

有限域上一类方程的解数

余杜鹃, 曹 炜*

(宁波大学 理学院, 浙江 宁波 315211)

摘要: 研究有限域 $\mathbb{F}_q$ 上一类方程

$$\beta y^{d_1} = \alpha_1 x_1^{d_2} + \alpha_2 x_2^{d_3} + \alpha_3 x_3^{d_4}, \quad \beta, \alpha_i \in \mathbb{F}_q^*, \quad d_i \in \mathbb{Z}^+$$

的解数. 在保持方程系数不变的前提下, 通过对其次数矩阵进行有效降次, 可以改进对原方程解数的各种估计. 若对方程未知变量和系数进行适当限定, 则可将其化为椭圆曲线方程, 从而利用 Hasse 定理得到原方程解数的一个精确界.

关键词: 次数矩阵; 有效降次; 椭圆曲线; Hasse 定理

中图分类号: O156

文献标志码: A

文章编号: 1001-5132 (2014) 01-0066-04

由于有限域上的方程在密码学上具有重要的应用价值, 因而一直受到人们的极大关注. 在文中, 用 $\mathbb{F}_q$ 表示含有 q 个元的有限域, 其中 $q = p^l$, $l \in \mathbb{Z}^+$, 素数 $p \neq 2, 3$. 设 f 是 $\mathbb{F}_q$ 上的 n 元 d 次多项式, 用 $N_q(f)$ 表示方程 $f = 0$ 在 $\mathbb{F}_q$ 中的解数.

早在 1936 年, Chevalley^[1]和 Warning^[2]就得到了关于 $N_q(f)$ 的 p -adic 估计, 即若 $n > d$, 则有 $p \mid N_q(f)$. Ax^[3]改进了 Chevalley-Warning 定理, 证明了 $\text{ord}_q N_q(f) \geq \lceil (n-d)/d \rceil$, 其中 $\lceil x \rceil$ 为不小于 x 的最小整数, ord_q 是 q 进制加法赋值, 即对任意的 $n \in \mathbb{N}^+$, 总存在非负整数 v , 有 $q^v \mid n$, 且 $q^{v+1} \nmid n$, 则 $\text{ord}_q n = v$, 满足 $\text{ord}_q q = 1$. Ax 还将上述结论推广到了多项式组: 设 $f_1, f_2, \dots, f_r \in \mathbb{F}_q[x_1, x_2, \dots, x_n]$, $\deg f_i \geq 1$, 用 $N_q(f_1, \dots, f_r)$ 表示 $f_1 = \dots = f_r = 0$ 在 $\mathbb{F}_q$ 中的公共零点个数, 则有:

$$\text{ord}_q N_q(f_1, \dots, f_r) \geq \left\lceil \frac{(n - \sum_{i=1}^r \deg f_i) / (\sum_{i=1}^r \deg f_i)}{1} \right\rceil.$$

Katz^[4]改进了 Ax 的结论, 证明了

$$\text{ord}_q N_q(f_1, \dots, f_r) \geq \left\lceil \frac{(n - \sum_{i=1}^r \deg f_i) / \max_{1 \leq i \leq r} \{\deg f_i\}}{1} \right\rceil.$$

Sun 等^[5], Wan 等^[6]对有限域上方方程的解数均有

研究. Cao^[7]提出了对方程次数进行有效降次的方法, 即保持方程系数不变的同时, 对方程的次数矩阵进行降次变换, 降次后的方程与原方程有相等的解数. 这一方法在许多情形下使寻求高次方程的解数变得更加简单快捷. 基于此, 笔者采用逆推法研究有限域上的一类对角方程, 使其在经过 D_p -降次以及 ω -降次后成为次数相对较低的对角方程, 从而可由 Wan^[6], Cao^[8-9], Weil^[10]等关于对角方程解数的相关结论改进对原方程解数的估计. 进而若对方程中的未知变量和系数进行适当限定, 则可将方程化为椭圆曲线方程, 从而可利用 Hasse 定理得到原方程解数的一个精确界.

1 预备知识

在有限域 $\mathbb{F}_q$ 上, 形如

$$E: y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_q \quad (1)$$

的方程称为 Weierstrass 方程. 若 $\Delta = 4a^3 + 27b^2 \neq 0$, 则由(1)式定义的平面曲线非奇异, 其上所有的点 $(x, y) \in \mathbb{F}_q^2$ 和一个无穷远点 O 组成的点集称为定义在 $\mathbb{F}_q$ 上的椭圆曲线, 记为 $E(\mathbb{F}_q)$. 在弦切律定义的加法运算下, $E(\mathbb{F}_q)$ 中所有点构成一个有限 Abel 群. 用 $|E(\mathbb{F}_q)|$ 表示 $E(\mathbb{F}_q)$ 中点的个数, 则有:

收稿日期: 2013-04-30.

宁波大学学报(理工版) 网址: <http://journalg.nbu.edu.cn/>

基金项目: 宁波市自然科学基金 (2012A610034).

第一作者: 余杜鹃 (1988-), 女, 江西上饶人, 在读硕士研究生, 主要研究方向: 数论与密码. E-mail: pinganjiankangydj@163.com

*通信作者: 曹 炜 (1974-), 男, 湖北潜江人, 博士/副研究员, 主要研究方向: 数论、有限域及其应用. E-mail: caowei@nbu.edu.cn

引理 1^[11] $|E(\mathbb{F}_q)| = q + 1 - t_q$, 其中 $|t_q| \leq 2\sqrt{q}$.

注 1 Hasse 定理后被 Weil 推广到有限域的一般曲线上. Weil-Hasse 定理是代数几何中的一个深刻结论, 它说明黎曼猜想对于函数域是成立的(但对于数域上的黎曼猜想至今仍无法证明).

设多项式 $h_1, \dots, h_r \in \mathbb{F}_q[x_1, \dots, x_n, z_1, \dots, z_t]$, 多项式中所有含 z_i 的项为 $b_i z_i^{l_i}$, $b_i \in \mathbb{F}_q^*$, $l_i \geq 1$, 称 z_i 为独立变量. h_i 可以表示为 $h_i = h_i(X) + h_i(Z)$, $h_i(X) \in \mathbb{F}_q[x_1, \dots, x_n]$, $h_i(Z) \in \mathbb{F}_q[z_1, \dots, z_t]$. 设非空集合 $A \subset \{1, 2, \dots, n\}$, 定义 $\deg_A h_i(X) = \max\{\deg_A X^d\}$, 其中: $\max$ 取遍 $h_i(X)$ 中系数为非零的单项式: $X^d = x_1^{d_1} x_2^{d_2} \dots x_n^{d_n}$, $\deg_A X^d = \sum_{i \in A} d_i$. Cao^[7] 改进了 Ax-Katz 定理关于多项式组零点个数的估计.

引理 2^[7] 设非空集合 $A \subset \{1, 2, \dots, n\}$. 如果 $\deg_A h_i(X) > 0$, $i = 1, \dots, r$, 则

$$\text{ord}_q N_q(h_1, \dots, h_r) \geq \left\lceil \frac{|A| - \sum_{i=1}^r \deg_A h_i(X)}{\max_{1 \leq i \leq r} \{\deg_A h_i(X)\}} + \sum_{j=1}^t \frac{1}{l_j} \right\rceil,$$

特别地, 我们有:

$$\text{ord}_q N_q(h_1, \dots, h_r) \geq \left\lceil \sum_{i=1}^t 1/l_i \right\rceil - r.$$

在有限域 $\mathbb{F}_q$ 上, 设多项式

$$f(x_1, x_2, \dots, x_n) = a_1 x_1^{d_{11}} x_2^{d_{21}} \dots x_n^{d_{n1}} + \dots + a_m x_1^{d_{1m}} x_2^{d_{2m}} \dots x_n^{d_{nm}}, \quad (2)$$

其中: $a_j \in \mathbb{F}_q$, $d_{ij} \in \mathbb{Z}^+$, $1 \leq i \leq n$, $1 \leq j \leq m$. 记 $D_j = (d_{1j}, \dots, d_{nj})^T$ 为第 j 项各未知量的次数所组成的向量, 称 $D = (D_1, D_2, \dots, D_m)$ 为多项式 $f(x_1, x_2, \dots, x_n)$ 的次数矩阵.

令 $S_q(D)$ 为同余式组 $DT \equiv 0 \pmod{q-1}$ 的解集, 其中 $T = (t_1, \dots, t_m)^T$, $0 \leq t_i \leq q-1$. 定义 $g(D) := \deg f = \max\{d_{1j} + d_{2j} + \dots + d_{nj}, j = 1, \dots, m\}$.

定义 1^[12] 设 $f \in \mathbb{F}_q[x_1, x_2, \dots, x_n]$, 其次数矩阵为 $D = (d_{ij}) \in M_{n \times m}$. 称变换

$$\sigma: M_{n \times m} \rightarrow M_{n \times m}, \quad D \mapsto \sigma(D) = (\sigma(d_{ij})),$$

是多项式 $f(x_1, x_2, \dots, x_n)$ 的有效降次, 若它满足:

- (i) $S_q(D) = S_q(\sigma(D))$,
- (ii) $\text{sgn}(\sigma(d_{ij})) = \text{sgn}(d_{ij})$, $\deg(D) > \deg(\sigma(D))$.

引理 3^[12] 设 $f \in \mathbb{F}_q[x_1, x_2, \dots, x_n]$. 若 σ 是多项式 f 的有效降次, 则有:

$$N_q(f) = N_q(\sigma(f)).$$

在有限域 $\mathbb{F}_q$ 上, 形如

$$a_1 x_1^{d_1} + a_2 x_2^{d_2} + \dots + a_n x_n^{d_n} = 0, \quad a_i \in \mathbb{F}_q^*, \quad d_i \in \mathbb{Z}^+, 1 \leq i \leq n, \quad (3)$$

的方程称为对角方程. 令 $d = (d_1, d_2, \dots, d_n)$, $a^* = (a_1, a_2, \dots, a_n)$ 分别为方程(3)的次数向量和系数向量, 用 $N(d; a^*)$ 表示方程(3)在 $\mathbb{F}_q$ 上的解的个数.

引理 4^[10] 方程(3)在 $\mathbb{F}_q$ 上的解 $(x_1, \dots, x_n)$ 的个数 $N(k; a^*)$ 满足:

$$|N(d; a^*) - q^{n-1}| \leq M(q-1)q^{n/2-1}, \quad (4)$$

其中: M 表示元组 $(\chi_1, \chi_2, \dots, \chi_n)$ 的个数, $\chi_1, \chi_2, \dots, \chi_n$ 为 $\mathbb{F}_q$ 上 n 个阶整除 d_i 的非平凡特征, 但其乘积 $\chi_1 \chi_2 \dots \chi_n$ 为平凡特征.

注 2 由文献[9, 12-15]知, 引理 4 中的元组 $(\chi_1, \chi_2, \dots, \chi_n)$ 与同余式

$$\frac{x_1}{d_1} + \dots + \frac{x_n}{d_n} \equiv 0 \pmod{1}, \quad 1 \leq x_i < d_i, \quad i = 1, \dots, n,$$

的解 $(x_1, \dots, x_n)$ 存在一一对应关系, 因此引理 4 中的 M 与上述同余式的解数相等.

注 3 Sun 等^[14] 证明了 $M = 0$ 的充要条件为至少满足以下情形之一:

- (i) 对某个 d_i , 有 $\gcd(d_i, d_1 \dots d_n / d_i) = 1$,
- (ii) 若 $\{d_{i_1}, \dots, d_{i_k}\}$ ($1 \leq i_1 < \dots < i_k \leq n$) 是 $\{d_1, \dots, d_n\}$ 中全部偶数组成的集合, 则 k 是奇数, $d_{i_1}/2, \dots, d_{i_k}/2$ 两两互素且 d_{i_j} ($j = 1, \dots, k$) 与 $\{d_1, \dots, d_n\}$ 中任一个奇数互素.

2 主要结论及其证明

在有限域 $\mathbb{F}_q$ 上, 考察方程

$$C: \beta y^{d_1} = \alpha_1 x_1^{d_2} + \alpha_2 x_2^{d_3} + \alpha_3 x_3^{d_4}, \quad \beta, \alpha_i \in \mathbb{F}_q^*, \quad d_j \in \mathbb{Z}^+.$$

显而易见, 方程 C 的次数矩阵为矩阵 $D = \text{diag}(d_1, d_2, d_3, d_4)$. 用 $N_q(C)$ 表示方程 C 在 $\mathbb{F}_q$ 中解的个数, 并对次数矩阵 D 进行如下变换:

Step1 对 D 进行 D_p -降次:

$$D = \text{diag}(d_1, d_2, d_3, d_4) \xrightarrow{D_p} \text{diag}(k_1, k_2, k_3, k_4), \quad k_j = \gcd(d_j, q-1).$$

Step2 再进行 ω -降次:

$$\text{diag}(k_1, k_2, k_3, k_4) \xrightarrow{\omega} \text{diag}(w_1, w_2, w_3, w_4), \quad w_j = \gcd(k_j, \text{lcm}[k_l, l \neq j]).$$

在经过 D_p -降次及 ω -降次后, 则可得到新的方程:

$$C_1: \beta y^{w_1} = \alpha_1 x_1^{w_2} + \alpha_2 x_2^{w_3} + \alpha_3 x_3^{w_4}, \\ \beta, \alpha_i \in \mathbb{F}_q^*, w_j \in \mathbb{Z}^+.$$

同上, 用 $N_q(C_1)$ 表示方程 C_1 在 $\mathbb{F}_q$ 中解的个数. 则有:

定理 1 $N_q(C) = N_q(C_1)$.

证明 方程 C_1 的次数矩阵为 $\bar{D} = \text{diag}(w_1, w_2, w_3, w_4)$. 易证同余式组 $DT \equiv 0 \pmod{q-1}$ 和 $\bar{D}T \equiv 0 \pmod{q-1}$ 同解, 因而 D_p -降次与 ω -降次均为有效降次变换. 由引理 3 可得:

$$N_q(C) = N_q(C_1).$$

定理 2 $\text{ord}_q N_q(C) \geq \sum_{i=2}^4 \lceil 1/\omega_i \rceil - 1$.

证明 由定理 3 和引理 2 可得.

定理 3 $|N_q(C) - q^3| \leq \prod_{i=1}^4 (\omega_i - 1)q(q-1)$.

特别地, 若对某个 $1 \leq i \leq 4$, 有 $\omega_i = 1$, 则 $N_q(C) = q^3$.

证明 由定理 3、引理 4 及注 2、注 3 可得.

我们还可由定理 2 和定理 3 得到下面的结论 (证明略).

推论 1 进一步地, 若有:

- (a) $\gcd(w_1, q-1) = \gcd(w_3, q-1) = 2$,
- (b) $\gcd(w_2, q-1) = \gcd(3, q-1)$,

则有:

- (i) $q \mid N_q(C)$,
- (ii) $|N_q(C) - q^3| \leq 2(\omega_4 - 1)q(q-1)$.

下面考虑方程

$$\bar{E}: y^{\bar{r}_1} = x^{\bar{r}_2} + ax^{\bar{r}_3} + b, \quad (5)$$

其中: $a, b \in \mathbb{F}_q^*$, $r_i \in \mathbb{Z}^+$, $1 \leq i \leq 3$, 且 $4a^3 + 27b^2 \neq 0$. 显然, 方程 $\bar{E}$ 是对方程 C 的未知变量和系数进行限定而得到的. 我们将证明, 若方程 $\bar{E}$ 的次数矩阵能有效降次为 Weierstrass 方程的次数矩阵, 则可以利用 Hasse 定理得到方程 $\bar{E}$ 的解数的精确界.

定理 4 设方程 $\bar{E}$ 如(5)所示. 若方程 $\bar{E}$ 的次数 r_1, r_2, r_3 同时满足:

- (i) $\gcd(r_1, q-1) = 2$,
- (ii) $\gcd(r_3, q-1) = 1$, $r_2 \equiv 3r_3 \pmod{q-1}$,

则方程 $\bar{E}$ 在 $\mathbb{F}_q$ 中解的个数为:

$$N_q(\bar{E}) = q - t_q, \quad |t_q| \leq 2\sqrt{q}.$$

证明 易见, 方程 $\bar{E}$ 的次数矩阵为:

$$\bar{D} = \begin{pmatrix} r_1 & 0 & 0 & 0 \\ 0 & r_2 & r_3 & 0 \end{pmatrix},$$

而椭圆曲线方程 E 的次数矩阵为:

$$D = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 1 & 0 \end{pmatrix}.$$

由定义 1 可知, 若存在从方程 $\bar{E}$ 到方程 E 的有效降次, 则以矩阵 $\bar{D}$ 和 D 为系数矩阵的齐次线性方程组在剩余类环 $\mathbb{Z}_{q-1}$ 中同解, 即

(a) $r_1 t_1 \equiv 0 \pmod{q-1}$ 与 $2t_1 \equiv 0 \pmod{q-1}$ 同解, 且

(b) $r_2 t_2 + r_3 t_3 \equiv 0 \pmod{q-1}$ 与 $3t_2 + t_3 \equiv 0 \pmod{q-1}$ 同解.

不难证明, r_1, r_2, r_3 同时满足下列条件即可:

- (i) $\gcd(r_1, q-1) = \gcd(2, q-1) = 2$,
- (ii) $r_2 - 3r_3 \equiv 0 \pmod{q-1}$, 且 $\gcd(r_3, q-1) = 1$.

注意到在 Hasse 定理中, 有限域 $\mathbb{F}_q$ 上椭圆曲线是射影平面上的点集, 由 $(x, y) \in \mathbb{F}_q^2$ 和一个无穷远点 O 组成. 而方程 $\bar{E}$ 的解集在不存在无穷远点 O 的笛卡尔平面直角坐标系中. 由 Hasse 定理, 可知方程 $\bar{E}$ 在 $\mathbb{F}_q$ 中的解的个数满足:

$$N_q(\bar{E}) = q - t_q,$$

其中 $|t_q| \leq 2\sqrt{q}$.

定理证毕.

参考文献:

- [1] Chevalley C. Démonstration d'une hypothèse de M Artin Abh[J]. Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg, 1936, 11(1):73-75.
- [2] Warning E. Bemerkung zur vorstehenden Arbeit[J]. Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg, 1936, 11(1):76-83.
- [3] Ax J. Zeroes of polynomials over finite fields[J]. American Journal of Mathematics, 1964, 86(2):255-261.
- [4] Katz N M. On a theorem of Ax[J]. American Journal of Mathematics, 1971, 93(2):485-499.
- [5] Sun Q, Yuan P Z. On the number of solutions of diagonal equations over a finite field[J]. Finite Fields and Their Applications, 1996, 2(1):35-41.
- [6] Wan D Q. Zeros of diagonal equations over finite fields[J]. American Mathematical Society, 1988, 103(4):

- 1049-1052.
- [7] Cao W. A partial improvement of the Ax-Katz theorem[J]. Journal of Number Theory, 2012, 132(4): 485-494.
- [8] Cao W. A reduction for counting the number of zeros of general diagonal equation over finite fields[J]. Finite Fields and Their Applications, 2006, 12(4):681-692.
- [9] 柯召, 孙琦. 数论讲义(下)[M]. 北京: 高等教育出版社, 2003:72-80.
- [10] Weil A. Numbers of solutions of equations in finite fields[J]. American Mathematical Society, 1949, 55:497-508.
- [11] Hoffstein J, Pipher J, Silverman J H. An introduction to mathematical cryptography[M]. New York: Springer, 2008.
- [12] Cao W. A special degree reduction of polynomials over finite fields with applications[J]. International Journal of Number Theory, 2011, 7(4):1093-1102.
- [13] Andrew G, Shu G L, Sun Q. On the number of solutions to the equation $\sum_{i=1}^n x_i / d_i \equiv 0 \pmod{1}$ [J]. 四川大学学报: 自然科学版, 1995, 32(3):243-248.
- [14] Sun Q, Wan D Q. On the solvability of the equation $\sum_{i=1}^n x_i / d_i \equiv 0 \pmod{1}$ and its application[J]. American Mathematical Society, 1987, 100(2):220-224.
- [15] Sun Q, Wan D Q. On the diophantine equation $\sum_{i=1}^n x_i / d_i \equiv 0 \pmod{1}$ [J]. American Mathematical Society, 1991, 112(1):25-29.

Number of Solutions to a Class of Equations over Finite Fields

YU Du-juan, CAO Wei *

(Faculty of Science, Ningbo University, Ningbo 315211, China)

Abstract: We study the number of solutions to the following equation:

$$\beta y^{d_1} = \alpha_1 x_1^{d_2} + \alpha_2 x_2^{d_3} + \alpha_3 x_3^{d_4}, \quad \beta, \alpha_i \in \mathbb{F}_q^*, \quad d_i \in \mathbb{Z}^+.$$

While keeping the coefficients unchanged, we effectively reduce the degree matrix to improve the estimates on the number of solutions to the equation. Furthermore with certain constraint conditions on the variables and coefficients, we obtain a sharp bound on the number of solutions to the equation using Hasse's theorem for elliptic curves over finite fields.

Key words: degree matrix; effective reduction; elliptic curve; Hasse's theorem

(责任编辑 史小丽)