文章编号:0583-1431(2007)02-0357-06 **文献标识码:A**

有限域上由一组对角多项式确定的簇中的点

曹 炜

四川大学数学学院 成都 610064
E-mail: caowei433100@vip.sina.com

摘 要 设 F_q 为有限域, $f_i(x) = a_{i1}x_1^{d_{i1}} + \cdots + a_{in}x_n^{d_{in}} + c_i$ $(i = 1, \ldots, m)$ 为 F_q 上一组对角多项式, 用 $N(V)$ 表示由 f_i $(i = 1, \ldots, m)$ 确定的簇中的 F_q- 有理点的个数. 通过应用 Adolphson 和 Sperber 所引进的牛顿多面体方法, 证明了 $\mathrm{ord}_q N(V) \geqslant \lceil \frac{1}{d_1} + \ldots + \frac{1}{d_n} \rceil - m$, 其中 $d_i = \max\{d_{1i}, \ldots, d_{mi}\}$. 该结果在许多情形下可以改进 Ax–Katz 定理, 并推广了 Wan 在 $m = 1$ 时得到的一个定理, 而且我们对 Wan 的定理给出了一个不同的证明.

关键词 有限域; 对角多项式; 牛顿多面体
MR(2000) 主题分类 11H06, 52C07, 14G05
中图分类 O156.1

Points on the Variety Defined by a System of Diagonal Polynomials over Finite Fields

Wei CAO

Department of Mathematics, Sichuan University, Chengdu 610064, *P. R. China*
*E-mail: caowei*433100*@vip.sina.com*

Abstract Let F_q be the finite field, and let $N(V)$ denote the number of F_q-rational points on the variety defined by the diagonal polynomials over F_q: $f_i(x) = a_{i1}x_1^{d_{i1}} + \cdots + a_{in}x_n^{d_{in}} + c_i$, $i = 1, \ldots, m$. By using the Newton polyhedra technique introduced by Adolphson and Sperber, we show that $\mathrm{ord}_q N(V) \geqslant \lceil \frac{1}{d_1} + \cdots + \frac{1}{d_n} \rceil - m$ with $d_i = \max\{d_{1i}, \ldots, d_{mi}\}$, which can improve the Ax–Katz theorem in many cases. This generalizes Wan's theorem for the case $m = 1$. Moreover, we provide a different proof to Wan's theorem.

Keywords finite field; diagonal polynomial; Newton polyhedron
MR(2000) Subject Classification 11H06, 52C07, 14G05
Chinese Library Classification O156.1

1 引言及定理

设 F_q 为 q 元有限域, 其特征为 p, F_q^* 为它的乘法群. 设 $f_i(x_1, \ldots, x_n)$ $(i = 1, \ldots, m)$ 为 $F_q[x_1, \ldots, x_n]$ 中一组多项式, 用 V 表示由 f_i $(i = 1, \ldots, m)$ 在 F_q 中的公共零点所确定的簇. 用

收稿日期: 2005-07-07; 接受日期: 2006-03-30
基金项目: 国家自然科学基金 (10128103) 部分资助

$N(V)$ 表示 V 中 F_q- 有理点的个数, 即

$$N(V)=\#\{(x_1,\dots,x_n)\in F_q^n \mid f_i(x_1,\dots,x_n)=0,\ i=1,\dots,m\}.$$

关于 $N(V)$ 的 p- 整除性有大量的研究. 其中经典的 Chevalley–Warning 定理是说：如果 $n>\sum_{i=1}^m \deg f_i$, 则有 $p\,|\,N(V)$. 设 x 为一实数, 令 $\lceil x\rceil$ 表示 $\geqslant x$ 的最小整数. 令 ord_q 表示满足 $\mathrm{ord}_q q=1$ 的加法赋值函数. 1964 年, Ax [1] 证明了

$$\mathrm{ord}_q N(V)\geqslant \max\left\{\left\lceil\frac{n-\sum_{i=1}^m \deg f_i}{\sum_{i=1}^m \deg f_i}\right\rceil,\ 0\right\}.$$

这极大地改进了 Chevalley–Warning 定理. 在有关编码理论的启示下, Ward [2] 发现了 $m=1$ 时 Ax 定理的一种新的证明方法. 1971 年, Katz [3] 又进一步证明了

$$\mathrm{ord}_q N(V)\geqslant \max\left\{\left\lceil\frac{n-\sum_{i=1}^m \deg f_i}{\max_{1\leqslant i\leqslant m}\deg f_i}\right\rceil,\ 0\right\}. \tag{1}$$

Wan [4, 5] 对 Ax–Katz 定理分别给出了两种不同的证明. 最近, Hou [6] 通过将一组方程上的 Ax–Katz 定理简约为单个方程的 Ax 定理而得到了一个新的证明.

虽然 Ax–Katz 定理有可能达到最佳, 即在 (1) 式中可取等号, 但它在一些特殊情形下还是可以改进的. 设簇 V 是由下面 F_q 上单个对角多项式确定的

$$f(x)=a_1x_1^{d_1}+a_2x_2^{d_2}+\cdots+a_nx_n^{d_n}+c, \tag{2}$$

其中 $1\leqslant d_i\,|\,(q-1)$, $a_i\in F_q^*$ $(i=1,\dots,n)$, $c\in F_q$. Morlaye [7] 和 Joly [8] (参见文 [9, 297–298] 页) 证明了 $p\,|\,N(V)$ 如果下面的条件成立

$$\frac{1}{d_1}+\frac{1}{d_2}+\cdots+\frac{1}{d_n}>1.$$

利用关于高斯和的 Stickelberger 定理, 并通过复杂的计算, Wan [10] 改进了关于单个对角多项式的 Ax–Katz 定理和 Morlaye–Joly 定理：

定理 1.1[10] 设簇 V 由 (2) 式所确定, 则有

$$\mathrm{ord}_q N(V)\geqslant\left\lceil\frac{1}{d_1}+\frac{1}{d_2}+\cdots+\frac{1}{d_n}\right\rceil-1. \tag{3}$$

本文将考虑 F_q 上一组对角多项式

$$\begin{cases} f_1(x)=a_{11}x_1^{d_{11}}+a_{12}x_2^{d_{12}}+\cdots+a_{1n}x_n^{d_{1n}}+c_1,\\ \qquad\vdots\\ f_m(x)=a_{m1}x_1^{d_{m1}}+a_{m2}x_2^{d_{m2}}+\cdots+a_{mn}x_n^{d_{mn}}+c_m, \end{cases} \tag{4}$$

其中 $a_{ij}\in F_q^*$, $c_i\in F_q$ 且 d_{ij} 均为正整数. 我们的主要结果是:

定理 1.2 设簇 V 由 (4) 式所确定. 令 $d_j=\max\{d_{ij}\,|\,1\leqslant i\leqslant m\}$ for $1\leqslant j\leqslant n$, 则有

$$\mathrm{ord}_q N(V)\geqslant\max\left\{\left\lceil\sum_{j=1}^n\frac{1}{d_j}\right\rceil-m,\ 0\right\}. \tag{5}$$

Wolfmann [11] 研究了当 (4) 式中所有 d_{ij} 都相同的的特殊情形. 我们将研究更为广泛的情形. 通过应用 Adolphson 和 Sperber 所引进的牛顿多面体方法, 我们不但把 Wan 的定理推广到了对角多项式组中去, 而且对 Wan 在 $m=1$ 时所得到的结论给出了一种不同的证明.

2 牛顿多面体

本节先简单介绍一下由 Adolphson 和 Sperber 所引进的牛顿多面体理论 (见文 [12] 和 [13]). 照例, 用 $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ 和 $\mathbb{N}$ 分别表示实数集、有理数集、整数集和非负整数集.

对于 F_q 上一个给定的多项式 $f(x_1,\dots,x_n)$, 记 $f=\sum_{j\in J}a_j\mathbf{X}^j$, 这里 J 是 $\mathbb{N}^n$ 中的一个有限集. 令 $\Delta(f)$ 为 f 的牛顿多面体, 它是集 $J\cup\{(0,\dots,0)\}$ 在 $\mathbb{R}^n$ 中的凸包. 设 $\omega(f)$ 为使得 $\omega(f)\Delta(f)$ 包含一个格点的最小正有理数. 这里的格点是指 $\mathbb{R}^n$ 中所有坐标均为正整数的点. Adolphson 和 Sperber [12] 证明了: 如果 f 不是一个变量属于 $x_1,\dots,x_n$ 的某个真子集的多项式, 则下面的指数和

$$S(f)=\sum_{x_1,\dots,x_n\in F_q}\Psi(f(x_1,\dots,x_n))$$

(其中 Ψ 是定义在 F_q 上的一个非平凡的加法特征) 满足

$$\mathrm{ord}_q S(f)\geqslant\omega(f). \tag{6}$$

Adolphson 和 Sperber [12] 还给出了如何确定 $\omega(f)$ 的一个方法. 令 $\mathscr{A}$ 为一个 $n\times|J|$ 矩阵, 其列向量为 $j=(j_1,\dots,j_n)\in J$. 对于给定的 $r\in\mathbb{N}^n$, 考虑下面的矩阵方程

$$\mathscr{A}\begin{pmatrix}u_1\\ \vdots\\ u_{|J|}\end{pmatrix}=\begin{pmatrix}r_1\\ \vdots\\ r_n\end{pmatrix}. \tag{7}$$

定义一个权函数 $w_f(r)$ 为

$$w_f(r)=\inf\{u_1+\cdots+u_{|J|}\}, \tag{8}$$

其中 inf 取遍方程 (7) 的所有非负有理解 $u=(u_1,\dots,u_{|J|})$; 若无此解, 记 $w_f(r)=+\infty$.

关于 w_f 有一个几何上的解释. 令 $\mathbb{R}^+\langle f\rangle$ 为 $\mathbb{R}^n$ 中的一个子集, 它由 J 中元取非负实数为系数的所有线性组合组成. 这样 $\mathbb{R}^+\langle f\rangle$ 可以看作是所有以原点为始点并经过 $\Delta(f)$ 的射线的并. 方程 (7) 有一个非负有理解 u 当且仅当 $r\in\mathbb{R}^+\langle f\rangle$, 故 $w_f(r)=+\infty$ 当且仅当 $r\notin\mathbb{R}^+\langle f\rangle$. 若 $r\in\mathbb{R}^+\langle f\rangle$, 则从原点出发并通过 r 的射线与 $\Delta(f)$ 在其不包含原点的一个面相交. 设 $\sum_{i=1}^n\alpha_iX_i=1$ 为通过该面的超平面的方程 (这个超平面并不唯一确定, 除非它具有维数 $n-1$). 由线性规划中的经典结果可知

$$w_f(r)=\sum_{i=1}^n\alpha_ir_i. \tag{9}$$

这样, 我们就得到了

$$\omega(f)=\min_{r\in(\mathbb{Z}^+)^n}\{w_f(r)\}. \tag{10}$$

现令 V 为由 F_q 上一组多项式 $f_1,\dots,f_m$ 在 F_q 中的公共零点所确定的簇, $N(V)$ 为 V 中 F_q- 有理点的个数. 我们有下面熟知的关于加法特征和的性质

$$\sum_{y\in F_q}\Psi(yx)=\begin{cases}0, & x\in F_q^*,\\ q, & x=0,\end{cases}$$

从而易得

$$q^mN(V)=\sum_{\substack{y_1,\dots,\ y_m\in F_q\\ x_1,\dots,\ x_n\in F_q}}\Psi\Big(\sum_{i=1}^m y_if_i(x_1,\dots,x_n)\Big)=S\Big(\sum_{i=1}^m y_if_i\Big). \tag{11}$$

假设每个 f_i 都不是变量属于 $x_1,\dots,x_n$ 的某个真子集的多项式. 由 (11) 和 (6) 式, 可得

$$\mathrm{ord}_qN(V)\geqslant\omega\Big(\sum_{i=1}^m y_if_i\Big)-m. \tag{12}$$

因此关键是要确定 $\omega(\sum_{i=1}^m y_if_i)$. 令 $y_1,\dots,y_m$ 为方程 (7) 中矩阵 $\mathscr{A}$ 相对应的最后 m 行, 并记方程 (7) 的右边为 $(r;s)=(r_1,\dots,r_n,s_1,\dots,s_m)^T$, 则有

$$u_1+\cdots+u_{|J|}=s_1+\cdots+s_m. \tag{13}$$

故由 (13) 和 (10) 式, 可得

$$\omega\Big(\sum_{i=1}^m y_if_i\Big)=\min\left\{\sum_{i=1}^m s_i\mid(r;s)\in\mathbb{R}^+\left\langle\sum_{i=1}^m y_if_i\right\rangle\cap(\mathbb{Z}^+)^{n+m}\right\}, \tag{14}$$

联立 (14) 和 (12) 式, 有

$$\mathrm{ord}_qN(V)\geqslant\min\left\{\sum_{i=1}^m s_i\mid(r;s)\in\mathbb{R}^+\left\langle\sum_{i=1}^m y_if_i\right\rangle\cap(\mathbb{Z}^+)^{n+m}\right\}-m. \tag{15}$$

3 主要结果

虽然 (15) 式右边关于 $\sum_{i=1}^m s_i$ 的最小值 (显然与 J 有关) 可以通过线性规划的专门软件精确计算出来, 但把它用 J 中元具体表示出来, 一般来讲并不是一件容易的事. 然而, 对于对角多项式组这种特殊情形, 我们有下面的引理, 它对于本文主要定理的证明具有重要作用.

引理 3.1 设簇 V 由多项式组 (4) 确定, 则有

$$\mathrm{ord}_qN(V)\geqslant\min\left\{\sum_{i=1}^m\left\lceil\sum_{j=1}^n u_{ij}\right\rceil\Big|\,u_{ij}\in\mathbb{Q}^+\cup\{0\},\ \sum_{i=1}^m d_{ij}u_{ij}\in\mathbb{Z}^+,\ 1\leqslant j\leqslant n\right\}-m. \tag{16}$$

证明 此时矩阵方程 (7) 关于多项式 $\sum_{i=1}^m y_if_i$ (这里 $y_1,\dots,y_m$ 对应于矩阵 $\mathscr{A}$ 的最后 m

行) 变为

$$\begin{pmatrix} d_{11} & \cdots & 0 & 0 & \cdots & d_{m1} & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & d_{1n} & 0 & \cdots & 0 & \cdots & d_{mn} & 0 \\ 1 & \cdots & 1 & 1 & \cdots & 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 1 & \cdots & 1 & 1 \end{pmatrix} \begin{pmatrix} u_{11} \\ \vdots \\ u_{1n} \\ \delta_1 \\ \vdots \\ u_{m1} \\ \vdots \\ u_{mn} \\ \delta_m \end{pmatrix} = \begin{pmatrix} r_1 \\ \vdots \\ r_n \\ s_1 \\ \vdots \\ s_m \end{pmatrix}, \tag{17}$$

其中 u_{ij}, δ_i 为非负有理数 ($\delta_i = 0$ 若 $c_i = 0$) 且 $(r; s) = (r_1, \ldots, r_n, s_1, \ldots, s_m)^T$ 满足 (15) 式右边的极小性条件. 由 (17) 式, 可得

$$r_j = \sum_{i=1}^{m} d_{ij} u_{ij} \in \mathbb{Z}^+, \quad 1 \leqslant j \leqslant n \tag{18}$$

和

$$s_i = \sum_{j=1}^{n} u_{ij} + \delta_i \in \mathbb{Z}^+, \quad 1 \leqslant i \leqslant m. \tag{19}$$

因此, 我们有

$$\sum_{i=1}^{m} s_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} u_{ij} + \delta_i \right) \geqslant \sum_{i=1}^{m} \left\lceil \sum_{j=1}^{n} u_{ij} \right\rceil. \tag{20}$$

由此结论立得.

在下文中, 令 $d_j = \max\{d_{ij} \,|\, 1 \leqslant i \leqslant m\}$, $1 \leqslant j \leqslant n$. 现在可以给出本文主要定理的证明. 实事上, 我们得到了 (16) 式右边关于 $\sum_{i=1}^{m} \lceil \sum_{j=1}^{n} u_{ij} \rceil$ 用 d_j 表示的一个紧下界.

定理 1.2 的证明 设 $1 \leqslant j \leqslant n$, 由 (18) 式可得

$$\sum_{i=1}^{m} u_{ij} \geqslant \sum_{i=1}^{m} (d_{ij}/d_j) u_{ij} = \left(\sum_{i=1}^{m} d_{ij} u_{ij} \right) / d_j = r_j / d_j,$$

因此有

$$\sum_{i=1}^{m} \left\lceil \sum_{j=1}^{n} u_{ij} \right\rceil \geqslant \sum_{i=1}^{m} \sum_{j=1}^{n} u_{ij} \geqslant \sum_{j=1}^{n} (r_j/d_j) \geqslant \sum_{j=1}^{n} (1/d_j).$$

其中最后一个不等式用到了 $r_j \in \mathbb{Z}^+$ 这一事实. 这样, 由 (16) 式, 我们得到

$$\mathrm{ord}_q N(V) \geqslant \left\lceil \sum_{j=1}^{n} \frac{1}{d_j} \right\rceil - m. \tag{21}$$

由 (21) 式和 $\mathrm{ord}_q N(V) \in \mathbb{N}$, 即可得到 (5) 式.

推论 3.2 若 $d_{1j} = \cdots = d_{mj} = d_j$ ($j = 1, \ldots, n$), 则有

$$\mathrm{ord}_q N(V) \geqslant \max \left\{ \left\lceil \sum_{j=1}^{n} \frac{1}{d_j} \right\rceil - m, \, 0 \right\}. \tag{22}$$

推论 3.3 若 $m=1$, 则 (5) 式变为 (3) 式, 即有

$$\mathrm{ord}_q N(V) \geqslant \left\lceil \sum_{j=1}^{n} \frac{1}{d_j} \right\rceil - 1. \tag{23}$$

由于推论 3.2 和 3.3 很容易从定理 1.2 中推导出来, 故我们略去它们的证明.

推论 3.4 与 (1) 式即 Ax–Katz 定理联立, 我们有

$$\mathrm{ord}_q N(V) \geqslant \max\left\{ \left\lceil \sum_{j=1}^{n} \frac{1}{d_j} \right\rceil - m,\ \left\lceil \frac{n-\sum_{i=1}^{m} \deg f_i}{\max_{1\leqslant i\leqslant m} \deg f_i} \right\rceil, 0 \right\}. \tag{24}$$

特别地, 如果 $\deg f_1 = \cdots = \deg f_m = d$, 则有

$$\left\lceil \sum_{j=1}^{n} \frac{1}{d_j} \right\rceil - m \geqslant \left\lceil \frac{n-\sum_{j=1}^{m} \deg f_j}{d} \right\rceil, \tag{25}$$

这说明 Ax–Katz 定理在这种情形下的确能被我们的结果所改进.

证明 由 (1) 式和 (5) 式知, (24) 式是平凡的. 因此只须证明 (25) 式成立. 由于 $\deg f_1 = \cdots = \deg f_m = d$, 因而 (25) 式与

$$\sum_{j=1}^{n} \frac{1}{d_j} \geqslant \frac{n}{d} \tag{26}$$

等价. 而后者 (26) 式由 $d \geqslant d_j$ $(1 \leqslant j \leqslant n)$ 可知是显然成立的.

参 考 文 献

[1] Ax J., Zeros of polynomials over finite fields, *Amer. J. Math.*, 1964, **86**: 255–261.
[2] Ward H. N., Weight polarization and divisibility, *Discrete Math.*, 1990, **83**: 315–326.
[3] Katz N. M., On a theorem of Ax, *Amer. J. Math.*, 1971, **93**: 485–499.
[4] Wan D., An elementary proof of a theorem of Katz, *Amer. J. Math.*, 1989, **111**: 1–8.
[5] Wan D., A Chevalley-Warning proof of the Ax–Katz theorem and character sums, *Proc. Amer. Math. Soc.*, 1995, **123**: 1681–1686.
[6] Hou X. D., A note on the proof of a theorem of Katz, *Finite Fields Appl.*, 2005, **11**: 316–319.
[7] Morlaye B., Équations diagonales non homogènes sur un corps fini, *C. R. Acad. Sci. Paris Ser A.*, 1971, **272**: 1545–1548.
[8] Joly J. R., Équations et variétés algébriques sur un corps fini, 1973, *Enseign. Math.*, **19**: 1–117.
[9] Lidl R., Niederreiter H., Finite fields, Cambridge: Cambridge University Press, 1987.
[10] Wan D., Zeros of diagnol equations over finite fields, *Proc. Amer. Math. Soc.*, 1988, **103**: 1049–1052.
[11] Wolfmann J., Some systems of diagonal equations over finite fields, *Finite Fields Appl.*, 1988, **4**: 29–37.
[12] Adolphson A., Sperber S., p-adic estimates for exponential sums and the theorem of Chevalley–Warning, *Ann. Sci. Ecole. Norm. Sup.*, 1987, **20**: 545–556.
[13] Sperber S., On the p-adic theory of exponential sums, *Amer. J. Math.*, 1986, **108**: 255–296.