

高斯和与有理点的计算

姜 坤, 高 伟, 曹 炜*

(宁波大学 数学与统计学院, 浙江 宁波 315211)

摘要: 计算有限域上代数簇有理点个数是有限域研究中的重要课题. 设 $\mathbb{F}_q$ 为 q 元有限域, f 是 $\mathbb{F}_q$ 上的非零多项式, D_f 为其次数矩阵, 用 $N(f)$ 表示超曲面 $f=0$ 在 $\mathbb{F}_q$ 上的有理点个数. 若 D_f 在剩余类环 $\mathbb{Z}/(q-1)\mathbb{Z}$ 中与整数矩阵 A 行等价, 则记为 $D_f \sim_q A$. 利用高斯和给出了当 $D_f \sim_q \text{diag}(\lambda_1, \dots, \lambda_m)$, 其中 $\lambda_i \in \{1, p_1\}$, p_1 为 $q-1$ 的一个素因子时 $N(f)$ 的具体表达式, 从而推广了已知的结论.

关键词: 有限域; 有理点; 高斯和; 特征

中图分类号: O156.1

文献标志码: A

文章编号: 1001-5132 (2020) 01-0065-04

设 $\mathbb{F}_q$ 为 q 元有限域, 其中 $q = p^h$, $h \geq 1$, p 是素数. $\mathbb{N}_0$ 表示非负整数集. 对于 $\mathbb{F}_q$ 上的非零多项式

$$f(x_1, \dots, x_n) = a_1 x_1^{d_{11}} \cdots x_n^{d_{n1}} + \cdots + a_m x_1^{d_{1m}} \cdots x_n^{d_{nm}}, \quad a_i \in \mathbb{F}_q^*, d_{ij} \in \mathbb{N}_0, \quad (1)$$

简记为:

$$f(x_1, \dots, x_n) = \sum_{j=1}^m a_j X^{D_j},$$

其中:

$$D_j = (d_{1j}, \dots, d_{nj})^T \in \mathbb{N}_0^n, X^{D_j} = x_1^{d_{1j}} \cdots x_n^{d_{nj}},$$

则多项式 f 的次数矩阵定义为:

$$D_f = (D_1, \dots, D_m) = (d_{ij}) \in \mathbb{N}_0^{n \times m},$$

f 的增广次数矩阵定义为:

$$\tilde{D}_f = (\tilde{D}_1, \dots, \tilde{D}_m) \in \mathbb{N}_0^{(n+1) \times m},$$

其中:

$$\tilde{D}_j = (1, D_j)^T.$$

用 $N(f)$ 表示超曲面 $f=0$ 在仿射空间 $\mathbb{A}^n(\mathbb{F}_q)$ 中确定的 $\mathbb{F}_q$ -有理点的个数, 即

$$N(f) = \#\{(x_1, \dots, x_n) \in \mathbb{A}^n(\mathbb{F}_q) \mid f(x_1, \dots, x_n) = 0\}.$$

计算 $N(f)$ 的具体值是有限域研究中的重要课题^[1-8]. 对于 2 个同型整数矩阵 A 和 B , 若 A 中所有元素均为正整数, 则记为 $A > 0$, 若在环 $\mathbb{Z}/(q-1)\mathbb{Z}$ 中 A 与 B 行等价, 则记为 $A \sim_q B$.

文献[1]证明了定理 1.

定理 1^[1] 设多项式 f 如式(1)所示, 且

$$0 < D_f \sim_q \Lambda = \text{diag}(\overbrace{1, \dots, 1}^m),$$

则有:

$$N(f) = N_0 \triangleq q^n - \frac{(q-1)^{n-m+1}}{q} ((q-1)^m - (-1)^m). \quad (2)$$

注 1 定理 1 中用 N_0 表示式(2)中右边的表达式.

令 η 为 $\mathbb{F}_q^*$ 上的二次特征, 即对 $a \in \mathbb{F}_q^*$, 定义 $\eta(a) = 1$, 若存在 $c \in \mathbb{F}_q^*$, 使 $a = c^2$, 否则 $\eta(a) = -1$. 用 $\lfloor \cdot \rfloor$ 表示向下取整函数. 文献[2]利用二次特征和高斯和证明了定理 2.

定理 2^[2] 设多项式 f 如式(1)所示, 且

$$0 < D_f \sim_q \Lambda = \text{diag}(\overbrace{2, \dots, 2}^{t_1}, \overbrace{1, \dots, 1}^{m-t_1}),$$

并满足:

$$t_1 \geq 1, t_1 \geq t_2 \geq 0, \eta(a_1) = \cdots = \eta(a_{t_2}) = -1,$$

$$\eta(a_{t_2+1}) = \cdots = \eta(a_{t_1}) = 1,$$

则

(i) 若 $q \equiv 1 \pmod{4}$ 有:

$$N(f) = q^n - \frac{(-1)^m (q-1)^{n+1-m}}{q}.$$

$$\left((1-q)^m - 1 - \sum_{j=1}^{\lfloor t_1/2 \rfloor} \sum_{y=0}^{t_2} \binom{t_2}{y} \binom{m-t_2}{2j-y} (-1)^y q^j \right).$$

(ii) 若 $q \equiv 3 \pmod{4}$ 有:

$$N(f) = q^n - \frac{(-1)^m (q-1)^{n+1-m}}{q}.$$

$$\left((1-q)^m - 1 - \sum_{j=1}^{\lfloor t_1/2 \rfloor} \sum_{y=0}^{t_2} \binom{t_2}{y} \binom{m-t_2}{2j-y} (-1)^y (-q)^j \right).$$

考虑定理 2 的一般情形, 给出当

$$0 < \mathbf{D}_f \sim_q \mathbf{A} = \text{diag}(\overbrace{p_1, \dots, p_1}^{m_{p_1}}, \overbrace{1, \dots, 1}^{m-m_{p_1}}),$$

其中: p_1 为 $q-1$ 素因子时 $N(f)$ 的具体表达式.

1 预备知识

设 $a \in \mathbb{F}_q^*$, g 是 $\mathbb{F}_q^*$ 的一个生成元, 则存在唯一的正整数 $1 \leq t \leq q-1$, 使得 $g^t = a$, 记 $\text{ind}_g a = t$.

定义 $\mathbb{F}_q^*$ 上的 Teichmüller 特征 χ 满足:

$$\chi(a) = e^{2\pi i \text{ind}_g a / (q-1)},$$

则 $\mathbb{F}_q^*$ 上的所有特征均可由 χ 生成, 即

$$\hat{\mathbb{F}}_q^* = \{\chi^k : k=0, 1, \dots, q-2\},$$

其中: χ^k 在 $\hat{\mathbb{F}}_q^*$ 中的阶为 $(q-1) / \gcd(q-1, k)$.

设 p_1 为 $q-1$ 的素因子, 令

$$\psi = \chi^{(q-1)/p_1}, \theta = e^{2\pi i / p_1}, \text{ 则有:}$$

$$\psi(a) = \theta^{\text{ind}_g a}.$$

令 $\varsigma_p = e^{2\pi i / p}$, Tr 为从 $\mathbb{F}_q$ 到素域 $\mathbb{F}_p$ 上的绝对迹映射, 对于 $1 \leq k \leq q-2$, 定义高斯和为:

$$G(k) = \sum_{a \in \mathbb{F}_q^*} \chi(a)^{-k} \varsigma^{\text{Tr}(a)},$$

当 $k=0, q-1$ 时, 定义 $G(0) = q-1, G(q-1) = -q$.

为将 Teichmüller 特征 χ 推广到 $\mathbb{F}_q$ 上, 定义

$$\chi^0(0) = 0, \chi^i(0) = 0.$$

若 $t > 0$, 可验证对所有的 $a \in \mathbb{F}_q$, 高斯和满足下面的插值关系:

$$\varsigma^{\text{Tr}(a)} = \sum_{k=0}^{q-1} \frac{G(k)}{q-1} \chi(a)^k.$$

引理 1^[2] 设多项式 f 如式(1)所示. 令

$$\Omega = \{0, 1, \dots, q-1\},$$

对于 $\mathbf{k} = (k_1, \dots, k_m) \in \Omega^m$, 用 $s(\mathbf{k})$ 表示 $\tilde{\mathbf{D}}_f \mathbf{k}$ 中非零元的个数, 则有:

$$N(f) = \sum_{\tilde{\mathbf{D}}_f \mathbf{k} \equiv 0 \pmod{q-1}} \frac{(q-1)^{s(\mathbf{k})} q^{n-s(\mathbf{k})}}{(q-1)^m} \prod_{j=1}^m \chi(a_j)^{k_j} G(k_j). \quad (3)$$

引理 2^[3] 设 $M > 2$ 为正整数, 存在一个最小的正整数 u , 使得 $p^u \equiv -1 \pmod{M}$. 令

$$q = p^{2uv}, v \in \mathbb{Z}_+,$$

若 $M = (q-1) / \gcd(q-1, k)$, $0 \leq k \leq q-2$, 则有:

$$G(k) = \begin{cases} \sqrt{q}(-1)^{v-1}, & p=2, \\ \sqrt{q}(-1)^{v-1+\frac{v(p^u+1)}{M}}, & p>2. \end{cases} \quad (4)$$

当 $M = p_1$ 为素数时, 对于 $k_i = i(q-1) / p_1$, $i=1, \dots, p_1-1$, 有 $M = (q-1) / \gcd(q-1, k_i) = p_1$.

于是由引理 2 可得引理 3.

引理 3 设存在一个最小的正整数 u , 使得 $p^u \equiv -1 \pmod{p_1}$.

令 $q = p^{2uv}, v \in \mathbb{Z}_+$. 对于

$$k_i = i(q-1) / p_1, i=1, \dots, p_1-1, \text{ 有:}$$

$$g := G(k) = \begin{cases} \sqrt{q}(-1)^{v-1}, & p=2, \\ \sqrt{q}(-1)^{v-1+\frac{v(p^u+1)}{p_1}}, & p>2. \end{cases} \quad (5)$$

由二项式定理可得引理 4.

引理 4 设 $r \in \mathbb{Z}_+$, 则有:

$$\sum_{i=0}^r \binom{r}{i} (-q)^i (q-1)^{r-i} = (-1)^r.$$

2 主要结论

假设 f 是形如式 (1) 的多项式, $q = p^{2uc}$, 且存在一个最小的正整数 u , 使得 $p^u \equiv -1 \pmod{p_1}$, 并有:

$$0 < \mathbf{D}_f \sim_q \mathbf{\Lambda} = \text{diag}(\overbrace{p_1, \dots, p_1}^{m_{p_1}}, \overbrace{1, \dots, 1}^{m-m_{p_1}}).$$

令系数多重集合 $S_{m_{p_1}} = \{a_1, \dots, a_{m_{p_1}}\}$,

设

$$\Omega \subseteq \{0, 1, \dots, q-1\}, \mathbf{k} = (k_1, \dots, k_m) \in \Omega^m,$$

$$1 \leq i \leq p_1, \quad 0 \leq j \leq p_1,$$

$$0 = m_0 \leq m_1 \leq \dots \leq m_{p_1} \leq m,$$

对系数多重集合 $S_{m_{p_1}}$ 及向量 $\mathbf{k}$ 分量进行如下划分:

$$(i) t \in \{m_{i-1} + 1, \dots, m_i\}, \psi(a_t) = \theta^i,$$

$$(ii) \mathbf{k} \text{ 中所对应的元素记为 } \mathbf{k}_i = (k_{m_{i-1}+1}, \dots, k_{m_i}).$$

令 $t_i^{(j)}(\mathbf{k})$ 表示 $\mathbf{k}_i$ 中分量取值为 $j(q-1)/p_1$ 的个数. 定义 $\sigma_j(\mathbf{k}) = t_1^{(j)}(\mathbf{k}) + \dots + t_{p_1}^{(j)}(\mathbf{k})$, 即在 $(k_1, \dots, k_{m_{p_1}})$ 中分量取值为 $j(q-1)/p_1$ 的个数.

定理 3 如前所设, 有:

$$N(f) = N_0 + (-1)^{m-m_{p_1}} q^{-1} (q-1)^{n+1-m}.$$

$$\sum \theta^{\sum_{i=1}^{p_1-1} \sum_{j=1}^{p_1-1} j t_i^{(j)}} g^{\sum_{i=1}^{p_1-1} \sigma_i(\mathbf{k})} (-q)^{\sigma_{p_1}(\mathbf{k})} (q-1)^{\sigma_0(\mathbf{k})},$$

其中: 和号遍历所有的向量 $\mathbf{k} = (k_1, \dots, k_m) \in \Omega^m$, 且满足:

$$0 \leq \sigma_0(\mathbf{k}) + \sigma_{p_1}(\mathbf{k}) < m_{p_1},$$

$$\sum_{j=1}^{p_1-1} j \sigma_j(\mathbf{k}) \equiv 0 \pmod{p_1}.$$

证明 若 $\sigma_0(\mathbf{k}) + \sigma_{p_1}(\mathbf{k}) = m_{p_1}$, 则 $\mathbf{k} = (k_1, \dots, k_m)$ 中取值只有 $q-1$ 和 0 , 此情形下的解数为定理 1 中的 N_0 .

下设 $\sigma_0(\mathbf{k}) + \sigma_{p_1}(\mathbf{k}) < m_{p_1}$. 由于

$$\mathbf{D}_f \sim_q \mathbf{\Lambda} = \text{diag}(\overbrace{p_1, \dots, p_1}^{m_{p_1}}, \overbrace{1, \dots, 1}^{m-m_{p_1}}),$$

同余方程

$$\mathbf{D}_f \mathbf{k}^T \equiv 0 \pmod{q-1}, \mathbf{\Lambda} \mathbf{k}^T \equiv 0 \pmod{q-1},$$

同解, 且后者的解均取自

$$\mathbf{k} = (k_1, \dots, k_m) \in \Omega^m,$$

这里 $\Omega = \{i(q-1)/p_1 : i = 0, 1, \dots, p_1\}$.

对任一给定的 $\mathbf{k} = (k_1, \dots, k_m) \in \Omega^m$, 由同余方程 $\tilde{\mathbf{D}}_f \mathbf{k}^T \equiv 0 \pmod{q-1}$, 可知 $\sum_{j=1}^{p_1-1} j \sigma_j(\mathbf{k})$ 一定是 p_1 的倍数, 故有 $\sum_{j=1}^{p_1-1} j \sigma_j(\mathbf{k}) \equiv 0 \pmod{p_1}$. 又由 $0 < \mathbf{D}_f$ 知 $s(\mathbf{k}) = n+1$. 对于 $\sigma_0(\mathbf{k})$ 和 $\sigma_{p_1}(\mathbf{k})$, 有:

$$(i) k = 0 \text{ 时, } \chi(a_j)^k = 1, G(k) = q-1,$$

$$(ii) k = q-1 \text{ 时, } \chi(a_j)^k = 1, G(k) = -q,$$

故由引理 1 和引理 3 得:

$$N(f) = q^{-1} (q-1)^{n+1-m} \sum \theta^{\sum_{i=1}^{p_1-1} \sum_{j=1}^{p_1-1} j t_i^{(j)}} g^{\sum_{i=1}^{p_1-1} \sigma_i(\mathbf{k})}.$$

$$(-q)^{\sigma_{p_1}(\mathbf{k})} (q-1)^{\sigma_0(\mathbf{k})} \sum_{r=0}^{m-m_{p_1}} \binom{m-m_{p_1}}{r} (-q)^r.$$

$$(q-1)^{m-m_{p_1}-r},$$

其中: 和号遍历所有的向量 $\mathbf{k} = (k_1, \dots, k_m) \in \Omega^m$, 且满足:

$$0 \leq \sigma_0(\mathbf{k}) + \sigma_{p_1}(\mathbf{k}) < m_{p_1},$$

$$\sum_{j=1}^{p_1-1} j \sigma_j(\mathbf{k}) \equiv 0 \pmod{p_1},$$

又由引理 4 可得:

$$\sum_{r=0}^{m-m_{p_1}} \binom{m-m_{p_1}}{r} (-q)^r (q-1)^{m-m_{p_1}-r} = (-1)^{m-m_{p_1}},$$

定理得证.

注意到, 当系数多重集合 $S_{m_{p_1}}$ 中的元素均为 1 时, 有 $\psi(a) = \theta^{\text{ind}_{s^a}} = 1, \forall a \in S_{m_{p_1}}$. 因而定理 3 可以有如下相对比较简洁的形式.

推论 1 如前所设, 若系数多重集合 $S_{m_{p_1}}$ 中的元素均为 1, 则有:

$$N(f) = N_0 + (-1)^{m-m_{p_1}} q^{-1} (q-1)^{n+1-m}.$$

$$\sum g^{\sum_{i=1}^{p_1-1} \sigma_i(\mathbf{k})} (-q)^{\sigma_{p_1}(\mathbf{k})} (q-1)^{\sigma_0(\mathbf{k})},$$

其中: 和号遍历所有的向量 $\mathbf{k} = (k_1, \dots, k_m) \in \Omega^m$, 且满足:

$$0 \leq \sigma_0(\mathbf{k}) + \sigma_{p_1}(\mathbf{k}) < m_{p_1},$$

$$\sum_{j=1}^{p_1-1} j \sigma_j(\mathbf{k}) \equiv 0 \pmod{p_1}.$$

例 求方程 $f=0$ 在 $\mathbb{F}_{16}$ 中解的个数.

$$f(x_1, \dots, x_5) = x_1^5 x_2^5 x_3^5 x_4^5 x_5^5 + x_1^5 x_2^{10} x_3^5 x_4^5 x_5^5 + \\ x_1^5 x_2^5 x_3^{10} x_4^5 x_5^5 + x_1^5 x_2^5 x_3^5 x_4^{10} x_5^5 + x_1^5 x_2^5 x_3^5 x_4^5 x_5^{10},$$

易知:

$$q=16, p_1=5, \mathbf{D}_f \sim_q \text{diag}(5, 5, 5, 5, 5), \\ \varphi(a_1) = \varphi(a_2) = \varphi(a_3) = \varphi(a_4) = \varphi(a_5) = 1, \\ m_1 = m_2 = m_3 = m_4 = 0, \\ m_5 = m = n = 5.$$

又由引理 3 得 $g=4$, 应用推论 1 可计算得:

$$N(f)=476701,$$

通过 Maple 计算, 与该结果一致.

参考文献:

- [1] Cao W, Sun Q. On a class of equations with special degrees over finite fields[J]. Acta Arithmetica, 2007, 130(2):195-202.
- [2] Wang R Y, Wen B B, Cao W. Degree matrices and enumeration of rational points of some hypersurfaces over finite fields[J]. Journal of Number Theory, 2017, 177:91-99.
- [3] Berndt B, Evans R, Williams K. Gauss and Jacobi Sums[M]. New York: Wiley-Interscience, 1998:362-368.
- [4] Lidl R, Niederreiter H. Finite Fields[M]. Reading, MA: Addison-Wesley, 1983:186-204.
- [5] Cao W, Han S M, Wang R Y. Rational points on Fermat curves over finite fields[EB/OL]. [2019-03-10]. <https://doi.org/10.1142/S0219498817500463>.
- [6] Zan H X, Cao W. Powers of polynomials and bounds of value sets[J]. Journal of Number Theory, 2014, 143:286-292.
- [7] Zhu M L, Cao W. Invariant factors of degree matrices and L-functions of certain exponential sums[J]. Finite Fields and Their Applications, 2014, 28:188-198.
- [8] Pan X L, Zhao X R, Cao W. A problem of Carlitz and its generalizations[J]. Archiv der Mathematik, 2014, 102(4): 337-343.

Gauss sums and computation of rational points

JIANG Kun, GAO Wei, CAO Wei*

(School of Mathematics and Statistics, Ningbo University, Ningbo 315211, China)

Abstract: It is important in the area of finite fields study to compute the number of rational points on algebraic varieties in finite fields. Let $\mathbb{F}_q$ be the finite field of order q and f be a nonzero polynomial over $\mathbb{F}_q$ with degree matrix $\mathbf{D}_f$; denote by $N(f)$ the number of $\mathbb{F}_q$ -rational points of the hypersurface defined by $f=0$; write $\mathbf{D}_f \sim_q \mathbf{A}$ when $\mathbf{D}_f$ is row equivalent to an integer matrix $\mathbf{A}$ in the residue ring $\mathbb{Z}/(q-1)\mathbb{Z}$. Using Gauss sums, we obtain the explicit formula for $N(f)$ in the case of $\mathbf{D}_f \sim_q \text{diag}(\lambda_1, \dots, \lambda_m)$, where $\lambda_i \in \{1, p_1\}$ and p_1 is a prime divisor of $q-1$, which generalizes the known results.

Key words: finite field; rational point; Gauss sum; character

(责任编辑 史小丽)