ 的时候, 还可以进一步考虑变换

$$x'' = x' + \frac{a}{3}, \quad y'' = y,$$

则式(2.3)可转化为

$$(y'')^2 = g(x'') = (x'')^3 + dx'' + e, \tag{2.4}$$

其中 $d, e \in k$, 此时非奇异的条件是在 k 中判别式 $\Delta = -16(4d^3 + 27e^2) \neq 0$.

我们下面来考虑 $\mathrm{char}\, k = 3$ 时椭圆曲线的标准型. 此时标准型只能由式(2.3)给出. 我们考虑以下两种情形.

Case 1 $a \neq 0$. 此时可以考虑配方, 通过取某个 $u \in k$ 使得在坐标变换 $\hat{x} = x' + u, \hat{y} = y'$ 下有形式

$$\hat{y}^2 = \hat{x}^3 + \hat{a}\hat{x}^2 + \hat{c},$$

其中 $\hat{a}, \hat{c} \in k$, 此时非奇异的条件是 $\Delta = 2\hat{a}^3\hat{b} \neq 0$.

Case 2 $a = 0$. 此时即直接有形式

$$(y')^2 = f(x') = (x')^3 + bx' + c,$$

此时非奇异的条件是 $\Delta = 2b^3 \neq 0$.

我们最后来考虑 $\operatorname{char} k = 2$ 时的情况. 让我们回到式(2.2):

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Case 1 $a_1 \neq 0$. 考查坐标变换

$$x_1 = \frac{a_1x - a_3}{a_1^3}, y_1 = \frac{a_1^3y - a_1^2a_4 - a_3^2}{a_1^6}$$

时有

$$y_1^2 + x_1y_1 = x_1^3 + ax_1^2 + b.$$

注意到此时非奇异的条件是 $\Delta = b \neq 0$.

Case 2 $a_1 = 0$. 考查坐标变换

$$x_1 = x - a_2, y_1 = y$$

时有

$$y_1^2 + cy_1 = x_1^3 + ax + b.$$

注意到此时非奇异的条件是 $\Delta = c^2 \neq 0$.

2.1.4 椭圆曲线的群结构

我们在下文中统一记 $O = [0, 1, 0] \in \mathbb{P}^2(k)$ 是椭圆曲线 $C \subset \mathbb{P}^2(k)$ 的拐点.

椭圆曲线上的运算 为了表述椭圆曲线上的运算, 我们先引入 Bézout 定理.

定理 2.2 (Bézout): 设 C_1, C_2 是两条 $\mathbb{P}^2(k)$ 上的曲线, 相交于有限多个点. 记 $C_1 \cap C_2 = \{P_1, \cdots, P_s\}$, 则有

$$\sum_{j=1}^{s} i(P_j; C_1, C_2) = \deg(C_1)\deg(C_2).$$

证明: 关于曲线的次数 $\deg(C_i)$ 的定义和 Bézout 定理的证明, 请参考 [15]$^{52\text{-}54}$. □

设 C 是 k 上的一条椭圆曲线, 任取 $P, Q \in C$. 如果 P, Q 是相异的两点, 取 L 是过 P, Q 两点的直线; 否则取 L 是在 P 点曲线 C 的切线. 我们以下都按这一方法选取过两点的直线. 由 Bézout 定理, L 与 C 交于另一点 R. 设 L' 是过 O, R 两点的直线, 记 L' 和 C 的另一个交点为 $P + Q$, 由此给出椭圆曲线上点的运算 ($\mathscr{A}$).

椭圆曲线上的群结构 注意到 ($\mathscr{A}$) 显然满足交换律, 而且对于任意 $P \in C$, 过 O, P 做直线交 C 于点 Q, 则显然过 O, Q 的直线交 C 于点 P, 即说明 O 是运算 ($\mathscr{A}$) 的

零元素. 进一步地, 我们注意到上述 P, Q 所在的直线过 O 点, 而 O 点又是 C 的拐点, 所以过 O, O 的直线 (即 C 在 O 的切线 $T_O(C)$) 交 C 于点 O, 即说明 Q 是 P 关于运算 ($\mathscr{A}$) 的逆, 由此证明了逆元素的存在性.

为了验证椭圆曲线关于这一运算形成一个 Abel 群, 我们只需验证 ($\mathscr{A}$) 满足结合律. 为此, 我们先预备 Cayley-Bacharach 定理.

定理 2.3 (Cayley-Bacharach)： 设 k 是一个代数闭域, $\gamma_1 = Z_f(k)$, $\gamma_2 = Z_g(k)$ 是两条三次 (仿射) 曲线, 交在 9 个不同的点 $A_1, \cdots, A_9 \in \mathbb{A}^2(k)$. 设 $\gamma = Z_h(k)$ 也是一条三次曲线, 而且通过 $\{A_1, \cdots, A_9\}$ 中的 8 个点, 则 H 可以写成 F, G 的 k-线性组合, 即存在 $\lambda, \mu \in k$ 满足

$$h(x, y) = \lambda f(x, y) + \mu g(x, y).$$

特别地, γ 也通过剩下的那个点.

证明： 证明结合了 [19-20]. 记 $\mathcal{A} := \{A_1, \cdots, A_9\}$, 假设存在三次多项式 $h(x, y) \in k[x, y]_{\leqslant 3}$ 使得 $\gamma = Z_h(k) \subset \mathbb{A}^2(k)$ 通过 $\mathcal{A}' := \{A_1, \cdots, A_8\}$ 但不能写成 f, g 的 k-线性组合. 注意到 k 是一个无限域, 这保证了我们以下点的选取的合理性.

Step 1 观察到没有 4 个 $\mathcal{A}$ 中的点共线. 否则, 设 $L_1 \subset \mathbb{P}^2(k)$ 是一条直线, 而且 $\operatorname{card}(L_1 \cap \mathcal{A}) \geqslant 4$. 而 $\deg L_1 \deg \gamma_1 = \deg L_1 \deg \gamma_2 = 3$, Bézout 定理因此表明 $L_1 \subset \gamma_1 \cap \gamma_2$, 与 $\operatorname{card}(\gamma_1 \cap \gamma_2) = 9 < \infty$ 矛盾. 同理可以证明没有 7 个 $\mathcal{A}$ 中的点在同一条二次曲线上.

Step 2 我们来说明 5 个 $\mathcal{A}$ 中的点就可以确定唯一的一条二次曲线. 不妨设 $A_i = (x_i, y_i), 1 \leqslant i \leqslant 5$ 在二次曲线 $ax^2 + bxy + cy^2 + dx + ey + f = 0$ 上, 因此有线性方程组

$$x_i^2 a + x_i y_i b + y_i^2 c + x_i d + y_i e + f = 0 \quad (1 \leqslant i \leqslant 5).$$

这个线性方程组显然有解, 符合要求的二次曲线存在. 假设 Q, Q' 是两条都通过 $A_1, \cdots, A_5$ 的二次曲线, Bézout 定理表明这两条二次曲线一定至少有一条公共线. 但我们已经知道没有 4 个 $\mathcal{A}$ 中的点共线, 所以公共线上至多包含 3 个点, 而余下的 2 个点完全确定了二次曲线的另一分支, 所以 $Q = Q'$.

Step 3 我们来证明 $\mathcal{A}'$ 中没有 3 点共线. 不妨设 A_1, A_2, A_3 在同一条直线 L_2 上, 那么 $A_4, \cdots, A_8$ 确定一条二次曲线 Q_2. 在 L_2 上找到和给定三个点不同的另一个点 B, 在 $\mathbb{A}^2(k)$ 上找到既不在 L_2 也不在 Q_2 上的点 C. 那么, 类比上述二次曲线存在性证明, 我们可以找到一个线性组合 $\alpha = af + bg + ch (a, b, c \in k)$ 使得 $B, C \in Z_\alpha(k)$. 但注意到 $\mathcal{A}' \subset Z_\alpha(k)$, $\operatorname{card}(L_2 \cap Z_\alpha(k)) = 4 >$

$\deg(L_2)\deg(\alpha_k) = 3$, 所以 Bézout 定理表明直线 $L_2 \subset Z_\alpha(k)$. 记 $\mathcal{R}$ 是 $Z_\alpha(k)$ 在 L_2 外的分支, 则易见 $\mathrm{card}(\mathcal{R} \cap Q_2) \geqslant \mathrm{card}(\{A_4, \cdots, A_8\}) = 5 > \deg(\mathcal{R})\deg(Q_2) = 4$, 所以 $Z_\alpha(k) = L_2 \cup Q_2$, 但 $C \notin Z_\alpha(k)$, 矛盾.

同理可以证明 $\mathcal{A}'$ 中没有 6 个点在同一条二次曲线上. 不妨设 $A_1, \cdots, A_6$ 在同一条二次曲线 Q_3 上, 那么 A_7, A_8 确定了一条直线 L_3. 再找到 Q_3 上异于给定两点的新点 B, 不在 Q_3 和 L_3 上的一点 C, 重复以上线性组合方法的说明, 由 $7 > \deg(Z_\alpha(k))\deg(Q_3) = 6$ 知 $Q_3 \subset Z_\alpha(k)$, 而且 $2 > \deg(Z_\alpha(k) \setminus Q_3)\deg(L_3) = 1$ 表明 $Z_\alpha(k) = Q_3 \cup L_3$, 易知矛盾.

Step 4 记通过 $A_1, \cdots, A_5$ 的二次曲线为 Q, 通过 A_6, A_7 的直线为 $\mathcal{L}$, 上述讨论说明 $Q \cap \mathcal{L} \cap \mathcal{A}' = \varnothing, A_8 \notin Q \cup \mathcal{L}$. 再找二次曲线上异于给定点的新点 B, C, 构造 f, g, h 的线性组合 α 使得 $B, C \in Z_\alpha(k)$. 完全重复上述说明自然有 $Z_\alpha(k) = \mathcal{L} \cup Q$ 但 $A_8 \notin \mathcal{L} \cup Q$, 矛盾.

□

我们来证明椭圆曲线上的群结构.

定理 2.4： 设 C 是 $\mathbb{P}^2(k)$ 上的一条椭圆曲线, $O = [0, 1, 0]$. 那么, C 在给定运算 $(\mathscr{A})$ 下形成一个以 O 为零元素的 Abel 群.

证明： 根据上文讨论, 我们这里只需证明 $(\mathscr{A})$ 满足结合律. 我们记 $P * Q$ 是过 P, Q 的直线交 C 的第三个点, 易见 $P * Q = Q * P$, 而且 $(P * Q) * O = P + Q$, $(P + Q) * O = P * Q$. 任取 $P, Q, R \in C$, 为证明 $(P + Q) + R = P + (Q + R)$, 我们因此只需证明 $(P + Q) * R = P * (Q + R)$.

Case 1 我们先考查 $O, P, Q, R, P * Q, P + Q, Q * R, Q + R$ 互不相同的情况. 做过以下点的直线:

$$l_1 : P, Q, P * Q, \quad l_2 : O, Q * R, Q + R, \quad l_3 : P + Q, R, (P + Q) * R;$$
$$l_1' : Q, R, Q * R, \quad l_2' : O, P * Q, P + Q, \quad l_3' : P, Q + R, P * (Q + R).$$

同时, 设 S 是 l_3, l_3' 的交点. 易见这些点都在 C 内. 记 $F_i, G_i \in k[x, y, z]_1 (1 \leqslant i \leqslant 3)$ 使得 $l_i = Z_{F_i}(k) \subset \mathbb{P}^2(k), l_i' = Z_{G_i}(k) \subset \mathbb{P}^2(k)$.

我们考查 C 的方程在 $\mathbb{P}^2(\overline{k})$ 给出的椭圆曲线 $\mathcal{C}$. 记 $\mathcal{F} = F_1F_2F_3, \mathcal{G} = G_1G_2G_3 \in k[x, y, z]_3$, 易见 $Z_{\mathcal{F}}(\overline{k}), Z_{\mathcal{G}}(\overline{k})$ 是 $\mathbb{P}^2(\overline{k})$ 上的两条三次曲线, 而且 $O, P, Q, R, P * Q, P + Q, Q * R, Q + R, T \in Z_{\mathcal{F}}(\overline{k}) \cap Z_{\mathcal{G}}(\overline{k})$. 注意到 $\mathcal{C}$ 也是一条三次曲线, 而且 $\mathcal{C}$ 已经通过了 $O, P, Q, R, P * Q, P + Q, Q * R, Q + R$, Cayley-Bacharach 定理表明 $\mathcal{C}$ 通过点 S, 从而说明 $(P + Q) * R = S = P * (Q + R)$.

Case 2 考虑 $O, P, Q, R, P*Q, P+Q, Q*R, Q+R$ 中有两点相同的情况. 比如 $P*Q = O$, 则 $P+Q = O$, 比如 $P*Q = Q+R$. 则有 $P+Q = (P*Q)*O = Q*R$, 因此有 $(P+Q)*R = (Q*R)*R = Q = P*(P*Q) = P*(Q+R)$. 其他情况类比分析即可知结果仍然成立.

或者我们通过微扰的手段或 Zariski 拓扑下的闭包以及椭圆曲线的光滑性也可以得到结论, 具体请参考 [20]定理 4.

□

特别地, 我们考查椭圆曲线限制在 $\mathbb{A}^2(k) \cong U_3 \subset \mathbb{P}^2(k)$ 上的表现. 假设域特征不为 2, 则 $\mathbb{A}^2(k)$ 上椭圆曲线上一个点 $P = (x, y) \in C \subset \mathbb{A}^2(k)$ 的逆是 $(x, -y)$. 为证明这点, 我们只需要注意到 $\mathbb{P}^2(k)$ 上通过 O 点和 $[x, y, 1]$ 点的直线为

$$\left\{[\mu x, \lambda + \mu y, \mu] | [\lambda, \mu] \in \mathbb{P}^1(k)\right\}.$$

注意到这条直线限制在 $\mathbb{A}^2(k) \cong U_3 \subset \mathbb{P}^2(k)$ 中是一条与 y 轴平行的直线. 因此在 $\operatorname{char} k \neq 2$ 的情况下, 考查 Weierstrass 简化标准型式(2.3), 自然有 $-P = O*P = (x, -y)$.

在 $\operatorname{char} k = 2$ 的情况下, 我们将直线和一般 Weierstrass 形式联立得到

$$\mu(\lambda + \mu y)^2 + a_1\mu^2 x(\lambda + \mu y) + a_3\mu^2(\lambda + \mu y) = \mu^3(x^3 + a_2x^2 + a_4x + a_6).$$

不妨假设 $\mu \neq 0$ 来寻找点 (x, y) 的逆, 否则所求相交点是 $O = [0, 1, 0]$. 记 $\kappa = \frac{\lambda}{\mu}$, 则方程转化为

$$\kappa(\kappa + 2y + a_1x + a_3) = 0.$$

注意到 $\kappa = 0$ 给出 $\lambda = 0$, 所得相交点是 $[x, y, 1]$, 所以另一个相交点应由 $[\lambda, \mu] = [-(2y + a_1x + a_3), 1]$ 给出, 即 (x, y) 的逆是 $(x, -y - a_1x - a_3)$.

2.2 椭圆曲线的自同态环

在建立椭圆曲线的基本模型之后, 我们来考虑椭圆曲线之间的映射, 特别是从一条椭圆曲线到自己的映射. 为讨论方便, 我们考查椭圆曲线限制在 $\mathbb{A}^2(k) \cong U_3 \subset \mathbb{P}^2(k)$ 上的表现, 并记 $O = [0, 1, 0]$ 为椭圆曲线所配 Abel 群的零元素. 在所关心的 $\mathbb{A}^2(k)$ 中, 它表现为一个 “无穷远点”. 以后涉及 O 点的问题, 我们都可以考虑将我们定义的在 $\mathbb{A}^2(k)$ 上的操作以 ι_3 映射的方式自然嵌入到 $\mathbb{P}^2(k)$ 中, 然后延伸定义到 O 点上. 为讨论方便, 下文不再重复. 以下都用 $C(k)$ 或简写作 C 表示域 $k = \mathbb{F}_q$ 上的一条椭圆曲线并带有上文所表明的群结构.

2.2.1 椭圆曲线的自同态的定义

通过函数表达式的定义 我们先给出一个简单清楚的自同态的定义, 这不涉及过多的代数几何语言, 请参考 [21]章 2.9. 但为方便起见, 我们只对 $\operatorname{char} k \neq 2,3$ 的情况讨论.

定义 2.3： 椭圆曲线 C 上的一个**自同态**是一个由有理函数给出的群同态 $\alpha : C(\overline{k}) \to C(\overline{k})$.

更清楚地说, 它满足以下条件:

1. 存在 $R_1(x,y), R_2(x,y) \in \overline{k}(x,y)$ 使得

$$\alpha(x,y) = (R_1(x,y), R_2(x,y)), \quad \alpha(O) = O.$$

2. 对于任意 $P_1 = (x_1,y_1), P_2 = (x_2,y_2) \in C(\overline{k})$ 都有 $\alpha(P_1+P_2) = \alpha(P_1)+\alpha(P_2)$.

这里, 我们只考查那些使得 R_1, R_2 都良定义的点 (x,y), 我们将在下文中给出 α 在剩下点上的定义.

考查椭圆曲线上的一个有理函数 $R(x,y) \in \overline{k}[x,y]$, 根据式(2.3), 记 $y^2 = f(x)$, 则我们总可以写作

$$R(x,y) = \frac{p_1(x)+p_2(x)y}{p_3(x)+p_4(x)y} = \frac{(p_1(x)+p_2(x)y)(p_3(x)-p_4(x)y)}{(p_3(x)+p_4(x)y)(p_3(x)-p_4(x)y)} = \frac{q_1(x)+q_2(x)y}{q_3(x)},$$

其中 $p_1,\cdots,p_4 \in \overline{k}[x]$, $q_1 = p_1p_3 - p_2p_4f, q_2 = p_2p_3 - p_1p_4, q_3 = p_3^2 - p_4^2 f$. 因此, 我们将 $\alpha(x,y)$ 写作

$$\alpha(x,y) = \left(\frac{\varpi_1(x)+\varpi_2(x)y}{\varpi_3(x)}, \frac{\varrho_1(x)+\varrho_2(x)y}{\varrho_3(x)}\right).$$

注意到 $\alpha(x,-y) = (R_1(x,-y), R_2(x,-y)) = -\alpha(x,y) = (R_1(x,y), -R_2(x,y))$, 那么有 $\varpi_2(x) = 0, \varrho_1(x) = 0$, 因此记 $r_1, r_2 \in \overline{k}(x)$ 使得

$$\alpha(x,y) = (r_1(x), r_2(x)y) = \left(\frac{p(x)}{q(x)}, y\frac{s(x)}{t(x)}\right), \tag{2.5}$$

其中 $p,q,s,t \in \overline{k}[x], q,t \neq 0, (p,q) = 1 = (s,t)$. 此时, 我们在那些使得 $q(x) = 0$ 的点 (x,y) 上补定义 α 为:

$$\alpha(x,y) = O, \text{ if } q(x) = 0.$$

我们来证明如果 $t(x) = 0$, 则 $q(x) = 0$, 从而可以将自同态 α 定义在整条椭圆曲线. 我们称由式(2.5)和上述补定义给出的自同态为自同态的**标准型**.

引理 2.1： 设 $\operatorname{char} k \neq 2,3$. 给定 $\mathbb{A}^2(\overline{k})$ 上的一条椭圆曲线 $C(\overline{k})$, 其 Weierstrass 简化标准型为 $y^2 = f(x) = x^3 + ax^2 + bx + c$. 设 $\alpha : C(\overline{k}) \to C(\overline{k})$ 是一个自同态, 形

式是

$$\alpha(x,y)=\left(\frac{p(x)}{q(x)},y\frac{s(x)}{t(x)}\right),$$

其中 $p,q,s,t\in\overline{k}[x],q,t\neq 0,(p,q)=(s,t)=1$.

证明： 考查 $\alpha(x,y)\in C(\overline{k})$, 则有

$$\frac{s^2}{t^2}y^2=\frac{p^3+ap^2q+bpq^2+cq^3}{q^3},$$

记 $u(x)=p(x)^3+ap(x)^2q(x)+bp(x)q(x)^2+cq(x)^3$, 我们有

$$s^2q^3f=ut^2.$$

注意到 $(s,t)=1$, 所以 $t^2\mid q^3f$. 但是注意到 $f(x)$ 无重根, 所以 $t^2\mid q^3$, 因此 $t(x)$ 的根都是 $q(x)$ 的根. □

定义一个装备标准型的自同态

$$\alpha(x,y)=(r_1(x),r_2(x)y)=\left(\frac{p(x)}{q(x)},y\frac{s(x)}{t(x)}\right)$$

的**度**, $\deg\alpha$, 为

$$\deg\alpha=\max\{\deg p(x),\deg q(x)\},$$

如果 α 非平凡; 同时, 为了方便起见, 我们定义 $\deg(0)=0$.

通过同源的定义 在这部分中, 我们用代数几何的语言描述椭圆曲线上的自同态. 我们假设读者熟知代数簇相关内容, 此部分内容的具体细节请查阅 [15]章 1. 对于 k 上的一条椭圆曲线 $C(k)$, 设它由 Weierstrass 标准型 $f(x,y)=0$ 给出, 那么 $C(k)$ 的函数域 $k(C)$ 是环 $k[x,y]/(f)$ 的分式域.

定义 2.4： 设 C,C' 是 k 上的两条椭圆曲线. 我们称一个从 C 到 C' 的 $\overline{k}$ 上的非零态射 $\phi:C\to C'$ 是一个**同源** (isogeny), 如果 $\phi(O)=O$.

我们记从椭圆曲线 (C_1,O_1) 到 (C_2,O_2) 的所有同源形成的群为 $\mathrm{Hom}(C_1,C_2)$. 记从椭圆曲线 (C,O) 到自己的所有同源形成的群为 $\mathrm{End}(C)$, 其中的元素称为椭圆曲线 C 的**自同态**.

我们来说明上述同源的定义等价于 ϕ 是一个保持椭圆曲线 $(C_1,O_1),(C_2,O_2)$ 群结构的非零 $\overline{k}$-有理映射. 注意到 ϕ 诱导了 C_1,C_2 的 Picard 群间的映射 $\phi_*:\mathrm{Pic}^0(C_1)\to\mathrm{Pic}^0(C_2)$, 则考虑将 ϕ 写作复合

$$\phi:C_1\cong\mathrm{Pic}^0(C_1)\xrightarrow{\phi_*}\mathrm{Pic}^0(C_2)\cong C_2,$$

注意到其中映射都是群同态, 因此 ϕ 也是一个群同态, 保持椭圆曲线上的群结构. 这说明 ϕ 给出一个从 C_2 的函数域 $\overline{k}(C_2)$ 到 C_1 的函数域 $\overline{k}(C_1)$ 的嵌入, 我们定义 ϕ 的**度**为相应域扩张的度 $[\overline{k}(C_1) : \overline{k}(C_2)]$.

2.2.2 可分自同态

可分自同态

定义 2.5： 设 k 是一个域, $\operatorname{char} k \neq 2, 3$, C 是一条 k-椭圆曲线, $\alpha \in \operatorname{End}(C)$ 并装备自同态标准型

$$\alpha(x, y) = (r_1(x), r_2(x)y) = \left(\frac{p(x)}{q(x)}, y\frac{s(x)}{t(x)}\right).$$

我们称 α 是一个**可分**自同态, 如果 $r_1'(x) \neq 0$.

注意到这个条件等价于 $p'(x), q'(x)$ 中有一个不恒为 0. 显然, $r_1'(x) = 0$ 等价于 $p'(x)q(x) = p(x)q'(x)$. 易见 $p' = 0, q' = 0$ 自然有 $r_1' = 0$. 反过来, 如果 $r_1' = 0$, 由 $(p, q) = 1$ 知, $p \mid p', q \mid q'$, 显然有 $p' = 0, q' = 0$.

使用更多代数几何背景, 更普遍的定义是:

定义 2.6： 一个支配的 (dominant, 翻译参考 [22][32]) 态射称作**可分**的, 如果它诱导的域扩张是可分扩张.

我们通过自同态的可分性研究自同态的度和核之间的关系. 沿袭传统, 我们先给出一个较为直接的证明方式, 这时需要假设 $\operatorname{char} k \neq 2, 3$.

命题 2.2： 设 $\alpha : C(\overline{k}) \to C(\overline{k})$ 是一个 k 上椭圆曲线 C 的一个非零自同态. 我们有以下两种情况:

1. 如果 α 是可分的, 有

$$\deg \alpha = \operatorname{card} \ker \alpha.$$

2. 如果 α 是不可分的, 则

$$\deg \alpha > \operatorname{card} \ker \alpha.$$

证明： 考查 α 的自同态标准型

$$\alpha(x, y) = (r_1(x), r_2(x)y) = \left(\frac{p(x)}{q(x)}, y\frac{s(x)}{t(x)}\right).$$

如果 α 是可分的, 记 $\mathfrak{S} := \{x \in \overline{k} | (pq' - p'q)(x)q(x) = 0\}$. 由于 $r_1'(x) \neq 0$, $\mathfrak{S}$ 因而是一个有限集. 我们来考查某个特殊点 $(\mu, \nu) \in C(\overline{k})$ 关于 α 的原像中点的个数来表现 $\ker \alpha$ 中点的个数. 我们要求 (μ, ν) 满足以下条件:

- $(\mu, \nu) \in \alpha(C(\overline{k}))$.

- $\mu, \nu \neq 0$ 并且 $(\mu, \nu) \in \mathbb{A}^2(\overline{k})$, 即 $(\mu, \nu) \neq O$.
- $\mu \notin \mathfrak{S}$.
- $\deg(p(x) - \mu q(x)) = \deg \alpha = \max\{\deg p(x), \deg q(x)\}$.

注意到后三个条件事实上只排除了有限多个 μ 的取值, 准确地说, 至多排除了 $\operatorname{card} \mathfrak{S} + 2 < \infty$ 个 μ 的取值, 也即至多排除了 $2 \operatorname{card} \mathfrak{S} + 4$ 个 $\alpha(C(\overline{k}))$ 上的点. 而 $\overline{k}$ 是一个无限域, 所以 $\alpha(C(\overline{k}))$ 上有无限个点, 即满足条件的 (μ, ν) 总是存在的. 注意到由 $r_1(x_1) = \mu, y_1 r_2(x_1) = \nu$, 由于 $\mu, \nu \neq 0$, $y_1 = \frac{\nu}{r_2(x_1)}$ 可以被 x_1 的取值完全确定, 因此 $\operatorname{card} \alpha^{-1}(\mu, \nu) = \operatorname{card} r_1^{-1}(\mu) = \operatorname{card}\{x \in \overline{k} | p(x) - \mu q(x) = 0\}$. 由条件 4, $\deg(p - \mu q) = \deg \alpha$, 因而我们只需证明 $p - \mu q$ 无重根. 不妨假设有重根, 即存在 $x_0 \in \overline{k}$ 使得 $p(x_0) - \mu q(x_0) = 0, p'(x_0) - \mu q'(x_0) = 0$, 得到 $\mu(p'(x_0)q(x_0) - p(x_0)q'(x_0)) = 0$, 由 $\mu \neq 0$ 知 $(p'q - pq')(x_0) = 0$, 从而 $x_0 \in \mathfrak{S}$, 矛盾.

如果 α 不是可分的, 重复上述陈述, 但不要求 $\mu \notin \mathfrak{S}$, 但我们知道 $p'q - pq'$ 一定有重根, 因此 $\deg \alpha > \operatorname{card} \ker \alpha$. □

一个不变的微分形式 我们希望借助一个椭圆曲线上的不变的微分形式来研究倍乘运算 $\chi_m : C(\overline{k}) \to C(\overline{k}) (m \in \mathbb{Z})$ 的度和可分性, 其中 $\chi_m(P) = mP$.

为了方便起见, 我们这里直接给出使用代数几何语言的关于不变微分的结论.

引理 2.2： 设 C 是一条 k 上的椭圆曲线, 其 Weierstrass 标准型为

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

我们定义微分形式

$$\omega = \frac{dx}{2y + a_1 x + a_3} = \frac{dy}{3x^2 + 2a_2 x + a_4 - a_1 y}.$$

那么 ω 在 C 上是一个不恒为 0 的全纯的微分形式, 即 $(\omega) = 0$.

证明： 请参考 [17][48]. □

接下来, 我们考查它的平移不变性.

命题 2.3： 沿以上假设, 对于任意 $Q \in C$, 定义映射 $\tau_Q : C \to C$ 为

$$\tau_Q(P) = P + Q.$$

那么,

$$\tau_Q^* \omega = \omega.$$

证明： 注意到 Ω_C 是 1 维 $\overline{k}(C)$-线性空间, 那么, 存在一个依赖 Q 的函数 $h_Q \in$

$\overline{k}(E)^*$ 使得

$$\tau_Q^*\omega = h_Q\omega.$$

由于 τ_Q 是一个同构, $h_Q \neq 0$. 所以, 我们有

$$(h_Q) = (\tau_Q^*\omega) - (\omega) = \tau_Q^*(\omega) - (\omega) = 0.$$

因此 h_Q 在 C 上恒为常数, 即 $h_Q \in \overline{k}^*$.

那么, 接下来, 我们考查映射 $\varpi : C \to \mathbb{P}^1(\overline{k})$ 为

$$\varpi(Q) = [h_Q, 1].$$

注意到对于任意 $P \in C$, Vieta 定理和隐函数定理总说明 $P + Q$ 的坐标可以表示成为 $x(Q), y(Q)$ 的有理函数的形式, 所以 ϖ 是一个有理函数. 但注意到 ϖ 并不是满射, 因为显然 $[0, 1] \notin \varpi$. 由于 $h_Q \in \overline{k}^*$, 所以 ϖ 是一个常数映射, 而 $h_Q = h_O = 1$, 因为 $\tau_O = \mathrm{id}_C$. □

注释 2.2： 事实上, 更进一步地, 我们知道 ω 是 C 上在常数系数倍乘下唯一一个平移不变的微分形式, 见 [21]^{56}.

我们通过这个微分形式来考查自同态的和的表现, 我们仍然先给出一个基于直接计算的命题.

命题 2.4： 设 k 是一个特征不为 2,3 的域, C 是一条 k 上的椭圆曲线, $\alpha_1, \alpha_2, \alpha_3$ 是 C 的三个非零的自同态, 并有 $\alpha_1 + \alpha_2 = \alpha_3$. 我们将自同态们写成相应的标准型

$$\alpha_j(x, y) = (r_j(x), ys_j(x)) \quad (1 \leqslant j \leqslant 3),$$

其中 $r, s \in \overline{k}(x)$. 假设存在常数 c_1, c_2 使得

$$\frac{r_1'(x)}{s_1(x)} = c_1, \quad \frac{r_2'(x)}{s_2(x)} = c_2.$$

那么有

$$\frac{r_3'(x)}{s_3(x)} = c_1 + c_2.$$

证明： 注意到这时我们可以利用椭圆曲线的 Weierstrass 简化标准型

$$y^2 = x^3 + ax^2 + bx + c,$$

将不变微分形式写作

$$\omega = \frac{dx}{2y} = \frac{dy}{3x^2 + 2ax + b}.$$

记 $\alpha_i(x, y) = (x_i, y_i), 1 \leqslant i \leqslant 3$, 那么显然 x_i, y_i 都是 x, y 的有理函数. 由不变微分形

式, 我们知道

$$\frac{dx_3}{2y_3} = \frac{dx_1}{2y_3}\left(\frac{\partial x_3}{\partial x_1} + \frac{\partial x_3}{\partial y_1}\frac{dy_1}{dx_1}\right) = \frac{dx_1}{2y_1}.$$

同理有

$$\frac{\partial x_3}{\partial x_2} + \frac{\partial x_3}{\partial y_2}\frac{dy_2}{dx_2} = \frac{y_3}{y_2}.$$

而假设表明

$$\frac{dx_i}{dx} = c_i\frac{y_i}{y}, \quad i = 1, 2.$$

那么我们有

$$\begin{aligned}\frac{dx_3}{dx} &= \left(\frac{\partial x_3}{\partial x_1} + \frac{\partial x_3}{\partial y_1}\frac{dy_1}{dx_1}\right)\frac{dx_1}{dx} + \left(\frac{\partial x_3}{\partial x_2} + \frac{\partial x_3}{\partial y_2}\frac{dy_2}{dx_2}\right)\frac{dx_2}{dx} \\ &= c_1\frac{y_3}{y_1}\frac{y_1}{y} + c_2\frac{y_3}{y_2}\frac{y_2}{y} \\ &= (c_1 + c_2)\frac{y_3}{y},\end{aligned}$$

这即证明了结论. □

推论 2.1： 设 k 是一个特征不为 2,3 的域, C 是 k 上的一条椭圆曲线, $\chi_m : C(\overline{k}) \to C(\overline{k})(m \in \mathbb{Z})$, 其中 $\chi_m(P) = mP$. 显然, χ_m 是 C 上的自同态, 记 χ_m 的自同态标准型为

$$\chi_m(x, y) = (\mathfrak{r}_m(x), y\mathfrak{s}_m(x)),$$

其中 $\mathfrak{r}_m, \mathfrak{s}_m \in \overline{k}(x)$. 那么, 有

$$\frac{\mathfrak{r}_m(x)'}{\mathfrak{s}_m(x)} = m.$$

因此, $\chi_m(x)$ 在 $\mathbb{F}_{p^n}$ 上的椭圆曲线上是一个可分自同态当且仅当 $p = \operatorname{char}\mathbb{F}_{p^n} \nmid m$.

证明： 注意到 $\mathfrak{r}_{-m}(x) = \mathfrak{r}_m(x), \mathfrak{s}_{-m}(x) = -\mathfrak{s}_m(x)$, 因此

$$\frac{\mathfrak{r}_{-m}(x)'}{\mathfrak{s}_{-m}(x)} = -\frac{\mathfrak{r}_m(x)'}{\mathfrak{s}_m(x)}.$$

从而我们只需要对 $m \in \mathbb{N}$ 的情况证明结论即可. 由上述命题, 注意到 $\chi_m = m\chi_1 = m\,\mathrm{id}$, 而 $\mathfrak{r}_1(x) = x, \mathfrak{s}_1(x) = 1$, 则有

$$\frac{\mathfrak{r}_m'(x)}{\mathfrak{s}_m(x)} = m\frac{\mathfrak{r}_1'(x)}{\mathfrak{s}_1(x)} = m(m \in \mathbb{N}).$$

注意到 χ_m 可分当且仅当 $\mathfrak{r}_m'(x)$ 不恒为 0, 等价于 $\frac{\mathfrak{r}_m'(x)}{\mathfrak{s}_m(x)} = m \not\equiv 0 \mod p$. □

注意到以上内容事实上对于一般的域都是成立的, 而且有更为严格的基于更

多代数几何语言的证明, 囿于篇幅所限, 我们只给出对应的结论, 具体证明请读者参考 [17]$^{77\text{-}78}$.

命题 2.5： 设 C, C' 是两条椭圆曲线, ω 是 C 上的一个不变微分, $\phi, \psi : C \to C'$ 是同源, 那么

$$(\phi + \psi)^* \omega = \phi^* \omega + \psi^* \omega.$$

特别地, 我们也有

$$\chi_m^* \omega = m\omega, (m \in \mathbb{Z})$$

和同样的可分性的判断. 注意到由可分自同态的定义易知, 一个自同态 ϕ 是不可分的当且仅当 $\phi^* \omega = 0$, 其中 ω 是 C 上的不变微分.

2.3 有限域上椭圆曲线的有理点

在这一章, 我们来考虑有限域 $k = \mathbb{F}_q$ 上的椭圆曲线, 其中 $q = p^n$, p 是一个素数, $n \in \mathbb{N}$. 给定 Diophantine 方程

$$F(x, y, z) = 0,$$

其中 $F \in \mathbb{F}_q[x, y, z]_d$, $d \geqslant 1$. 我们称 $\mathbb{P}^2(k)$ 中满足给定方程的解为对应曲线 $C_F(k) := Z_F(k) \subset \mathbb{P}^2(k)$ 上的**有理点**. 注意到 $\mathbb{P}^2(\mathbb{F}_q)$ 上的点总是有限多个, 所以在这部分理论中我们关心的是给定椭圆曲线上有理点的准确个数或估计.

为此, 我们需要先准备一个重要的有限域上椭圆曲线的自同态, Frobenius 映射, 它来自于传统的有限域上的自同态.

2.3.1 Frobenius 映射

定义 2.7： 我们称 $\phi_q : C(\overline{k}) \to C(\overline{k})$ 满足

$$\phi_q(x, y) = (x^q, y^q), \quad \phi_q(O) = O$$

是一个 **Frobenius 映射**.

命题 2.6： 设 $\mathbb{F}_q$ 上的椭圆曲线 C 的 Weierstrass 标准型是

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

其中 $a_i \in \mathbb{F}_q$, 那么, Frobenius 映射 ϕ_q 是 C 上的度为 q 的不可分自同态.

证明： 易见 ϕ_q 是一个 $\mathbb{F}_q$-有理映射, 度是 q. 注意到由于 $a_i \in \mathbb{F}_q$, 所以 $a_i^q = q$, 方

程两侧取 q 次方后有

$$(y^q)^2 + a_1(x^q)(y^q) + a_3(y^q) = (x^q)^3 + a_2(x_q)^2 + a_4(x^q) + a_6,$$

所以 Frobenius 映射 ϕ_q 是从 C 映射到 C 上的. 因此, 我们只需验证 ϕ_q 保持 C 上的群结构. 考查 $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in C(\bar{k})$.

Case 1 设 $x_1 \neq x_2$. 由上文讨论可知 $P_1 + P_2$ 仍是一个有限平面内的点, 记 $P_3 = P_1 + P_2 = (x_3, y_3)$. 设 $y = \lambda x + \nu$ 是通过 P_1, P_2 的直线 L,

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

L 和 C 联立, 由 Vieta 定理可知:

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1.$$

注意到 $y = \lambda^q x + \nu^q$ 是连接 $P_1' = \phi_q(P_1) = (x_1^q, y_1^q), P_2' = \phi_q(P_2) = (x_2^q, y_2^q)$ 的直线 L', 设 $P_3' = P_1' + P_2' = (x_3', y_3')$. 将 L' 和 C 联立, Vieta 定理给出

$$x_3' = (\lambda^q)^2 + a_1(\lambda^q) - a_2 - x_1^q - x_2^q = x_3^q, \quad y_3' = \lambda^q(x_1^q - x_3^q) - y_1^q = y_3^q,$$

所以

$$\phi_q(P_3) = P_3' = \phi_q(P_1) + \phi_q(P_2).$$

Case 2 假设 $x_1 = x_2$. 如果 $P_1 = -P_2$, 则根据上文讨论的取逆公式可知 $\phi_q(P_1) = \phi_q(P_2)$. 如果 $P_1 = P_2$, 设 $2(x_1, y_1) = (x_3, y_3)$, $y = \lambda x + \nu$ 给出 C 在 P 点的切线 L, 隐函数定理给出

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}.$$

重复以上将 C 和 L 联立的过程, 类比得到同样的结论.

设 ω 是 C 上的不变微分, 注意到

$$\phi_q^*(\omega) = \phi_q^*\left(\frac{dx}{2y + a_1x + a_3}\right) = \frac{qx^{q-1}dx}{2y^q + a_1x^q + a_3} = 0,$$

所以 ϕ_q 不是可分的. □

推论 2.2： 设 C 是 $k = \mathbb{F}_q$ 上的一条椭圆曲线, $q = p^n, n \in \mathbb{N}$, p 是一个素数, $r, s \in \mathbb{Z}$ 不全为 0, 那么, 自同态 $r\phi_q + \chi_s$ 是可分的当且仅当 $p \nmid s$. 特别地, $\phi_q - \mathrm{id}$ 是可分的.

证明： 设 ω 是 C 上的不变微分, 由命题2.5知

$$(r\phi_q + \chi_s)^*\omega = r\phi_q^*\omega + s\omega.$$

注意到 ϕ_q 不是可分的, 所以 $\phi_q^*\omega = 0$, 因此 $r\phi_q + \chi_s$ 是可分的当且仅当 $(r\phi_q +$

$\chi_s)^*\omega \neq 0$, 这等价于 $s \not\equiv 0 \mod p$. □

2.3.2 Weil 配对定理

椭圆曲线上的扭群结构 设 C 是 k 上的一条椭圆曲线. 我们关心 $C(\bar{k})$ 上的特定的扭元素组成的群的结构, 定义

$$C_n := \{P \in C(\bar{k}) | nP = O\} \quad (n \in \mathbb{N}).$$

我们指出在 $k = \mathbb{C}$ 时, 著名的 Weierstrass-$\wp$ 函数

$$\wp(z; \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda, \omega \neq 0} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right]$$

给出了 C_n 完全的刻画.

命题 2.7： 设 $\Lambda \in C$ 是一个格, 定义

$$g_2 = 60 \sum_{\omega \in \Lambda, \omega \neq 0} \frac{1}{\omega^4}, \quad g_3 = 140 \sum_{\omega \in \Lambda, \omega \neq 0} \frac{1}{\omega^6}.$$

那么, 由多项式 $f(x) = 4x^3 - g_2 x - g_3$ 给出的曲线

$$y^2 = f(x) = 4x^3 - g_2 x - g_3$$

是一条椭圆曲线. 映射 $\phi : \mathbb{C}/\Lambda \to C(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C})$,

$$\phi(z) = [\wp(z; \Lambda), \wp'(z; \Lambda), 1].$$

是一个复 Lie 群的解析同构.

证明： 请参考 [17]$^{170\text{-}171}$ 或 [21]$^{章\ 9}$ 或 [16]$^{章\ \mathrm{VI}}$. □

更普遍地, 我们有下面这个命题:

命题 2.8： 设 C 是 k 上的一条椭圆曲线, n 是一个正整数. 如果 $\operatorname{char} k \nmid n$ 或者 $\operatorname{char} k = 0$, 那么

$$C_n \simeq \mathbb{Z}/n \oplus \mathbb{Z}/n.$$

证明： 请参考 [21]$^{章\ 3.2}$. □

Weil 配对定理 囿于篇幅所限, 我们给出 Weil 配对定理的陈述, 但不证明这个定理, 请读者参考 [17]$^{章\ \mathrm{III}.8}$ 或 [21]$^{章\ 11}$ 及 [23]$^{章\ 3.7}$.

定理 2.5： 设 C 是 k 上的一条椭圆曲线, n 是一个正整数. 记

$$\mu_n := \{x \in \bar{k} | x^n = 1\}.$$

假设 $\operatorname{char} k \nmid n$, 则存在一个配对 $e_n : C_n \times C_n \to \mu_n$ 满足以下性质: 对于任意 $P_1, P_2, P, Q_1, Q_2, Q \in C_n$ 有:

(a) $e_n(P, P) = 1$.

(b) 双线性: $e_n(P_1 + P_2, Q) = e_n(P_1, Q)e_n(P_2, Q)$,
$e_n(P, Q_1 + Q_2) = e_n(P, Q_1)e_n(P, Q_2)$.

(c) 非退化: 如果对于任意 $Q \in C_n$ 都有 $e_n(P, Q) = 1$, 则 $P = O$.

(d) 对于任意 $\sigma \in \operatorname{Gal}(\overline{k}/k)$, $e_n(\sigma P, \sigma Q) = \sigma(e_n(P, Q))$.

(e) 对于任意 $\alpha \in \operatorname{End}(C)$, $e_n(\alpha(P), \alpha(Q)) = e_n(P, Q)^{\deg \alpha}$.

注释 2.3： 注意到由 (a) 和 (b) 我们知道 e_n 是反对称的, 即对于任意 $P, Q \in C_n$ 有

$$e_n(P, Q) = e_n(Q, P)^{-1}.$$

基于 Weil 配对定理, 我们先给出以下推论. 由命题2.8知道, 在以上假设下, $C_n \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$.

推论 2.3： 设 T_1, T_2 是 C_n 的一组基, 则 $e_n(T_1, T_2)$ 是 μ_n 的生成元.

证明： 记 $\zeta := e_n(T_1, T_2) \in \mu_n$, 设 $\operatorname{ord}(\zeta) = d \leqslant n$, 则 $e_n(dT_1, T_2) = e_n(T_1, T_2)^d = \zeta^d = 1$. 考查任意 C_n 中的任意一个元素 $P = aT_1 + bT_2$, $a, b \in \mathbb{Z}$, 我们有

$$e_n(dT_1, P) = e_n(dT_1, aT_1 + bT_2) = e_n(T_1, T_1)^{ad} e_n(T_1, T_2)^{db} = \zeta^{db} = 1.$$

条件 (c) 因此给出 $dT_1 = O$, 由于 $\operatorname{ord}(T_1) = n$, 我们知道 $\operatorname{ord}(\zeta) = n$, 即有结论. □

2.3.3 Hasse 定理

Hasse 定理给出了有限域上椭圆曲线上有理点个数的最重要的一个估计.

定理 2.6 (Hasse)： 设 C 是有限域 $k = \mathbb{F}_q$ 上的一条椭圆曲线. 我们有以下估计:

$$\left|\operatorname{card} C(\mathbb{F}_q) - (q + 1)\right| \leqslant 2\sqrt{q}. \tag{2.6}$$

准备 我们先来给出 $C(\mathbb{F}_q)$ 中点的刻画. 由有限域上的 Frobenius 映射知识可知 $x \in \mathbb{F}_q$ 当且仅当 $x^q = x$. 那么一个 $C(\overline{\mathbb{F}}_q)$ 上的点 $(x, y) \in C(\mathbb{F}_q)$ 当且仅当 $x, y \in \mathbb{F}_q$, 也即 $\phi_q(x, y) = (x^q, y^q) = (x, y)$, 也即 $C(\mathbb{F}_q) = \ker(\phi_q - \mathrm{id}) \subset C(\overline{\mathbb{F}}_q)$.

由推论2.2知道自同态 $\phi_q - \mathrm{id}$ 是可分的, 再由命题2.2知道 $\operatorname{card} C(\mathbb{F}_q) = \operatorname{card} \ker(\phi_q - \mathrm{id}) = \deg(\phi_q - \mathrm{id})$.

为了完成 Hasse 定理的证明, 我们需要进一步清楚地表述映射 $\phi_q - \mathrm{id}$ 的度, 这即需要使用 Weil 配对定理.

设 C 是域 k 上的一条椭圆曲线, α 是 C 的一个自同态, $n \in \mathbb{N}$ 满足 $\operatorname{char} k \nmid n$.

因此, $C_n \simeq \mathbb{Z}/n \oplus \mathbb{Z}/n$, 我们从而可以选取 $T_1, T_2 \in C_n$ 作为一组基. 注意到 α 将 C_n 中的元素仍映回 C_n 中, 而且由于 α 保持群结构, 所以 α 在 C_n 中的限制在基 $\{T_1, T_2\}$ 下可以通过一个矩阵

$$\alpha_n = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

来表示, 其中 $a, b, c, d \in \mathbb{Z}/n$. 即是说

$$\alpha(xT_1 + yT_2) = \alpha_n \cdot \begin{bmatrix} x \\ y \end{bmatrix} = (ax + by)T_1 + (cx + dy)T_2.$$

命题 2.9： 设 C 是域 k 上的一条椭圆曲线, α 是 C 的一个自同态, $n \in \mathbb{N}$ 满足 $\operatorname{char} k \nmid n$, 则有 $\deg \alpha \equiv \det \alpha_n \mod n$.

证明： 我们记 $e_n(T_1, T_2)$ 为 ζ. 由推论2.3可知 ζ 是 μ_n 的生成元, 所以我们有

$$\begin{aligned} e_n(\alpha(T_1), \alpha(T_2)) &= e_n(aT_1 + cT_2, bT_1 + dT_2) \\ &= e_n(T_1, T_2)^{ad} e_n(T_2, T_1)^{bc} \\ &= e_n(T_1, T_2)^{ad-bc} = \zeta^{\det \alpha_n}. \end{aligned}$$

而注意到 $e_n(\alpha(T_1), \alpha(T_2)) = \zeta^{\deg \alpha}$, 由 $\operatorname{ord}(\zeta) = n$ 即知结论. □

推论 2.4： 沿以上假设, 设 $\alpha, \beta \in \operatorname{End}(C)$, $\lambda, \mu \in \mathbb{Z}$, 那么有

$$\deg(\lambda\alpha + \mu\beta) = \lambda^2 \deg \alpha + \mu^2 \deg \beta + \lambda\mu \left[\deg(\alpha + \beta) - \deg \alpha - \deg \beta\right].$$

证明： 取 $n \in \mathbb{N}$ 使得 $\operatorname{char} k \nmid n$, 设 $\alpha_n, \beta_n \in M_2(\mathbb{Z}/n)$ 分别是 α, β 在 C_n 上作用的表示矩阵. 注意到 $\lambda\alpha_n + \mu\beta_n$ 是 $\lambda\alpha + \mu\beta$ 在 C_n 上作用的表示矩阵.

我们暂时回到线性代数来解决一些问题. 设 $M, N \in M_2(R)$, 其中 R 是一个交换环. 记 N^* 是 N 的伴随矩阵, 我们注意到

$$\operatorname{Tr}(MN^*) = \det(M + N) - \det M - \det N.$$

记 $M = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix}, N = \begin{bmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{bmatrix}$, 直接计算就有

$$\operatorname{Tr}(MN^*) = x_{11}y_{22} - x_{12}y_{21} - x_{21}y_{12} + x_{22}y_{11}.$$

$$\det(M + N) = (x_{11} + y_{11})(x_{22} + y_{22}) - (x_{12} + y_{12})(x_{21} + y_{21}).$$

直接展开即有结论. 基于此, 我们有

$$\det(\lambda M + \mu N) - \lambda^2 \det M - \mu^2 \det N = \operatorname{Tr}((\lambda M)(\mu N)^*) = \lambda\mu \operatorname{Tr}(MN^*)$$

$$= \lambda\mu\left[\det(M+N) - \det M - \det N\right].$$

将 α_n, β_n 分别代入 M, N 即有结论. 这说明

$$\deg(\lambda\alpha + \mu\beta) \equiv \lambda^2 \deg\alpha + \mu^2 \deg\beta + \lambda\mu\left[\deg(\alpha+\beta) - \deg\alpha - \deg\beta\right] \mod n$$

对无限多个 n 成立, 由此可得结论. □

到此, 一切所需要的准备终于都已经全部完成, 我们来证明 Hasse 定理.

Hasse 定理的证明

证明： 上文讨论中得到

$$\operatorname{card} C(\mathbb{F}_q) = \deg(\phi_q - \mathrm{id}).$$

对于任意 $r, s \in \mathbb{Z}$, 由推论2.4知道:

$$\begin{aligned}\deg(r\phi_q - \chi_s) &= r^2 \deg(\phi_q) + s^2 \deg(-\mathrm{id}) + rs\left[\deg(\phi_q - \mathrm{id}) - \deg\phi_q - \deg(-\mathrm{id})\right] \\ &= r^2 q + s^2 + rs\left[\deg(\phi_q - \mathrm{id}) - q - 1\right].\end{aligned}$$

记 $\Phi = \deg(\phi_q - \mathrm{id}) - q - 1$. 特别地, 选取 $s \in \mathbb{Z}$ 使得 $(s, q) = 1$, 则由 $\deg(r\phi_q - \chi_s) \geqslant 0$ 知道

$$q\left(\frac{r}{s}\right)^2 + \Phi\left(\frac{r}{s}\right) + 1 \geqslant 0. \tag{2.7}$$

特别地, 选取 $s_0 \in \mathbb{N}$ 使得 $(s_0, q) = 1$, 则对于任意的 $m \in \mathbb{N}_0$, $(s_0^m, q) = 1$. 由 s_0-进制表示, 可知 $\{\frac{r}{s} | r, s \in \mathbb{Z}, (s, q) = 1\}$ 在 $\mathbb{R}$ 中是稠密的, 所以式(2.7)对任意 $x \in \mathbb{R}$ 都成立. 特别地, 考查判别式有

$$\Phi^2 - 4q \leqslant 0,$$

即证得

$$|\Phi| = \left|\operatorname{card} C(\mathbb{F}_q) - (q+1)\right| \leqslant 2\sqrt{q}.$$

□

第 3 章　线性码

3.1　基本概念

设 p 是一个素数, s 是一个正整数, 记 $q = p^s$, 下文考查有限域 $\mathbb{F}_q = \mathbb{F}_{p^s}$ 和它上的 n 维线性空间 $\mathbb{F}_q^n$. 值得提前指出的是, $\mathbb{F}_q^n$ 事实上作为 $\mathbb{F}_q$-线性空间 (或 $\mathbb{F}_q$-模) 同构于 $\mathbb{F}_{q^n}$. 关于以下内容及相关材料, 请读者参考 [4]章 3, 相关内容的中文翻译参考 [24]章 2.

线性码的概念

定义 3.1： 一个 **(q-进制) 线性码** C 指的是一个 $\mathbb{F}_q^n$ 的线性子空间, 我们称 C 中的一个元素是一个**码字**, n 称为**码字长度** (有时也简称为 "码长"). 我们称 $k = k(C) = \dim_{\mathbb{F}_q}(C)$ 是线性码 C 的**维数**.

我们在线性码上引入度量结构: Hamming 距离.

定义 3.2： 设 $\mathbf{x}, \mathbf{y} \in C$ 是两个码字, 我们定义 $\mathbf{x}$ 和 $\mathbf{y}$ 之间的 **(Hamming) 距离**是

$$d(\mathbf{x}, \mathbf{y}) := \mathrm{card}\{i \in \mathbb{Z} | 1 \leqslant i \leqslant n, x_i \neq y_i\}.$$

我们定义线性码 C 的**最小距离**为

$$d(C) = \begin{cases} \min\{d(\mathbf{x}, \mathbf{y}) | \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\} & \text{if } C \neq \{\mathbf{0}\} \\ +\infty & \text{if } C = \{\mathbf{0}\} \end{cases}.$$

自此, 我们使用 "$[n, k, d; q]$ 码" 来表示一个码长为 n, 维数为 k, 最小距离为 d 的 q-进制线性码. 有时, 在不强调域 $\mathbb{F}_q$ 的情况下, 我们也简写做 "$[n, k, d]$ 码", 也可能在不突出最小距离的情况下简写作 "$[n, k]$ 码".

我们定义一个 $[n, k, d; q]$ 码 C 中的一个码字 $\mathbf{x} = (x_1, x_2, \cdots, x_n)$ 的**重量**为

$$w(\mathbf{x}) := \mathrm{card}\{i \in \mathbb{Z} | 1 \leqslant i \leqslant n, x_i \neq 0\} = d(\mathbf{x}, \mathbf{0}).$$

研究一个码的重量的分布是编码理论中占据重要位置的问题. 我们称

$$\min\{w(\mathbf{x}) | \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\}$$

是线性码 C 的**最小重量**. 由线性易知, 线性码的最小重量即为它的最小距离. 的确, 注意到 $C \subset \mathbb{F}_q^n$ 里的元素是有限的, 所以存在 $\mathbf{x}, \mathbf{y} \in C$ 使得 $d(\mathbf{x}, \mathbf{y}) = d$, 也存在 $\mathbf{z} \in C$ 使得 $w(\mathbf{z}) = \min\{w(\mathbf{x}) | \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\}$. 而注意到 $w(\mathbf{z}) = d(\mathbf{z}, \mathbf{0}) \geqslant d$. 又由于 C

是一个线性子空间, $\mathbf{x}-\mathbf{y}\in C$, 而最小距离 $d=d(\mathbf{x},\mathbf{y})=d(\mathbf{x}-\mathbf{y},\mathbf{0})\geqslant w(\mathbf{z})$, 即证明结论.

注意到对于一个 $[n,k,d]$ 线性码而言, 我们最多可以准确地侦知其中**有** $d-1$ 个错误, 但只有在错误数量不多于 $\left[\frac{d-1}{2}\right]$ 的时候, 我们才能准确地通过接收的结果**复原**出原来的码字, 因此, 我们希望尽可能**增大**一个码的最小距离 d. 然而, 基于现实生活的经济性要求, 我们需要尽可能地**减小**码长 n, **扩大**线性码的维数 k. 这些要求和增大最小距离背道而驰, 编码理论也正是为了解决这样的困难, 找到最好的平衡位置.

线性码的构造 我们通常用矩阵来刻画一个线性码, 最为直接的方式是通过生成矩阵.

定义 3.3: 给定一个 $[n,k,d;q]$ 码 C, 我们称一个矩阵 $G\in M_{k\times n}(\mathbb{F}_q)$ 是 C 的**生成矩阵**, 如果 G 的行向量构成 C 的一组基.

除了生成矩阵之外, 我们也可以把 C 当作某个矩阵的化零空间来研究. 为此, 我们先准备对偶码的概念.

定义 3.4: 给定一个 $[n,k,d;q]$ 码 C, 我们称

$$C^{\perp}:=\left\{\mathbf{x}=(x_i)_{1\leqslant i\leqslant n}\in\mathbb{F}_q^n\middle|\sum_{i=1}^{n}x_iy_i=0\quad\forall\mathbf{y}=(y_i)_{1\leqslant i\leqslant n}\in C\right\}$$

为码 C 的**对偶码**. 我们称码 C 的对偶码的生成矩阵为码 C 的**校验矩阵**, 记作 H.

显然, 一个 $[n,k]$ 码的对偶码是一个 $[n,n-k]$ 码, 因此一个 $[n,k]$ 码的校验矩阵 $H\in M_{(n-k)\times n}(\mathbb{F}_q)$. 按照编码理论中的传统, 我们将一个码字记作一个行向量, 因此 $v\in C$ 的等价条件是 $vH^T=\mathbf{0}$.

我们来研究校验矩阵和最小距离之间的关系.

命题 3.1: 给定一个 $[n,k,d;q]$ 码 C 及其校验矩阵 H. 将 H 作列分划为 $H=(v_1,\cdots,v_n)$, 则有

$$d=\min\left\{l\in\mathbb{Z}|1\leqslant l\leqslant n,\forall\{i_1,\cdots,i_l\}\subset\{1,2,\cdots,n\}\left(v_{i_1},\cdots,v_{i_l}\text{ 线性相关}\right)\right\},\tag{3.1}$$

即 H 的任意 $d-1$ 个列向量都 $\mathbb{F}_q$-线性无关, 而且存在 H 的 d 个列向量 $\mathbb{F}_q$-线性相关.

证明: 假设 H 的列向量中有 l 个线性相关. 为简便起见, 不妨设 $v_1,\cdots,v_l(1\leqslant l\leqslant n)$ 线性相关, 那么存在不全为 0 的 $k_1,\cdots,k_l\in\mathbb{F}_q$ 使得 $k_1v_1+\cdots+k_lv_l=0$, 即

$k_1 v_1^T + \cdots + k_l v_l^T = 0$, 因而

$$(k_1, \cdots, k_l, 0, \cdots, 0)\boldsymbol{H}^T = (k_1, \cdots, k_l, 0, \cdots, 0)\begin{bmatrix} v_1^T \\ \vdots \\ v_l^T \\ \vdots \\ v_n^T \end{bmatrix} = \mathbf{0}.$$

这说明 $(k_1, \cdots, k_l, 0, \cdots, 0)$ 是一个码字. 显然, 我们可以删去 $k_1, \cdots, k_l$ 中为 0 的那些项而不改变剩下向量的线性相关性, 所以不妨设 $k_1, \cdots, k_l$ 都不为 0. 因此, 我们有 $(k_1, \cdots, k_l, 0, \cdots, 0) \in \mathcal{C}$ 且重为 l, 有 $l \geqslant d$, 故 RHS (3.1) $\geqslant d$.

同理, 假设有一个重为 d 的码字 $c = (c_i)_{1 \leqslant i \leqslant n} \in \mathcal{C}$, 设 $c_{i_1}, \cdots, c_{i_d} \neq 0$, 则由同样的推导知道

$$c_{i_1} v_{i_1}^T + \cdots + c_{i_d} v_{i_d}^T = \mathbf{0},$$

即存在 d 个 $\boldsymbol{H}$ 的列向量线性相关, $d \geqslant$ RHS (3.1). □

3.2 基于有限域上直线设计的线性码

考虑有限域 $\boldsymbol{K} = \mathbb{F}_q$ 上的仿射空间 $\mathbb{A}^2(\boldsymbol{K})$ 上的所有 q^2 个点形成的集合 $\mathcal{J}$, 并将其按一定顺序编号为 $\mathcal{J} = \{\boldsymbol{J}_1, \cdots, \boldsymbol{J}_{q^2}\}$. 考虑 $\mathbb{A}^2(\boldsymbol{K})$ 上的所有直线形成的集合 $\mathcal{I}$, 易知 $\operatorname{card} \mathcal{I} = q^2 + q$, 并将其也按一定的顺序编号为 $\mathcal{I} = \left\{\boldsymbol{I}_1, \cdots, \boldsymbol{I}_{q^2+q}\right\}$. 我们定义由 $\mathbb{F}_q$ 上的直线和点形成的关联矩阵 (incidence matrix)$\mathfrak{H}_q \in \boldsymbol{M}_{(q^2+q)\times q^2}\left(\mathbb{F}_2\right)$ 为:

$$\mathfrak{H}_q(i, j) = \begin{cases} 1 & \text{if } \boldsymbol{J}_j \in \boldsymbol{I}_i \\ 0 & \text{if } \boldsymbol{J}_j \notin \boldsymbol{I}_i \end{cases}.$$

记 $\mathfrak{C}_q$ 是由 $\mathfrak{H}_q$ 作为校验矩阵给出的线性码.

[7] 详细研究了这类矩阵的性质. 但同时, 我们注意到基于特征为 2 的有限域 $\mathbb{F}_{2^s}(s \in \mathbb{N})$ 设计的码和基于二符号位的 Reed-Solomon 码构造的低密度奇偶校验码 (RS-LDPC) 是等价的 [13]. 而 [14] 给出了一个清楚的如何将 RS-LDPC 的校验矩阵转化成分块循环阵, 并由此计算其秩的方案. 结合这两份资料, 我们陈述一个命题. 我们用 $\rho\left(\mathfrak{H}_q\right)$ 来表示矩阵 $\mathfrak{H}_q$ 作为 $\mathbb{F}_2$ 上矩阵的秩.

命题 3.2: 设 $s \in \mathbb{N}$ 是一个正整数, 矩阵 $\mathfrak{H}_{2^s}$ 是由有限域 $\mathbb{F}_{2^s}$ 的仿射平面 $\mathbb{A}^2\left(\mathbb{F}_{2^s}\right)$

上的点和直线族基于以上方案给出的 $\boldsymbol{M}_{(q^2+q)\times q^2}\left(\mathbb{F}_2\right)$ 中的矩阵, 则它的秩是

$$\rho\left(\mathfrak{H}_{2^s}\right)=3^s.$$

一个相对比较显然的推论如下.

推论 3.1： 设 s 是一个正整数, 记 $\mathfrak{R}_{2^s}$ 是有限域 $\mathbb{F}_{2^s}$ 的仿射平面 $\mathbb{A}^2\left(\mathbb{F}_{2^s}\right)$ 中去除原点和 $\mathbb{A}^2\left(\mathbb{F}_{2^s}\right)$ 的直线族中过原点的直线之后, 按上述规则形成的关联矩阵. 注意到 $\mathfrak{R}_{2^s}$ 是 $\mathfrak{H}_{2^s}$ 的子矩阵. 它的秩是

$$\rho\left(\mathfrak{R}_{2^s}\right)=3^s-1. \tag{3.2}$$

证明： 请参考 [14]. □

第 4 章　基于有限域上椭圆曲线设计的编码

在本章中, 我们将给出我们的核心课题: 基于椭圆曲线构造校验矩阵, 并由此校验矩阵构造一类线性码以研究它的性质. 具体细节请读者参考 [12]. 设 p 是一个素数, $s \in \mathbb{N}$, 记 $q = p^s$. 为了区分, 我们现在记 $K = \mathbb{F}_q$ 为一个有限域.

4.1　码的构造

根据节2.1.3中的讨论, 我们分为三类情况讨论.

Case 1　$\operatorname{char} K > 3$. 此时椭圆曲线的 Weierstrass 标准型是

$$C : y^2 = x^3 + ax + b,$$

一个点 $P = (x, y) \in C$ 的逆是 $-P = (x, -y)$. 考虑 $\mathbb{F}_q^2$ 上的等价关系 $P = (x_1, y_1) \sim Q = (x_2, y_2)$ 如果 $x_1 = x_2$, $y_1 = y_2$ 或 $y_1 = -y_2$. 记 $\mathbb{F}_q^2$ 在这个等价关系下的等价类的总体为 $\mathcal{N}$, 注意到对于任意 $P \in \mathbb{F}_q^2$, 如果 $P \in C, P \sim Q$, 那么 $Q \in C$. 所以对于任意 $\beta \in \mathcal{N}$, 我们称 $\beta \in C$, 如果存在 $P \in \beta$ 使得 $P \in C$.

注意到此时椭圆曲线 C 非奇异的条件是

$$\Delta = -16(4a^3 + 27b^2) \neq 0. \tag{4.1}$$

记 $\mathcal{M} \subset \mathbb{F}_q^2$ 包含所有满足条件(4.1)的参数对 (a, b), 即由参数 a, b 决定的曲线 $y^2 = x^3 + ax + b$ 是一条椭圆曲线.

注意到 $\mathcal{M}, \mathcal{N}$ 都是有限集, 记 $M = \operatorname{card} \mathcal{M}, N = \operatorname{card} \mathcal{N}$, 并将他们分别编号作 $\mathcal{M} = \{\alpha_1, \cdots, \alpha_M\}, \mathcal{N} = \{\beta_1, \cdots, \beta_N\}$, 其中 $\alpha_i (1 \leqslant i \leqslant M)$ 标记一个满足(4.1)的参数对 (a, b). 记由参数对 α_i 给出的椭圆曲线为 C_i. 则定义校验矩阵 $H_q = (H_q(i, j))_{1 \leqslant i \leqslant M, 1 \leqslant j \leqslant N} \in M_{M \times N}(\mathbb{F}_2)$ 为:

$$H_q(i, j) = \begin{cases} 1 & \text{if } \beta_j \in C_i \\ 0 & \text{if } \beta_j \notin C_i \end{cases}.$$

由此校验矩阵定义一个线性码, 我们记这个线性码为 C_q.

Case 2　$\operatorname{char} K = 3$. 此时椭圆曲线的 Weierstrass 标准型有两种

$$C_1 : y^2 = x^3 + ax + b, \quad C_2 : y^2 = x^3 + ax^2 + b.$$

但无论哪种标准型, 一个点 $P=(x,y)\in C$ 的逆都是 $-P=(x,-y)$. 我们这里只考虑第一种标准型, 即

$$C:\ y^2=x^3+ax+b.$$

重复上述讨论, 这时只需注意椭圆曲线 C 非奇异的条件由式(4.1)变为

$$\Delta=2a^3\neq 0. \tag{4.2}$$

相应地, 改记 $\mathcal{M}\subset\mathbb{F}_q^2$ 是所有满足条件(4.2)的参数对 (a,b), 其余定义校验矩阵的操作与 $\mathrm{char}\,K>3$ 时的讨论完全一致.

Case 3 $\mathrm{char}\,K=2$. 此时椭圆曲线的 Weierstrass 标准型有两种

$$C_1:\ y^2+xy=x^3+ax+b,\quad C_2:\ y^2+cy=x^3+ax+b.$$

我们只考虑只带两个参数的第一种标准型, 即

$$C:\ y^2+xy=x^3+ax+b.$$

这时椭圆曲线 C 非奇异的条件是

$$\Delta=b\neq 0. \tag{4.3}$$

一个点 $P=(x,y)\in C$ 的逆变为 $-P=(x,x+y)$. 所以根据这两个条件相应重新定义相关的 $\mathcal{M},\mathcal{N}$, 并沿上述流程生成校验矩阵 H_q. 但此时, 我们注意到原点 $(0,0)$ 不在我们选取的这一族椭圆曲线中的任意一条上. 所以, 我们删去 $(0,0)$ 所在的等价类规定的一列.

我们统一记在 $K=\mathbb{F}_q$ 中沿以上讨论方式生成的校验矩阵为 H_q, 由 H_q 定义的线性码为 C_q.

4.2 校验矩阵 H_q 的分析

本节给出校验矩阵的一些性质, 如尺寸, 围长 (girth) 和密度等.

4.2.1 校验矩阵的尺寸

本小节分析校验矩阵 H_q 的行数和列数.

校验矩阵的行数 我们仍旧按照 $\mathrm{char}\,K$ 的不同情况来分析.

Case 1 $\mathrm{char}\,K>3$. 此时我们来计算满足

$$\Delta(a,b)=-16(4a^3+27b^2)=0$$

的参数对 (a,b) 的个数.

如果 $a=0$, 则 $\Delta=0$ 表明 $b=0$.

如果 $a\neq 0$, 则 $\Delta=0$ 表明

$$b^2=-\frac{4a^3}{27}=\frac{4a^2}{9}\left(-\frac{a}{3}\right),$$

即 $-\frac{a}{3}$ 是一个二次剩余. 考查映射 $\chi_2:\mathbb{F}_q\to\mathbb{F}_q$ 定义为 $\chi_2(x)=x^2$. 注意到 $\mathbb{F}_q^*$ 是一个循环群, 而且 $\operatorname{card}\mathbb{F}_q^*=q-1=p^s-1$ 是偶数. 设 $\zeta\in\mathbb{F}_q^*$ 是 $\mathbb{F}_q^*$ 的生成元, 则有 $1=\zeta^{p^s-1}=\left(\zeta^{\frac{p^s-1}{2}}\right)^2$, 而 $\zeta^{\frac{p^s-1}{2}}\neq 1$. 所以, $\operatorname{card}\ker\chi_2=2$. 这说明

$$\operatorname{card}\operatorname{Im}\chi_2=\frac{1}{2}\operatorname{card}\mathbb{F}_q^*=\frac{p^s-1}{2}.$$

而对于每个 $a\neq 0$ 且 $-\frac{a}{3}$ 是一个二次剩余的情况, 都有 2 个满足条件的 b 使得 $\Delta(a,b)=0$, 所以共有

$$1+2\times\frac{p^s-1}{2}=p^n=q$$

个参数对 (a,b) 使得 $\Delta(a,b)=0$, 则

$$M=\operatorname{card}\mathcal{M}=q^2-q=q(q-1)=p^s(p^s-1).$$

Case 2 $\operatorname{char}K=2$ 或 $\operatorname{char}K=3$. 注意到前者只要求 $a\neq 0$, 后者只要求 $b\neq 0$, 所以自然有

$$M=\operatorname{card}\mathcal{M}=q(q-1)=p^s(p^s-1)$$

对 (a,b) 符合要求.

我们由此证明了校验矩阵 H_q 的行数一定是 $q(q-1)$.

校验矩阵的列数

Case 1 $\operatorname{char}K\geqslant 3$. 注意到此时等价关系都是由 $(x,y)\sim(x,-y)$ 给定的, 因此一个等价类 $\alpha\in\mathcal{M}$ 中只含一个元素当且仅当 $y=0$, 而这样的等价类共有 q 个, 其余等价类内每个都包含 2 个点, 因此我们有

$$N=\operatorname{card}\mathcal{N}=q+\frac{q^2-q}{2}=\frac{q(q+1)}{2}=\frac{p^s(p^s+1)}{2}.$$

Case 2 $\operatorname{char}K=2$. 我们选取的椭圆曲线族规定的等价关系是 $(x,y)\sim(x,x+y)$, 所以一个等价类 $\alpha\in\mathcal{M}$ 中只含一个元素当且仅当 $x=0$. 重复以上说明并注

意 $(0,0)$ 所在等价类被排除, 我们即得到

$$N = \operatorname{card} \mathcal{N} = (q-1) + \frac{q^2-q}{2} = \frac{(q+2)(q-1)}{2} = (2^{s-1}+1)(2^s-1).$$

4.2.2 校验矩阵的围长

我们给出围长 (girth) 的定义, 为此, 我们先准备 Tanner 图的概念, 具体内容请参考 [25].

定义 4.1： 设 C 是一个线性码, $H \in M_{m\times n}(\mathbb{F}_2)$ 是 C 的校验矩阵. 一张无向二部分图 (bipartite graph)G 被称为是 C 对应的 **Tanner 图**, 如果 G 的邻接矩阵 (adjacency matrix) 是 C 的校验矩阵 H.

为了辅助说明, 我们举一个具体的例子. 这是一个 “玩具车例子”(toy example).

例 4.1： 考虑矩阵 $H \in M_{2\times 4}(\mathbb{F}_2)$

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}.$$

设 C 是由 H 作为校验矩阵定义出的线性码, 它对应的 Tanner 图如图4.1所示.

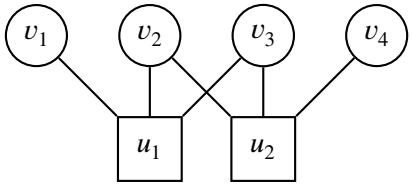

图 4.1　线性码 C 对应的 Tanner 图

基于 Tanner 图, 我们定义一个矩阵的围长.

定义 4.2： 给定一个矩阵 H, 以及对应的 Tanner 图 G, 我们称 G 中最短的环路的长度为矩阵 H 的**围长**.

注意到这一概念和图论中已有的一个图的围长的定义, 即这张图中最短环路的长度 [26][8] 是一致的.

例 4.2： 沿例4.1, 我们来分析它所给出的矩阵 H 的围长. 注意到图4.1中只有一条环路: $v_2 - u_1 - v_3 - u_2 - v_2$, 所以 C 的围长是 4.

注意到一张二部分图的环的长度总是偶数. 记 $G = (V, E)$ 是一张二部分图, 设 $A, B \subset V$ 使得 $V = A \cup B$ 而且每条边的端点都有一个属于 A 而另一个属于 B. 那么, 如果 $\sigma : v_1 - v_2 - v_3 - \cdots - v_l = v_1$ 是一个环路, 不妨设 $v_1 \in A$, 那么显然有 $v_{2k-1} \in A$, $v_{2k} \in B$, $1 \leqslant k \leqslant \frac{l}{2}, k \in \mathbb{Z}$. 特别地, 由 $v_l = v_1 \in A$ 知 l 是一个奇数, 由此知 σ 共有偶数条边. 更进一步地, 我们有下面这个命题.

命题 4.1： 一张图是一张二部分图当且仅当它的所有环路的长度是偶数.

证明： 请参考 [26][17-18]. □

让我们回到对基于椭圆曲线设计的码的校验矩阵的分析.

命题 4.2： 设 H_q 是由4.1节给出的通过 $\mathbb{F}_q$ 上椭圆曲线构造的 $M_{M\times N}(\mathbb{F}_2)$ 中的矩阵, 则由它作为校验矩阵定义的线性码 C_q 的围长大于等于 6.

证明： 一个直接的观察是由 H_q 定义的二部分图 G_q 中两个顶点间至多有一条边相连, 因此 H_q 的围长大于 2, 而命题4.1表明围长因此至少是 4, 我们只需证明 G_q 中没有长度为 4 的环路. 注意到围长是 4 的环路对应邻接矩阵 H_q 中形如 $\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}$ 的子矩阵, 我们只需证明 H_q 中没有这样的子矩阵, 也即两个不同的等价类 $\beta_1, \beta_2 \in \mathcal{N}$ 不可能同时在两条不同的椭圆曲线上.

设 $P_1 = (x_1, y_1) \in \beta_1, P_2 = (x_2, y_2) \in \beta_2$. 我们依旧分情况讨论什么样的参数对确定的椭圆曲线同时包含这两个点.

Case 1 $\operatorname{char} K \geqslant 3$. 此时我们考虑的椭圆曲线类的标准型是

$$y^2 = x^3 + ax + b.$$

因此, 同时包括 P_1, P_2 的椭圆曲线满足方程

$$\begin{cases} ax_1 + b = y_1^2 - x_1^3 \\ ax_2 + b = y_2^2 - x_2^3 \end{cases}$$

如果 $x_1 \neq x_2$, 线性方程组基本知识表明满足条件的参数对 (a, b) 至多只有一个.

如果 $x_1 = x_2$, 注意到方程给出 $y_1^2 = y_2^2$, 因此 $y_1 = y_2$ 或 $y_1 = -y_2$, 即 $P_1 = P_2$ 或 $P_1 = -P_2$, 这和 $\beta_1 \neq \beta_2$ 矛盾.

Case 2 $\operatorname{char} K = 2$. 此时我们考虑的椭圆曲线类的标准型是

$$y^2 + xy = x^3 + ax + b.$$

因此, 同时包括 P_1, P_2 的椭圆曲线满足方程

$$\begin{cases} ax_1 + b = y_1^2 + x_1y_1 + x_1^3 \\ ax_2 + b = y_2^2 + x_2y_2 + x_2^3 \end{cases}$$

如果 $x_1 \neq x_2$, 满足条件的参数对 (a, b) 仍至多只有一个.

如果 $x_1 = x_2$, 方程表明 $(y_1+y_2)(x_1+y_1+y_2) = 0$, 得到 $y_1 = y_2$ 或 $y_2 = x_1+y_1$, 即 $P_1 = P_2$ 或 $P_1 = -P_2$.

两种情形下都表明包含 β_1, β_2 的椭圆曲线至多只有一个. □

4.2.3 校验矩阵的密度

这一节来研究校验矩阵 H_q 的行重和列重.

校验矩阵的行重 注意到行重即是 $\mathbb{F}_q$ 上我们关注的 $\mathbb{A}^2(K)$ 上椭圆曲线上所含等价类的个数. Hasse 定理表明 $\mathbb{F}_q$ 上每条椭圆曲线 $C(\mathbb{F}_q) \subset \mathbb{P}^2(K)$ 所含有理点的个数 $\operatorname{card} C(\mathbb{F}_q)$ 满足估计式(2.6), 因此我们只需关注这些点在哪些等价类中. 记 $C_1 = \{\alpha \in \mathcal{M} | \operatorname{card} \alpha = 1\}, C_2 = \mathcal{M} \setminus C_1$. 记 $w_r(H_q; i)(1 \leqslant i \leqslant M)$ 为校验矩阵 H_q 第 i 行的行重, 有时为突出参数, 我们也记作 $w_r(H_q; a_i, b_i)$, 其中 (a_i, b_i) 是对应 H_q 第 i 行的参数对. 我们有以下命题.

命题 4.3： 对于任意 $1 \leqslant i \leqslant M(H_q)$ 成立估计式

$$\begin{cases} \frac{1}{2}(p^s - 1) - p^{\frac{s}{2}} \leqslant w_r(H_q; i) \leqslant \frac{1}{2}(p^s + 2) + p^{\frac{s}{2}} & \text{if } q = p^s, p \neq 2 \\ 2^{s-1} - 2^{\frac{s}{2}} \leqslant w_r(H_q; i) \leqslant 2^{s-1} + 2^{\frac{s}{2}} & \text{if } q = 2^s \end{cases}.$$

证明： 我们仍分情况来分析.

Case 1 $\operatorname{char} K \geqslant 3$. 注意到此时 $P = -P$ 等价于 $y = 0$, 而方程 $y^2 = x^3 + ax + b$ 给出

$$0 \leqslant \operatorname{card} C_1 \leqslant 3.$$

而

$$q - 2\sqrt{q} \leqslant \operatorname{card} C_1 + 2 \operatorname{card} C_2 \leqslant q + 2\sqrt{q}.$$

注意到此时我们需要去掉 $O = [0, 1, 0]$. 联立即有

$$\frac{q-1}{2} - \sqrt{q} \leqslant \operatorname{card} C_1 + \operatorname{card} C_2 \leqslant \frac{q+2}{2} + \sqrt{q}.$$

Case 2 $\operatorname{char} K = 2$. 注意到此时 $P = -P$ 等价于 $x = 0$, 而方程 $y^2 + xy = x^3 + ax + b$ 给出 $y^2 = b \neq 0$. 注意到映射 $\chi_2 : \mathbb{F}_q^* \to \mathbb{F}_q^*$, 其中 $\chi_2(x) = x^2$, 但 $\operatorname{card} \mathbb{F}_q^* = q - 1 = 2^s - 1$, 所以 $\ker \chi_2$ 是平凡的, 而 $\operatorname{Im} \chi_2 = \mathbb{F}_q^*$, 所以

$$\operatorname{card} C_1 = 1.$$

而

$$q - 2\sqrt{q} \leqslant \operatorname{card} C_1 + 2 \operatorname{card} C_2 \leqslant q + 2\sqrt{q}.$$

联立即有

$$\frac{q}{2}-\sqrt{q}\leqslant \operatorname{card} C_1+\operatorname{card} C_2\leqslant \frac{q}{2}+\sqrt{q}.$$

□

推论 4.1： 考虑有限域 $K=\mathbb{F}_q$, 假设 $q\geqslant 12$, 则 K 上的每条椭圆曲线都至少包含 2 个不同的等价类.

这只需要我们注意到 $\frac{q-1}{2}-\sqrt{q}\geqslant 2$ 的解是 $q\geqslant 7+2\sqrt{6}\approx 11.90$, 而 $\frac{q}{2}-\sqrt{q}\geqslant 2$ 的解是 $q\geqslant 2(3+\sqrt{5})\approx 10.47$.

校验矩阵的列重 这一小节需要我们在 $q\geqslant 12$ 的条件下讨论问题. 这一假设是保证不同的参数对 (a,b) 一定能给出不同的椭圆曲线. 的确, 考查 $(a,b)\neq(a',b')$ 但 $(a,b),(a',b')\in\mathcal{M}$, 注意到 $C(a,b)$ 和 $C(a',b')$ 都分别至少包含 2 个等价类, 但这 2 个等价类不可能同时都在 2 条不同的椭圆曲线上, 否则与围长大于等于 6 的条件矛盾, 即说明它们给出不同的椭圆曲线.

注意到列重即是对应等价类所在的椭圆曲线的个数. 记 $w_c(H_q;j)(1\leqslant j\leqslant N)$ 为校验矩阵 H_q 第 j 列的列重, 有时为突出点或等价类, 我们也记作 $w_r(H_q;P)$ 或 $w_r(H_q;\alpha_j)$. 我们仍按照情况分析. 设 $P_0=(x_0,y_0)\in\alpha_0\in\mathcal{N}$.

Case 1 $\operatorname{char} K>3$. 如果 $P_0\in C(a,b)$, 则有

$$b=y_0^2-x_0^3-ax_0. \tag{4.4}$$

注意到共有 $\mathbb{F}_q^2$ 中 q 对 (a,b) 满足式(4.4), 我们因此只需去除奇异条件下的参数对. 注意到奇异条件是

$$\Delta=4a^3+27b^2=0.$$

与式(4.4)联立有

$$4a^3+27x_0^2a^2+54x_0(x_0^3-y_0^2)a+27(x_0^3-y_0^2)^2=0.$$

注意到此方程最多有 3 个解, 即最多有 3 对 (a,b) 给出奇异的三次曲线, 所以

$$q-3=p^s-3\leqslant w_c(H_q;P_0)\leqslant q=p^s.$$

Case 2 $\operatorname{char} K=3$. 同理共有 $\mathbb{F}_q^2$ 中 q 对 (a,b) 满足式(4.4), 但此时奇异条件是

$$\Delta=2a^3=0.$$

因此有且只有 1 对给出奇异, 所以

$$w_c(H_q; P_0) = q - 1 = p^s - 1.$$

Case 3 $\operatorname{char} K = 2$. 此时 $P_0 \in C(a, b)$ 给出

$$b = y_0^2 + x_0 y_0 + x_0^3 + a x_0. \tag{4.5}$$

此时仍有 q 对满足式(4.5). 但非奇异条件是

$$\Delta = b \neq 0. \tag{4.6}$$

如果 $x_0 \neq 0$, 式(4.6)给出

$$a \neq \frac{y_0^2 + x_0 y_0 + x_0^3}{x_0},$$

由此只排除 1 对. 但如果 $x_0 = 0$, $b = y_0^2 \neq 0$, 由于 $(0,0)$ 已经被排除, 所以所有符合式(4.5)的参数对 (a, b) 都被保留. 即有

$$w_c(H_q; x_0, y_0) = \begin{cases} q - 1 = 2^s - 1 & \text{if } x_0 \neq 0 \\ q = 2^s & \text{if } x_0 = 0 \end{cases}. \tag{4.7}$$

4.3 关于线性码 C_q 的一些数值计算和猜想

以上我们陈述了一些关于校验矩阵 H_q 已知的一些特性的分析, 下面我们来陈述一些计算结果和猜想.

4.3.1 H_p 的秩

设 p 是一个素数, 考虑在 $\mathbb{F}_p$ 的情况下构造的校验矩阵 H_p. 在 $p = 2$ 时, 非奇异的条件是 $b \neq 0$, 共有 2 个参数对符合条件: $\alpha_1 = (0,1), \alpha_2 = (1,1), \mathcal{M} = \{\alpha_1, \alpha_2\}$. 而去除原点 $(0,0)$ 的情况下共有 2 个等价类: $\beta_1 = \{(0,1)\}, \beta_2 = \{(1,0), (1,1)\}, \mathcal{N} = \{\beta_1, \beta_2\}$. 那么, 我们得到的校验矩阵 H_2 为

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

注意到 H_2 是 $M_{2\times 2}(\mathbb{F}_2)$ 上的一个满秩矩阵, 即 $\rho(H_2) = 2$.

在 $p = 3$ 时, 由节4.2.1的讨论知 $H_3 \in M_{6\times 6}(\mathbb{F}_2)$. 此时非奇异条件为 $a \neq 0$, $\mathbb{F}_3^2$ 上的等价条件是 $(x, y) \sim (x, -y)$. 我们规定

$$\mathcal{M} = \{(1,0), (1,1), (1,2), (2,0), (2,1), (2,2)\},$$

$\mathcal{N}$ 中元素顺序是

$$\beta_1 = \overline{(0,0)}, \beta_2 = \overline{(0,1)}, \beta_3 = \overline{(1,0)}, \beta_4 = \overline{(1,1)}, \beta_5 = \overline{(2,0)}, \beta_6 = \overline{(2,1)}.$$

我们由此给出 H_3 为

$$H_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

计算得到 $\rho(H_3) = 4 < 6$.

表4.1给出了给定素数 $p \leqslant 59$ 时矩阵 H_p 的尺寸和秩 $\rho(H_p)$ 的计算结果. 我们从中发现除 $p = 3$ 一个特例以外, 每个由 $\mathbb{F}_p$ 上椭圆曲线确定的校验矩阵 H_p 都是列满秩的. 计算程序在节B.1给出.

我们由此提出猜想:

猜想 4.1： 设 p 是一个不同于 3 的素数, 则由 $\mathbb{F}_p$ 上由节4.1给出的校验矩阵 H_p 是一个 $M_{M\times N}(\mathbb{F}_2)$ 上的列满秩矩阵, 即

$$\rho(H_p) = \begin{cases} 2 & \text{if } p = 2 \\ \frac{1}{2}p(p+1) & \text{if } p \geqslant 5 \end{cases}.$$

从而我们知道除 $p = 3$ 的情况外, H_p 只能定义一个平凡的线性码.

我们注意到这个猜想同时也具备一定的代数几何意义. 我们可以将有限平面 $\mathbb{A}^2(\mathbb{F}_q)$ 中 q^2 个点视作顶点集 V^q（或考虑射影平面 $\mathbb{P}^2(\mathbb{F}_q)$）, 由参数 (a_i, b_i) 给出的椭圆曲线 $C(a_i, b_i)$ 给定的顶点间的连接方式视作边集 $E^q(a_i, b_i)$, 这从而给定了一张图 $G_i^q = (V^q, E^q(a_i, b_i))$. 设 $\mathfrak{G}$ 是 V^q 及其子集上所有图形成的集合, 我们定义两张图 $G_1 = (V_1, E_1), G_2 = (V_2, E_2) \in \mathfrak{G}$ 的加法为

$$G_1 + G_2 = (V_1 \cup V_2, E_1 \bigtriangleup E_2),$$

其中 $A \bigtriangleup B$ 表示两个集合 A, B 的对称差, 即 $A \bigtriangleup B = (A \setminus B) \cup (B \setminus A)$. 注意到对于任意一张图 $G \in \mathfrak{G}$, $2G := G + G$ 是一张空图, 记作 0. 因此装备有如此结构的 $\mathfrak{G}$ 是一个 $\mathbb{F}_2$ 上的线性空间. 特别地, 我们关心的问题是由我们给定的有限域 $\mathbb{F}_q$ 上的椭圆曲线族给出的图 $\{G_i^q\}_{1\leqslant i\leqslant M(H_q)}$ 在 $\mathfrak{G}$ 中生成的线性空间的维数. 我们因此也就能够通过研究模 (或线性空间) 的方式研究有限域上的椭圆曲线结构了. 关于

表 4.1　校验矩阵 H_p 的秩

素数 p	行数 $M\left(H_p\right)$	列数 $N\left(H_p\right)$	秩 $\rho\left(H_p\right)$
2	2	2	2
3	6	6	4
5	20	15	15
7	42	28	28
11	110	66	66
13	156	91	91
17	272	153	153
19	342	190	190
23	506	276	276
29	812	435	435
31	930	496	496
37	1332	703	703
41	1640	861	861
43	1806	946	946
47	2162	1128	1128
53	2756	1431	1431
59	3422	1770	1770

图上线性空间结构的深入讨论, 请读者参考 [26]章 1.9.

4.3.2　C_{2^s} 的分析

我们回到通过特征为 2 的域上的椭圆曲线构造的校验矩阵 H_{2^s} 和它所定义的线性码 C_{2^s} 的分析, 其中 $s \in \mathbb{N}$. 我们已经计算过 $s = 1$ 的情形: $H_2 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$. 下面来讨论更一般的情况.

H_{2^s} 的维数　我们计算几则具体的例子来说明情况.

考查 $s = 2$ 的情形. 注意到 $x^2 + x + 1$ 是 $\mathbb{F}_2[x]$ 中的一个 2 次不可约多项式, 因此考虑域 $\mathbb{F}_2[x]/(x^2 + x + 1)$ 是一个 $\mathbb{F}_2$ 上扩张次数是 2 的域, 即是一个包含 4 个元素的域的一种构造, 记 α 是 $\mathbb{F}_4$ 的生成元, 则 $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$. 根据节4.1中规则计

算并重排之后得到

$$H_4 = \begin{bmatrix} \Xi & \Xi & \Xi' \\ \Xi & 0 & \Xi \\ \Xi & I_3 & 0 \\ \Xi & \Xi'' & 0 \end{bmatrix}.$$

其中

$$\Xi = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad \Xi' = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \quad \Xi'' = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

计算进而得到

$$\rho(H_4) = 8.$$

表4.2给出了给定正整数 $1 \leqslant s \leqslant 8$ 时矩阵 H_{2^s} 的尺寸和秩 $\rho(H_{2^s})$ 的计算结果. 我们从中发现每个由 $\mathbb{F}_{2^s}$ 上椭圆曲线确定的校验矩阵 H_{2^s} 都满足

$$\rho\left(H_{2^s}\right) = 3^s - 1.$$

计算过程在节B.2中给出.

表 4.2　校验矩阵 H_{2^s} 的秩

正整数 s	行数 $M\left(H_{2^s}\right)$	列数 $N\left(H_{2^s}\right)$	秩 $\rho\left(H_{2^s}\right)$
1	2	2	2
2	12	9	8
3	56	35	26
4	240	135	80
5	992	527	242
6	4032	2079	728
7	16256	8255	2186

我们由此提出猜想:

猜想 4.2： 设 $s \in \mathbb{N}$ 是一个正整数, 则由 $\mathbb{F}_{2^s}$ 上由节4.1给出的校验矩阵 $H_{2^s} \in \boldsymbol{M}_{M\times N}(\mathbb{F}_2)$ 满足

$$\rho\left(H_{2^s}\right) = 3^s - 1.$$

我们注意到, 这一结果和式(3.2)中给出的结果完全一致. 但我们需要指出的是, 我们在节3.2中的证明方式并不能推广到对椭圆曲线定义的码的分析中来. 比如在 $s = 3$ 的情况下, H_8 是不可以类似 H_4 一样转化成分块循环阵的. 我们需要设计新的证明思路.

C_{2^s} 的最小距离 下面我们来讨论线性码 C_{2^s} 的最小距离. 我们先陈述这样一个命题.

命题 4.4： 设 C 是一个由校验矩阵 H 给出的线性码, 如果 H 的围长大于等于 6, 则 C 的最小距离满足

$$d(C) \geqslant \gamma + 1,$$

其中 γ 表示 H 的最小列重.

证明： 请参考 [27] 或 [4][40]. □

由 H_q 的围长至少是 6 的条件, 注意到在特征为 2 的域 $\mathbb{F}_{2^s}$ 的情况下, 式(4.7)给出此时 $\gamma = 2^s - 1$, 我们由此可以知道 C_{2^s} 的最小距离至少是 2^s, 即

$$d\left(C_{2^s}\right) \geqslant 2^s.$$

表4.3给出了给定正整数 $1 \leqslant s \leqslant 4$ 时线性码 C_{2^s} 的码字长度, 维数和最小距离. 其中带有 "(估计)" 字样的数据是我们通过概率搜索算法得到的数据, 虽然这

表 4.3 线性码 C_{2^s} 的计算结果

正整数 s	C_{2^s} 的码字长度	C_{2^s} 的维数	C_{2^s} 的最小距离
1	2	0	$+\infty$
2	9	1	9
3	35	9	10
4	135	55	18(估计)

里没有进行穷尽搜索, 但我们认为这一数据仍有较高的可信度. 我们在B.3节给出计算线性码 C_8 最小距离的计算程序. 表4.4给出了线性码 C_8 的所有码重的分布情况. 注意到这一重量谱分布关于 $\frac{35}{2}$ 是对称的, 这是因为全为 1 的码字在 C_8 中.

除了 $s = 1, 2$ 这类域中元素较少的情况, 我们注意到 C_{2^s} 的最小距离应当是 $2^s + 2$. 我们由此提出猜想:

猜想 4.3： 设 $s \geqslant 3$ 是一个正整数, 则由 $\mathbb{F}_{2^s}$ 上由节4.1给出的校验矩阵 $H_{2^s} \in$

表 4.4　线性码 C_8 的码重的分布

码重 d	个数 W_d
0	1
10	24
12	12
13	30
14	54
15	24
16	27
17	84
18	84
19	27
20	24
21	54
22	30
23	12
25	24
35	1

$\boldsymbol{M}_{M\times N}(\mathbb{F}_2)$ 确定的线性码 C_{2^s} 的最小距离是

$$d\left(C_{2^s}\right)=2^s+2.$$

第 5 章　结论

我们研究了基于有限平面上的直线族和椭圆曲线族决定的线性码. 在此基础上, 我们通过数值计算提出了关于在 $\mathbb{F}_p, \mathbb{F}_{2^s}$ 的情形下椭圆曲线族决定的线性码的维数和最小距离等的猜想. 这些猜想给出了这类码具体的代数特征, 说明了这类线性码设计的理论和现实意义, 表明此类线性码比直线族决定的线性码可能具备更出色的特性. 此外, 我们同时还给出了通过分块循环矩阵证明 $\mathbb{F}_{2^s}$ 上有限平面直线族决定的线性码的维数的思路.

研究中主要遇到的困难包括:

1. 由于有限域上的计算较为复杂, 我们对于一般特征下的有限域上相关码的研究遇到了极大的障碍, 没有获得一般情形下的结论.
2. 受计算能力所限, 我们对最小距离的分析不可能进行穷尽搜索, 而现下关于此问题所得的数据极为有限, 尚不具备完全的说服能力.
3. 关于校验矩阵的秩的证明无法利用我们设计的循环矩阵或直接利用直线族上的代数几何的相关证明方式 (如 [10]). 而且基于椭圆曲线族的构造为研究造成了极大的困难.

我们进一步的工作计划是参考 [10], 利用更深入的代数几何语言来证明相关猜想.

插图索引

表格索引

参考文献

[1] GRIFFITHS P A. Introduction to algebraic curves[M]. Providence, Rhode Island, U.S.A.: American Mathematical Society, 1989.

[2] ARBARELLO E, CORNALBA M, GRIFFITHS P A, et al. Geometry of algebraic curves: volume 1[M]. New York: Springer, 1985.

[3] BLAHUT R E. Algebraic codes on lines, planes, and curves[M]. New York: Cambridge University Press, 2008.

[4] VAN LINT J H. Graduate texts in mathematics: number 86 introduction to coding theory [M]. 3rd ed. Springer-Verlag, 1999.

[5] VAN DER GEER G, VAN DER VLUGT M. Reed-Muller codes and supersingular curves. I [J/OL]. Compositio Math., 1992, 84(3): 333-367. http://www.numdam.org/item?id=CM_1992__84_3_333_0.

[6] E. J. WELDON J. Difference-set cyclic codes[J]. Bell System Technical Journal, 1966, 45(7): 1045−1055.

[7] GRAHAM R L, MACWILLIAMS J. On the number of information symbols in difference-set cyclic codes[J]. Bell System Technical Journal, 1966, 45(7): 1057−1070.

[8] SMITH K J C. On the rank of incidence matrices in finite geometries: number 555[Z]. Chapel Hill, N.C., U.S.A., 1967.

[9] GOETHALS J M, DELSARTE P. On a class of majority-logic decodable cyclic codes[J/OL]. IEEE Transactions on Information Theory, 1968, 14(2): 182-188. DOI: 10.1109/TIT.1968.1054126.

[10] HAMADA N. The rank of incidence matrix of points and d-flats in infinite geometries[J]. Journal of Science of the Hiroshima University. Series A-I, Mathematics, 1968, 32(2): 381-396.

[11] JUNGNICKEL D, TONCHEV V D. Polarities, quasi-symmetric designs, and hamada' s conjecture[J/OL]. Designs, Codes and Cryptography, 2009, 51: 131−140. DOI: https://doi.org/10.1007/s10623-008-9249-8.

[12] SAOUTER Y. Constructions of ldpcs from elliptic curves over finite fields[J/OL]. IEEE Communications Letters, 2017, 21(12): 2558-2561. DOI: 10.1109/LCOMM.2017.2750660.

[13] KOVALEV S, KRACHKOVSKY V Y. A simple method to construct ldpc codes based on projective planes[C/OL]//2011 IEEE International Symposium on Information Theory Proceedings. 2011: 737-741. DOI: 10.1109/ISIT.2011.6034231.

[14] LIU H, HUANG Q, DENG G, et al. Quasi-cyclic representation and vector representation of rs-ldpc codes[J/OL]. IEEE Transactions on Communications, 2015, 63(4): 1033-1042. DOI: 10.1109/TCOMM.2015.2399395.

[15] HARTSHORNE R. Algebraic geometry[M]. New York: Springer, 2006.

[16] KNAPP A W. Mathematical notes: number 40　elliptic curves[M]. Princeton, New Jersey: Princeton University Press, 1992.

[17] SILVERMAN J H. Graduate texts in mathematics: number 106　the arithmetic of elliptic curves[M/OL]. New York: Springer, 2009. DOI: https://doi.org/10.1007/978-0-387-09494-6.

[18] ATIYAH M F, MACDONALD I G. Introduction to commutative algebra[M]. Reading, MA: Addison-Wesley Publishing Company, 1969.

[19] HUSEMöLLER D. Elliptic curves[M]. New York: Spriner-Verlag, 2004.

[20] TAO T. Pappus’ s theorem and elliptic curves[EB/OL]. (2011-07-15). https://terrytao.wordpress.com/2011/07/15/pappuss-theorem-and-elliptic-curves/.

[21] WASHINGTON L C. Elliptic curves[M]. 2nd ed. Chapman & Hall/CRC, 2008.

[22] HARTSHORNE R. 数学名著译丛: 代数几何[M]. 冯克勤, 刘木兰, 胥鸣伟, 译. 北京: 科学出版社, 2001.

[23] ENGE A. Elliptic curves and their applications to cryptography: An introduction[M]. Dordrecht: Kluwer Academic Publishers, 1999.

[24] 冯克勤. 研究生数学丛书: 第 4 册　纠错码的代数理论[M]. 北京: 清华大学出版社, 2005.

[25] TANNER R. A recursive approach to low complexity codes[J/OL]. IEEE Transactions on Information Theory, 1981, 27(5): 533-547. DOI: 10.1109/TIT.1981.1056404.

[26] DIESTEL R. Graduate texts in mathematics: number 173　graph theory[M]. 3rd ed. New York: Springer, 2005.

[27] MASSEY J L. Threshold decoding[Z]. Cambridge, 1963.

[28] SILVERMAN J H, TATE J. Undergraduate texts in mathematics: Rational points on elliptic curves[M]. New York: Springer-Verlag, 1992.

致　　谢

感谢我的父母及所有家人对我生活中的一切帮助, 关心, 爱护和照顾. 他们身上所具备的勤劳朴实, 认真刻苦, 勇敢实干的品质在任何时刻都是我最深切的感动.

感谢我的导师马连荣老师和刘海洋学长. 他们对我极尽全力的帮助和对我行为中的错误, 性格中的缺点的极大包容使我触动至深, 难以用言辞表达.

感谢 Silverman 和 Tate 合著的 *Rational Points on Elliptic Curves* [28]. 这本书用完全清楚明白的语言完全打开了我对椭圆曲线相关内容的兴趣, 培养了我对代数几何相关内容的感觉. 但囿于逻辑严密所限, 文中并未引用此书, 我至为抱歉.

感谢我的朋友田洋和张中弛对本文的极大贡献. 数个深夜, 我以私事占用他们的时间, 压榨他们的劳动, 挑战他们的思考能力. 他们对本文居功至伟.

感谢杨一龙老师提供了对称差的思路, 感谢扶磊老师提供了椭圆函数和椭圆积分历史部分的回顾工作. 特别地, 我在写作本文的过程中向他们咨询了相关猜想, 他们的帮助举足轻重.

感谢我所有最亲爱的朋友们, 他们对我的无私和包容是我人生欢畅的源泉. 特别感谢其他在本文写作过程中与我沟通交流, 排解压抑和苦闷的朋友们, 如果没有他们, 本文可能会更早和大家见面.

声　明

本人郑重声明：所呈交的学位论文，是本人在导师指导下，独立进行研究工作所取得的成果。尽我所知，除文中已经注明引用的内容外，本学位论文的研究成果不包含任何他人享有著作权的内容。对本论文所涉及的研究工作做出贡献的其他个人和集体，均已在文中以明确方式标明。

签　名：侯智冬　　日　期：2021/06/07

附录 A　外文资料的调研阅读报告

Contents

A.1 Elliptic Curves

Studies on elliptic curves have taken the cardinal part of number theory for centuries, and this subject gave birth to lots of advanced topics, including Sato-Tate Conjecture and Birch and Swinnerton-Dyer Conjecture, etc. There are two traditional ways leading to the study of elliptic curves, one from algebra, the other from analysis.

From the viewpoint of algebra, we focus on the solutions to the so-called Diophantine equations, i.e., the zero locus of integer-coefficient polynomials in $\mathbb{Z}$ or $\mathbb{Q}$. The simplest case with merely one variable can be solved rather easily by the Rational Root Theorem. There are more interesting phenomenon occurring for the two-variable case. The linear case is trivial, while the conic case can be solved using projection. However, we need more sophisticated designs on non-singular cubic curves, which are so-called elliptic curves.

Mathematical analysts, however, developed interests in this topic from the study of such an integral,

$$z = \int_0^x \frac{1}{\sqrt{(1-t^2)(1-k^2t^2)}}, \tag{A.1}$$

where $0 < k < 1$. This comes from the circumference of an ellipse and the study of vibration. Euler first noticed that even though we could not obtain an explicit formula, some connections between different upper limits in the integral could be constructed as

$$\int_0^\alpha \frac{dt}{\sqrt{f(t)}} + \int_0^\beta \frac{dt}{\sqrt{f(t)}} = \int_0^\gamma \frac{dt}{\sqrt{f(t)}},$$

where $f(t) = \sqrt{(1-t^2)(1-k^2t^2)}, \gamma = g(\alpha, \beta)$ for some rational polynomial $g(x, y)$ [1].

Jacobi firstly introduced the addition law on elliptic curves [2]. Meanwhile, Abel generalized the elliptic integral to complex numbers. He also proposed the viewpoint of regarding x as the implicit function of z [3], which prepared a most useful weapon, the invariant differential. Furthermore, Weierstrass constructed the widely-famous $\wp$-function for a lattice $\Lambda \subset \mathbb{C}$ as

$$\wp(z) = \sum_{\omega \in \Lambda, \omega \neq 0} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right].$$

He also proved that all the elliptic functions could be written as the rational function of $\wp(z)$ and $\wp'(z)$ [4].

Some significant results on elliptic curves are listed here. Poincaré finally explicitly introduced the group structure of elliptic curves and made a conjecture on the finite-generated property of rational points on elliptic curves [5]. Mordell proved this conjecture through height function and infinite descent theorem [6], while Weil extended the result to elliptic curves over number fields [7]. Nagell [8] and Lutz [9] proved that all the rational torsion points are actually of integer coordinates, and gave a tight bound on their coordinates.

Another breakthrough happened in the studies of elliptic curves over finite fields. E. Artin conjectured in his thesis that

$$\left| \#C\left(\overline{\mathbb{F}}_q\right) - (q+1) \right| \leqslant 2\sqrt{q},$$

where $C\left(\overline{\mathbb{F}}_q\right)$ denotes an elliptic curve over the finite field $\overline{\mathbb{F}}_q$ [10]. This gives a rather tight upper bound of estimation. Hasse proved it [11], and a further generalization to general algebraic curves was due to Weil [12] as follows.

Theorem A.1 (Hasse-Weil): Let C be a non-singular irreducible curve of genus g defined over the finite field $\mathbb{F}_q$. Then the number of points on C with coordinates in $\mathbb{F}_q$ is $q + 1 + \epsilon$, where ϵ satisfies that

$$|\epsilon| \leqslant 2g\sqrt{q}.$$

Furthermore, Weil proposed a series of conjectures in [13] about the Hasse-Weil zeta functions on general varieties, which was motivated by the studies on elliptic curves. They were partially proved by Dwork [14] and finished by Deligne [15].

An exciting application of elliptic curves is to prove Fermat's Last Theorem, which

states as follows.

Theorem A.2: Let $n \geqslant 3$ be an integer, and then the equation

$$x^n + y^n = z^n$$

has no integer solution.

Frey [16], Serre [17], and Ribet [18] showed the elaborate links between Fermat's Last Theorem and Taniyama-Shimura Conjecture, while Wiles proved the latter [19].

We thank [20-21] for providing us with hints for arranging such an chronological order of this history and clues for references.

A.2 Elliptic Curves in Coding Theory

A large number of present scientific literature makes advantage of algebraic geometry to construct new codes or determine the weight distributions, especially the theory of families of algebraic curves over a finite field [22]. We, here, take several codes for instance. Goppa codes are constructed from a fixed algebraic curve, and we can determine the weight distributions and frequency of Melas codes and Zetterberg cords using elliptic curves [23-26].

A more in-depth relationship between coding theory and elliptic curves is shown via Reed-Muller codes. Consider the space

$$R(r,m) = \left\{ (f(v))_{v \in \mathbb{F}_2^m} \,|\, f \in \mathbb{F}_2[X_1, \cdots, X_m], \deg f \leqslant r \right\}.$$

Let $q = 2^m$ for some $m \geqslant 3$ as an integer and consider the space

$$\mathcal{R}_h = \left\{ R = \sum_{i=0}^{h} a_i X^{2^i} \middle| a_i \in \mathbb{F}_q \right\} \quad \left(h \leqslant \left[\frac{m}{2} \right] \right).$$

Note that

$$\mathcal{C}_h = \left\{ (\mathrm{Tr}[xR(x)])_{x \in \mathbb{F}_q} \,|\, R \in R_h \right\}$$

is a sub-code of $R(2,m)$. Let $\mathfrak{N}(R)$ be the number of rational points on the affine curve $y^2 + y = xR(x)$ for $R \in \mathcal{R}_h$, and it is obvious that

$$w\left((\mathrm{Tr}[xR(x)])_{x \in \mathbb{F}_q} \right) = q - \frac{1}{2}\mathfrak{N}(R),$$

which leading us to study the family of curves

$$C_R : y^2 + y = xR(x), \quad R \in \mathcal{R}_h.$$

The automorphism group of algebraic curves helps solve this problem. Let

$$W_R := \left\{ x \in \mathbb{F}_q | \operatorname{Tr}[xR(y) + yR(x)] = 0 \quad \forall y \in F_q \right\},$$
$$V_R := \left\{ x \in W_R | \operatorname{Tr}[xR(x)] = 0 \right\}.$$

We hence have the criterion as follows.

Proposition A.1: Follow the above notations, and it holds that

$$\operatorname{card} C_R(\mathbb{F}_q) = \begin{cases} q+1 & \text{if } V_R = W_R, \\ q+1 \pm \sqrt{2^w q} & \text{if } V_R = W_R, \end{cases}$$

where $w = \dim_{\mathbb{F}_2} W_R$.

Moreover, we know that in case $h = 1$, these curves C_R are super-singular curves over $\mathbb{F}_q$. See [27] for references.

More amazingly, it turns out coding theory can also help algebraic geometry to find many maximal and minimal curves, which denotes the curves touching the Hasse-Weil upper and lower bounds, respectively. Note that the formulas of numbers

$$n_w^h := \operatorname{card} \left\{ R \in R_h | a_0 = 0, a_h \neq 0, \dim(W_R) = w \right\}$$

can be explicitly shown by results on sub-codes of binary Reed-Muller codes $R(2, m)$. Relations between these numbers are given as

$$\sum_w (2^w - 1) n_w^h = \begin{cases} 2(q-1)^2 q^{h-2} & \text{if } h \geqslant 2 \\ q-1 & \text{if } h = 1 \end{cases}.$$

More detailed analysis and further generalization for finite fields of general characteristics can be found in [27-28].

A novel method of constructing low density parity-check codes (LDPCs) was given in [29]. He selected some particular families of elliptic curves on finite planes of different characteristics. In addition to this, using the inverse of elliptic curves, he partitioned the whole finite plane and then obtained the incidence matrix. This matrix, regarded as the parity-check matrix, hence gives a kind of linear code. Actually, such method is rather omnipresent to construct linear codes via families of lines on finite planes. A series of papers [30-34] studied such construction of projective planes and flat planes of arbitrary

dimension over finite fields, while affine-plane cases were shown in [34-35].

参考文献

[1] Burt Totaro. Euler and algebraic geometry. URL https://www.math.ucla.edu/~totaro/papers/public_html/euler.pdf.

[2] Carl Gustav Jacob Jacobi. *Fundamenta nova theoriae functionum ellipticarum*. Cambridge Library Collection - Mathematics. Cambridge University Press, 2012. doi: 10.1017/CBO9781139344081.

[3] Niels Henrik Abel. Recherches sur les fonctions elliptiques. *Acta Mathematica*, 26(none):3 – 41, 1902. doi: 10.1007/BF02415484. URL https://doi.org/10.1007/BF02415484.

[4] Karl Weierstrass. *Mathematische Werke: Herausgegeben unter Mitwirkung einer von der königlich preussischen Akademie der Wissenschaften eingesetzten Commission*, volume 4 of *Cambridge Library Collection - Mathematics*. Cambridge University Press, 2013. doi: 10.1017/CBO9781139567893.

[5] Henri Poincaré. Sur les propriétés arithmétiques des courbes algébriques. *Journal de Mathématiques Pures et Appliquées*, 7:161–234, 1901.

[6] Louis Joel Mordell. On the rational solutions of the indeterminate equations of the third and fourth degree. *Proceedings of the Cambridge Philosophical Society*, 21:179–192, 1922.

[7] André Weil. Sur un théorème de mordell. *Bulletin des Sciences Mathématiques*, 54:182–191, 1930.

[8] Trygve Nagell. Solution de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre. *Skrifter Norske Videnskaps-Akademi i Oslo*, 1:1–25, 1935.

[9] Élisabeth Lutz. Sur l'equation $y^2 = x^3 - ax - b$ dans les corps $\mathfrak{p}$-adiques. *Journal für die reine und angewandte Mathematik*, 177:238–247, 1937.

[10] Emil Artin. Quadratische Körper im Gebiete der höheren Kongruenzen. II. *Math. Z.*, 19(1): 207–246, 1924. ISSN 0025-5874. doi: 10.1007/BF01181075. URL https://doi.org/10.1007/BF01181075.

[11] Helmut Hasse. Zur Theorie der abstrakten elliptischen Funktionenkörper. I: Die Struktur der Gruppe der Divisorenklassen endlicher Ordnung. *J. Reine Angew. Math.*, 175:55–62, 1936. ISSN 0075-4102; 1435-5345/e.

[12] André Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*. Actualités Scientifiques et Industrielles [Current Scientific and Industrial Topics], No. 1041. Hermann et Cie., Paris, 1948. Publ. Inst. Math. Univ. Strasbourg **7** (1945).

[13] André Weil. Numbers of solutions of equations in finite fields. *Bulletin of the American Mathematical Society*, 55(5):497 – 508, 1949. doi: bams/1183513798. URL https://doi.org/.

[14] Bernard Dwork. On the rationality of the zeta function of an algebraic variety. *Amer. J. Math.*, 82:631–648, 1960. ISSN 0002-9327. doi: 10.2307/2372974. URL https://doi.org/10.2307/2372974.

[15] Pierre Deligne. La conjecture de weil. i. *Amer. J. Math.*, 43:273–307, 1974. URL https://doi.org/10.1007/BF02684373.

[16] Gerhard Frey. Links between stable elliptic curves and certain Diophantine equations. *Ann. Univ. Sarav. Ser. Math.*, 1(1):iv+40, 1986. ISSN 0933-8268.

[17] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de Gal($\overline{\mathbf{Q}}$/$\mathbf{Q}$). *Duke Math. J.*, 54(1):179–230, 1987. ISSN 0012-7094. doi: 10.1215/S0012-7094-87-05413-5. URL https://doi.org/10.1215/S0012-7094-87-05413-5.

[18] Kenneth Alan Ribet. On modular representations of Gal($\overline{\mathbf{Q}}$/$\mathbf{Q}$) arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990. ISSN 0020-9910. doi: 10.1007/BF01231195. URL https://doi.org/10.1007/BF01231195.

[19] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995. ISSN 0003-486X. doi: 10.2307/2118559. URL https://doi.org/10.2307/2118559.

[20] Joseph H. Silverman and John Tate. *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992. ISBN 3-540-97825-9.

[21] Anthony W. Knapp. *Elliptic Curves*. Number 40 in Mathematical Notes. Princeton University Press, Princeton, New Jersey, 1992.

[22] Gerard van der Geer. Codes and elliptic curves. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 159–168. Birkhäuser Boston, Boston, MA, 1991.

[23] Gilles Lachaud and Jacques Wolfmann. Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristique 2. *C. R. Acad. Sci. Paris Sér. I Math.*, 305(20):881–883, 1987. ISSN 0249-6291.

[24] René Schoof and Marcel van der Vlugt. Hecke operators and the weight distributions of certain codes. *J. Combin. Theory Ser. A*, 57(2):163–186, 1991. ISSN 0097-3165. doi: 10.1016/0097-3165(91)90016-A. URL https://doi.org/10.1016/0097-3165(91)90016-A.

[25] Gerard van der Geer, René Schoof, and Marcel van der Vlugt. Weight formulas for ternary Melas codes. *Math. Comp.*, 58(198):781–792, 1992. ISSN 0025-5718. doi: 10.2307/2153217. URL https://doi.org/10.2307/2153217.

[26] Gerard van der Geer and Marcel van der Vlugt. Artin-Schreier curves and codes. *J. Algebra*, 139(1):256–272, 1991. ISSN 0021-8693. doi: 10.1016/0021-8693(91)90293-H. URL https://doi.org/10.1016/0021-8693(91)90293-H.

[27] Gerard van der Geer and Marcel van der Vlugt. Reed-Muller codes and supersingular curves. I. *Compositio Math.*, 84(3):333–367, 1992. ISSN 0010-437X. URL http://www.numdam.org/item?id=CM_1992__84_3_333_0.

[28] Gerard van der Geer and Marcel van der Vlugt. Trace codes and families of algebraic curves. *Math. Z.*, 209(2):307–315, 1992. ISSN 0025-5874. doi: 10.1007/BF02570836. URL https://doi.org/10.1007/BF02570836.

[29] Yannick Saouter. Constructions of ldpcs from elliptic curves over finite fields. *IEEE Communications Letters*, 21(12):2558–2561, 2017. doi: 10.1109/LCOMM.2017.2750660.

[30] Ronald Graham and Jessie MacWilliams. On the number of information symbols in difference-set cyclic codes. *Bell System Technical Journal*, 45(7):1057–1070, 1966.

[31] Jr. E. J. Weldon. Difference-set cyclic codes. *Bell System Technical Journal*, 45(7):1045–1055, 1966.

[32] K. J. C. Smith. On the rank of incidence matrices in finite geometries, 1967.

[33] J.-M. Goethals and P. Delsarte. On a class of majority-logic decodable cyclic codes. *IEEE Transactions on Information Theory*, 14(2):182–188, 1968. doi: 10.1109/TIT.1968.1054126.

[34] Noboru Hamada. The rank of incidence matrix of points and d-flats in infinite geometries. *Journal of Science of the Hiroshima University. Series A-I, Mathematics*, 32(2):381–396, 1968.

[35] Dieter Jungnickel and Vladimir D. Tonchev. Polarities, quasi-symmetric designs, and hamada's conjecture. *Designs, Codes and Cryptography*, 51:131–140, 2009. doi: https://doi.org/10.1007/s10623-008-9249-8.

附录 B　计算程序

B.1　计算校验矩阵 H_p 的秩 $\rho(H_p)$ 的程序

我们这节给出节4.3.1中计算校验矩阵 H_p 的秩 $\rho(H_p)$ 的程序, 这一程序感谢田洋和张中弛的鼎力相助. 这是一份 Matlab 代码.

Listing B.1　计算 $\rho(H_p)$ 的 Matlab 程序代码

```
%% P
Number = [1:1:10];
index = isprime(Number);
Number(~index)= [];
P=Number;

%%定义(X,Y)
CellofAnswerMatrix=cell(length(P),1);
RKVector=zeros(length(P),1);
PVector=zeros(length(P),1);
P1Vector=zeros(length(P),1);
P2Vector=zeros(length(P),1);
P3Vector=zeros(length(P),1);
IndexVector=zeros(length(P),1);
for IDP=2
NeedP=P(IDP);  %% 输入素数n
disp(IDP)
[X,Y]=meshgrid([0:1:NeedP-1],[0:1:(NeedP-1)/2]); %% 定义(X,Y)
PointLocation=[X(:),Y(:)];

%%定义(A,B)
[A,B]=meshgrid([0:1:NeedP-1],[0:1:NeedP-1]);  %% 定义(A,B)
ABPossibility=[A(:),B(:)];
NeededAB=[];
```

```
for ID=1:size(ABPossibility,1)
    if ABPossibility(ID,1)~=0
        NeededAB=[NeededAB;ABPossibility(ID,:)];
    end
end

%%计算矩阵并输出
AnswerMatrix=zeros(size(NeededAB,1),size(PointLocation,1));
for ID1=1:size(NeededAB,1)
    NeededCurve=NeededAB(ID1,:);
    for ID2=1:size(PointLocation,1)
        Value=PointLocation(ID2,1)^3+
        NeededCurve(1)*PointLocation(ID2,1)+
        NeededCurve(2)-PointLocation(ID2,2)^2;
        if mod(Value,NeedP)==0
            AnswerMatrix(ID1,ID2)=1;
        elseif mod(Value,NeedP)~=0
            AnswerMatrix(ID1,ID2)=0;
        end
    end
end
CellofAnswerMatrix{IDP,1}=AnswerMatrix;
SAVector=sum(AnswerMatrix);
PVector(IDP)=length(find(SAVector==NeedP));
P1Vector(IDP)=length(find(SAVector==NeedP-1));
P2Vector(IDP)=length(find(SAVector==NeedP-2));
P3Vector(IDP)=length(find(SAVector==NeedP-3));
RKVector(IDP) = gfrank(AnswerMatrix,2);
if RKVector(IDP)==size(AnswerMatrix,2)
    IndexVector(IDP)=1;
end
end
```

```
figure('Color',[1,1,1]);
hold on;
plot(PVector,'LineWidth',3);
plot(P1Vector,'LineWidth',3);
plot(P2Vector,'LineWidth',3);
plot(P3Vector,'LineWidth',3);
hold off
```

B.2 计算校验矩阵 H_{2^s} 的秩 $\rho(H_{2^s})$ 的程序

我们这节给出节4.3.2中计算校验矩阵 H_{2^s} 的秩 $\rho(H_{2^s})$ 的程序, 这一程序感谢刘海洋和田洋的鼎力相助. 这是一份 Matlab 代码.

Listing B.2 计算 $\rho(H_{2^s})$ 的 Matlab 程序代码

```
    Nvector=2:12;
RankH=zeros(1,length(Nvector));
HCell=cell(length(Nvector),1);
for ID=4:6
    n = Nvector(ID);
    alpha = gf(2,n); % pm of F_16
    % Step 1: form a complete H
    q = 2^n;
    H = [];
    GF0=gf(0,n);
    for A = 0:q-1
        GFA=gf(A,n);
        for B = 0:q-1
            GFB=gf(B,n);
            for C = 1:q-1
                GFC=gf(C,n);
                tic;
                disp([q-1-A,q-1-B,q-1-C])
```

```
                HRaw = zeros(1,q^2);
                for X = 0:q-1
                    GFX=gf(X,n);
                    for Y = 0:q-1
                        GFY=gf(Y,n);
                        sY = GFY * GFY;
                        CY = GFC * GFY;
                        cX = GFX * GFX * GFX;
                        AX = GFA * GFX;
                        sM = sY + CY + cX + AX + GFB;
                        if sM == GF0
                            HRaw(X*q+Y+1) = 1;
                        end
                    end
                end
                H = [H;HRaw];
            end
            toc;
        end
    end
    % save H_F8.mat H;
    RankH(ID)=gfrank(H,2);
    HCell{ID,1}=H;
end
```

B.3 计算线性码 C_8 的最小距离的程序

我们这节给出节4.3.2中计算线性码 C_8 的最小距离的程序, 这一程序感谢刘海洋的无私付出. 这是一份 Matlab 代码.

Listing B.3 计算 $C(H_8)$ 最小距离的 Matlab 程序代码

```
    clear all;
load H_F8.mat;
```

```
H2 = H(1:5,:);
H3 = H(11:16,:);
H4 = H(20:30,:);
H5 = H(42:44,:);
H6 = H(56,:);
HH = [H2;H3;H4;H5;H6];
% gfrank(HH)
% rv = randperm(35);
load rv.mat;
H_new = [];
for i = 1:35
    H_new = [H_new,HH(:,rv(i))];
end
gfrank(H_new)
for i = 1:26
    %i
    if H_new(i,i) == 0
        flag = 0;
        for k = i+1:26
            if H_new(k,i) == 1
                h_tmp = H_new(k,:);
                H_new(k,:) = H_new(i,:);
                H_new(i,:) = h_tmp;
                flag = 1;
            end
            if flag == 1
                break;
            end
        end
    end
    for j = 1:26
        if j ~= i
```

```
            if H_new(j,i) == 1
                H_new(j,:) = mod(H_new(j,:)+H_new(i,:),2);
            end
        end
    end
end
P = H_new(:,27:35);
G = [P',eye(9)];
cw_set = [];
pc_set = [];
for ii = 1:511
    ii
    ms = deci2bin(ii,9);
    cw = mod(ms*G,2);
    % 反向check
    c_tmp = zeros(1,35);
    for k = 1:35
        c_tmp(rv(k)) = cw(k);
    end
    pp = sum(mod(H*c_tmp',2));
    pc_set = [pc_set,pp];
    cw_set = [cw_set;cw];
end
ss = sum(cw_set')
```

在学期间参加课题的研究成果

个人简历

1998 年 12 月 22 日出生于黑龙江省鸡西市。

2016 年 8 月考入清华大学电机工程与应用电子技术系电气工程及其自动化专业。

2018 年 5 月转入清华大学数学科学系数学与应用数学专业至今。

在学期间完成的相关学术成果

学术论文：

[1] Hou H, Liu H, Ma L. Some results on incorrigible sets of binary linear codes[J/OL]. IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences,2021, E104-A(2): 582-586. DOI:10.1587/transfun.2020EAL2021.

综合论文训练记录表

<table>
<tr><td>学生姓名</td><td>侯贺冬</td><td>学号</td><td>2016010919</td><td>班级</td><td>数 71</td></tr>
<tr><td>论文题目</td><td colspan="5">有限域上代数曲线在编码理论中的应用</td></tr>
<tr><td>主要内容以及进度安排</td><td colspan="5">主要内容：学习椭圆曲线的基本理论，包括椭圆曲线的群结构，扭群结构中的 Nagell-Lutz 定理和 Mordell 定理，椭圆曲线的自同态环理论和 Hasse 定理。学习线性码的基本知识，特别关注基于有限平面上的直线族和点构造的线性码的分析，并基于此研究有限平面上的椭圆曲线族构造的线性码。进行数值计算，提出对于此类码的更进一步地分析，并以这类码为引，深入研究代数几何和编码理论的相互影响的各种联系。

进度安排：

2021 年 1 月—2021 年 4 月：开展椭圆曲线讨论班，综合各类参考材料研究椭圆曲线的基本理论。

2021 年 4 月—2021 年 5 月：开展对基于椭圆曲线族构造的线性码的研究工作并初步进行数值计算。

2021 年 5 月—2021 年 6 月：结合已有研究梳理这类码的特性，并对直线族定义的码进行了梳理和研究工作，开展论文的撰写和答辩工作。

指导教师签字：王连荣
考核组组长签字：钟金元
2021 年 3 月 19 日</td></tr>
<tr><td>中期考核意见</td><td colspan="5">学生研究进展顺利，已完成阶段性任务：基本完成对椭圆曲线基本知识的学习，具备较强的理论基础，对这一领域已有较好的理解，完全准备好后续对该领域前沿工作开展研究。但学生的演讲表达能力还需提高，答辩时神情拘束，缺乏互动。

考核组组长签字：钟金元
2021 年 4 月 24 日</td></tr>
</table>

指导教师评语	有限域上代数曲线及应用是代数领域的研究热点。论文作者在学习了椭圆曲线和代数编码的相关知识的基础上，深入研究了基于有限平面的直线族的线性码和基于有限域的椭圆曲线的线性码的构造过程和性质分析。特别地，论文作者采用数值观察的方法，给出了一类基于有限域的椭圆曲线的线性码的维数和最小距离的猜想，说明了基于有限域的椭圆曲线可以构造出良好参数的线性码，这一结果在代数编码领域有着深刻意义。论文选题意义明确，结构清晰，写作严谨，达到了本科综合论文训练的要求，同意安排论文答辩。 指导教师签字：马建荣 2021 年 6 月 8 日
评阅教师评语	论文以有限平面上的直线和椭圆曲线为核心，讨论了有限域上的代数曲线在编码理论中的应用，并基于此给出了一类基于有限平面上的椭圆曲线族构造的线性码的深入分析。在核心部分，依据数值计算提出了一系列猜想，展示了这类线性码可能具备的突出的良好基础特性，同时具备一定的纯数学背景意义。论文逻辑思路清晰、观点鲜明准确、论证内容详实，值得进一步的深入研究。 评阅教师签字：李宇翔 2021 年 6 月 9 日
答辩小组评语	论文具备较多的创新点，在呈现椭圆曲线群结构时避免了一般教材证明中的误用，还给出了有限平面上直线族和点形成的关联矩阵的秩的新证明方式，说明作者经过了独立充分的思考。论文根据大量数值计算的结果，进一步提出了一系列有价值的猜想。答辩时思路清晰、语言流畅、条理清楚，对于内容有着清晰、完整、准确的把握，对于提问的回答符合礼仪规范，回答精炼，体现了学生独立深入的见解。 答辩小组组长签字： 2021 年 6 月 10 日

总成绩：A+

教学负责人签字：

2021 年 6 月 18 日