中国科学: 数学 2021 年 第 51 卷 第 10 期: 1～8
SCIENTIA SINICA Mathematica
论 文

有限域上完全对称多项式有很多零点

献给冯克勤教授 80 华诞

万大庆[1], 张俊[2*]

1. Department of Mathematics, University of California at Irvine, Irvine, CA 92697, USA;
2. 首都师范大学数学科学学院, 北京 100048
E-mail: dwan@math.uci.edu, junz@cnu.edu.cn

收稿日期: 2020-11-23; 接受日期: 2021-02-03; 网络出版日期: 2021-02-25; * 通信作者
国家自然科学基金 (批准号: 11971321 和 11826102) 和科技部重点研发计划 (批准号: 2018YFA0704703) 资助项目

摘要 有限域上多项式的零点计数问题是算术代数几何的核心问题之一. 本文考虑有限域 $\mathbb{F}_q$ 上完全对称多项式的零点问题, 主要结果如下: 设 $h(x_1,\ldots,x_k)\in\mathbb{F}_q[x_1,\ldots,x_k]$ 是有限域 $\mathbb{F}_q$ 上一个 m 次完全对称多项式 ($k\geqslant 3$, $1\leqslant m\leqslant q-3$),

(1) 若 m 为奇数或者 q 为奇数, 则多项式 $h(x_1,\ldots,x_k)$ 在 $\mathbb{F}_q^k$ 中至少有 $6q^{k-3}$ 个零点;

(2) 若 $k\geqslant 4$, 则多项式 $h(x_1,\ldots,x_k)$ 在 $\mathbb{F}_q^k$ 中至少有 $6(q-1)q^{k-4}$ 个零点.

作为推论, 我们证明了文献 Zhang 和 Wan (2020) 中的猜想 1.7.

关键词 完全对称多项式 零点 有限域

MSC (2020) 主题分类 11T06, 14G05

1 引言

有限域上代数曲线以及超曲面的有理点计数问题一直都是算术代数几何的核心问题之一, 而且在很多其他学科中有重要应用. 本文考虑对称超曲面的有理点问题.

众所周知, Newton 引入了 3 类对称多项式: 初等对称多项式、幂和对称多项式及完全对称多项式. 前两类对称多项式已经被数论学家们广泛研究, 本文研究第 3 类对称多项式的零点个数问题.

定义 1.1 以 $\{x_1,x_2,\ldots,x_k\}$ 为变元的 m 次齐次完全对称多项式定义如下:

$$h_m(x_1,x_2,\ldots,x_k):=\sum_{1\leqslant i_1\leqslant i_2\leqslant\cdots\leqslant i_m\leqslant k}x_{i_1}x_{i_2}\cdots x_{i_m}.$$

英文引用格式: Wan D, Zhang J. Complete symmetric polynomials over finite fields have many rational zeros (in Chinese). Sci Sin Math, 2021, 51: 1–8, doi: 10.1360/SSM-2020-0328

根据定义, 显然有

$$\begin{aligned}
h_0(x_1,x_2,\ldots,x_k) &= 1,\\
h_1(x_1,x_2,\ldots,x_k) &= x_1+x_2+\cdots+x_k,\\
h_2(x_1,x_2,\ldots,x_k) &= \sum_{i=1}^{k} x_i^2 + \sum_{1\leqslant i<j\leqslant k} x_ix_j,
\end{aligned}$$

等等. 一个完全对称多项式则定义为齐次完全对称多项式的线性组合.

定义 1.2 设 $\mathbb{F}_q$ 是一个具有 q 个元素的有限域, $\mathbb{F}_q$ 上一个以 $\{x_1,x_2,\ldots,x_k\}$ 为变元的 m 次完全对称多项式定义如下:

$$h(x_1,\ldots,x_k) := \sum_{e=0}^{m} a_e h_e(x_1,x_2,\ldots,x_k),$$

其中 $a_e\in\mathbb{F}_q$, 并且 $a_m\neq 0$.

记号 1.1 设 $h(x_1,\ldots,x_k)$ 是有限域 $\mathbb{F}_q$ 上一个 k 元 m 次完全对称多项式, 记

$$N_q(h) := \#\{(a_1,\ldots,a_k)\in\mathbb{F}_q^k \mid h(a_1,\ldots,a_k)=0\}$$

为 $h(x_1,\ldots,x_k)=0$ 所确定的超曲面的 $\mathbb{F}_q$- 有理点的个数.

在实际应用中, 往往需要考虑坐标分量互不相同的零点. 文献 [1] 指出这个问题和有限几何中最大弧问题 [2–4]、编码中深洞问题 [5,6] 和组合数论中子集和问题 [7] 等密切相关.

记号 1.2 设 $h(x_1,\ldots,x_k)$ 是有限域 $\mathbb{F}_q$ 上一个 k 元 m 次完全对称多项式, 记

$$N_q^*(h) := \#\{(a_1,\ldots,a_k)\in\mathbb{F}_q^k \mid h(a_1,\ldots,a_k)=0, a_i\neq a_j, \forall\, i\neq j\}$$

为 $h(x_1,\ldots,x_k)=0$ 确定的超曲面上坐标分量互不相同的 $\mathbb{F}_q$- 有理点的个数.

一个基本的问题是, 何时 $N_q(h)>0$ 以及 $N_q^*(h)>0$, 并且是否可以给出一个好的下界? 文献 [1] 利用有限几何和编码理论的技巧, 对 $k\geqslant 3$ 及有限域特征为奇数的情形, 给出了超越常规数论手段的一个下界, 即如下结论:

结论 1.1 (参见文献 [1, 定理 1.4]) 设 $\mathbb{F}_q$ 是一个奇特征有限域, $h(x_1,\ldots,x_k)\in\mathbb{F}_q[x_1,\ldots,x_k]$ 是一个 m 次完全对称多项式 ($k\geqslant 3$). 若 $1\leqslant m\leqslant q-3$, 则 $N_q(h)\geqslant 6q^{k-3}$.

进而, 对于偶特征有限域情形给出如下猜想:

猜想 1.1 (参见文献 [1, 猜想 1.7]) 设 $\mathbb{F}_q$ 是一个偶特征有限域, 并设 $h(x_1,\ldots,x_k)$ 是 $\mathbb{F}_q$ 上一个 k ($k\geqslant 4$) 个变元 m 次完全对称多项式. 若 $1\leqslant m\leqslant q-4$, 则 $N_q(h)\geqslant 24q^{k-4}$.

文献 [1] 中研究奇特征有限域情形时, 对下界 $N_q(h)\geqslant 6q^{k-3}$ 的证明中最主要的一步是证明如下结论.

结论 1.2 (参见文献 [1, 定理 2.5 中 $k=3$ 情形]) 设 $h(x_1,x_2,x_3)$ 是奇特征有限域 $\mathbb{F}_q$ 上一个 m 次完全对称多项式, 若 $1\leqslant m\leqslant q-3$, 则 $N_q^*(h)\geqslant 6$.

注 1.1 对于偶特征的一般情形, 结论 1.2 不一定成立, 从而文献 [1] 无法将结论 1.1 推广到偶特征的情形. 例如, 任取互素整数 r 和 s ($r>s>1$), 令 $q=2^r$, $m=2^s-2$, 考虑有限域 $\mathbb{F}_q$ 上 m 次齐次完全对称多项式 $h_m(x_1,x_2,x_3)$. 对 $\mathbb{F}_q$ 中任意 3 个互不相同的元素 a_1、a_2 和 a_3, 有

$$h_m(a_1,a_2,a_3) = \frac{1}{a_2-a_1}\left(\frac{a_2^{2^s}-a_3^{2^s}}{a_2-a_3} - \frac{a_1^{2^s}-a_3^{2^s}}{a_1-a_3}\right)$$

$$= \frac{1}{a_2 - a_1}((a_2 - a_3)^{2^s-1} - (a_1 - a_3)^{2^s-1}).$$

因为

$$\gcd(2^s - 1, q - 1) = \gcd(2^s - 1, 2^r - 1) = 2^{\gcd(r,s)} - 1 = 1,$$

所以多项式 x^{2^s-1} 是有限域 $\mathbb{F}_q$ 上的一个置换多项式, 进而有 $h_m(a_1, a_2, a_3) \neq 0$. 于是, $N_q^*(h_m) = 0$.

文献 [1] 指出, 若假设最大距离可分码 (maximum distance separable code, MDS 码) 猜想成立, 则猜想 1.1 成立. 若不假设任何猜想, 在偶特征时, 文献 [1] 证明了更弱的下界: 若 $k \geqslant \frac{q}{2} \geqslant 4$ 且 $1 \leqslant m \leqslant \frac{q}{2}$, 则 $N_q(h) \geqslant (\frac{q}{2})!q^{k-\frac{q}{2}}$. 本文的主要结果如下:

(1) 在特定的条件下, 结论 1.2 对于偶特征情形仍然正确;

(2) 给出猜想 1.1 的一个证明, 实际上, 我们给出一个更强的下界;

(3) 所用的代数方法更为简单直接.

定理 1.1 设有限域 $\mathbb{F}_q$ 的特征为 2, $h(x_1, x_2, x_3) = \sum_{e=0}^{m} a_e h_e(x_1, x_2, x_3) \in \mathbb{F}_q[x_1, x_2, x_3]$ 是一个 m 次完全对称多项式. 若 $1 \leqslant m \leqslant q - 3$, 并且存在奇数 e_0 满足 $a_{e_0} \neq 0$, 则 $N_q^*(h) \geqslant 6$.

推论 1.1 设 $h(x_1, \ldots, x_k) \in \mathbb{F}_q[x_1, \ldots, x_k]$ 是有限域 $\mathbb{F}_q$ 上一个 m 次完全对称多项式. 若 $1 \leqslant m \leqslant q - 3$ 且 m 为奇数, 则 $N_q(h) \geqslant 6q^{k-3}$.

定理 1.2 设有限域 $\mathbb{F}_q$ 的特征为 2, 并设 $h(x_1, \ldots, x_k)$ 是有限域 $\mathbb{F}_q$ 上一个 m 次完全对称多项式 ($k \geqslant 4$). 若 $1 \leqslant m \leqslant q - 3$, 则 $N_q(h) \geqslant 6(q - 1)q^{k-4}$.

推论 1.2 猜想 1.1 成立.

2 证明

本节给出本文主要定理的证明.

引理 2.1 [8] 设 $f(x) \in \mathbb{F}_q[x]$ 是有限域 $\mathbb{F}_q$ 上一个 d 次多项式, 若 $f(x)$ 不是 $\mathbb{F}_q$ 上的置换多项式, 则

$$\#\{f(a) \mid a \in \mathbb{F}_q\} \leqslant q - \left\lceil \frac{q-1}{d} \right\rceil.$$

记号 2.1 设 $f(x) \in \mathbb{F}_q[x]$ 是任意 d 次多项式 ($1 \leqslant d \leqslant q-1$), 则对任意 $u \in \mathbb{F}_q$, $x-u \mid f(x)-f(u)$, 即存在 $d-1$ 次多项式 $\phi_u(x) \in \mathbb{F}_q[x]$ 使得 $f(x) - f(u) = \phi_u(x)(x - u)$. 对等式两边求导, 再代入 u, 显然有 $\phi_u(u) = f'(u)$.

定理 2.1 记号如上, 若对任意 $u \in \mathbb{F}_q$, $\phi_u(x)$ 都是 $\mathbb{F}_q$ 上的置换多项式, 即 $\{\phi_u(a) \mid a \in \mathbb{F}_q\} = \mathbb{F}_q$, 则以下结论成立:

(1) 若 q 是奇数, 则多项式 $f(x)$ 的次数是 2;

(2) 若 q 是偶数, 则存在 $g(x) \in \mathbb{F}_q[x]$ 满足 $f(x) = g(x)^2$.

证明 由题设知, 对任意两个不同元素 $u, v \in \mathbb{F}_q$, 有

$$\{\phi_u(a) \mid a \in \mathbb{F}_q \setminus \{u, v\}\} = \mathbb{F}_q \setminus \{f'(u), \phi_u(v)\}, \quad f'(u) \neq \phi_u(v).$$

于是,

$$\prod_{a \in \mathbb{F}_q \setminus \{u,v\}} (\phi_u(a) - \phi_u(v)) = \frac{-1}{\phi_u(u) - \phi_u(v)} = \frac{-1}{f'(u) - \frac{f(v)-f(u)}{v-u}}.$$

另一方面,

$$\begin{aligned}
&\prod_{a\in\mathbb{F}_q\setminus\{u,v\}}(\phi_u(a)-\phi_u(v))\\
&=\prod_{a\in\mathbb{F}_q\setminus\{u,v\}}\left(\frac{f(a)-f(u)}{a-u}-\frac{f(v)-f(u)}{v-u}\right)\\
&=\prod_{a\in\mathbb{F}_q\setminus\{u,v\}}\frac{1}{(a-u)(v-u)}\prod_{a\in\mathbb{F}_q\setminus\{u,v\}}((v-u)(f(a)-f(u))-(a-u)(f(v)-f(u)))\\
&=\frac{-1}{(v-u)^{q-3}}\prod_{a\in\mathbb{F}_q\setminus\{u,v\}}((v-u)f(a)+a(f(u)-f(v))+uf(v)-vf(u)).
\end{aligned}$$

令

$$F(x,u,v)=f(x)(v-u)+x(f(u)-f(v))+uf(v)-vf(u),$$

则有等式

$$\frac{-1}{f'(u)-\frac{f(v)-f(u)}{v-u}}=\frac{-1}{(v-u)^{q-3}}\prod_{a\in\mathbb{F}_q\setminus\{u,v\}}F(a,u,v).$$

因此,

$$(v-u)\prod_{a\in\mathbb{F}_q\setminus\{u,v\}}F(a,u,v)=\frac{-1}{f'(u)(u-v)+f(v)-f(u)}.$$

注意到上面等式的左边关于 u 和 v 对称, 因为 $F(a,u,v)=-F(a,v,u)$ 和 $v-u=-(u-v)$. 所以等式右边也应该关于 u 和 v 对称. 从而, 对任意不同的两个元素 $u,v\in\mathbb{F}_q$, 有

$$f'(u)(u-v)+f(v)-f(u)=f'(v)(v-u)+f(u)-f(v).$$

进而, 对任意 $u,v\in\mathbb{F}_q$, 有恒等式

$$(f'(u)+f'(v))(u-v)=2(f(u)-f(v)).$$

从而

$$(f'(x)+f'(y))(x-y)=2(f(x)-f(y)). \tag{2.1}$$

若 q 是奇素数 p 的幂, 不妨设 ax^d 是 $f(x)$ 的最高次项 ($a\neq 0$), 比较等式 (2.1) 两边最高次项, 可以得到

$$d(x^{d-1}+y^{d-1})(x-y)=2(x^d-y^d).$$

从而 $d\equiv 2 \pmod p$, 并且 $xy^{d-1}=x^{d-1}y$, 于是 $d=2$.

若 q 是偶数, 则

$$(f'(x)+f'(y))(x-y)=0.$$

从而 $f'(x)=0$, 于是, $f(x)$ 只含有偶数次项, 进而存在 $g(x)\in\mathbb{F}_q[x]$ 满足 $f(x)=g(x)^2$. □

有了以上的准备, 下面证明本文的主要结果: 定理 1.1、1.2 及推论 1.1 和 1.2.

定理 1.1 的证明 注意到 $h(x_1,x_2,x_3)$ 是一个完全对称多项式, 所以任何一个坐标互不相同的零点任意坐标分量的置换仍然是它的零点. 因此, $N_q^*(h)\geqslant 6$ 等价于 $N_q^*(h)\geqslant 1$. 反设 $N_q^*(h)=0$.

记 $f(x)=x^2\sum_{e=0}^{m}a_ex^2\in\mathbb{F}_q[x]$, 则多项式 $f(x)$ 的次数满足 $3\leqslant\deg(f)=m+2\leqslant q-1$. 因为

$$\begin{aligned}h_e(x_1,x_2,x_3)&=\sum_{k=0}^{e}x_3^k\sum_{i+j=e-k,\,i,j\geqslant 0}x_1^ix_2^j\\&=\sum_{k=0}^{e}x_3^k\left(\frac{x_2^{e-k+1}-x_1^{e-k+1}}{x_2-x_1}\right)\\&=\frac{1}{x_2-x_1}\left(\frac{x_3^{e+2}-x_2^{e+2}}{x_3-x_2}-\frac{x_3^{e+2}-x_1^{e+2}}{x_3-x_1}\right),\end{aligned}$$

所以

$$\begin{aligned}h(x_1,x_2,x_3)&=\frac{1}{x_2-x_1}\left(\frac{f(x_2)-f(x_3)}{x_2-x_3}-\frac{f(x_1)-f(x_3)}{x_1-x_3}\right)\\&=\frac{1}{x_2-x_1}(\phi_{x_3}(x_2)-\phi_{x_3}(x_1)).\end{aligned}$$

因为 $N_q^*(h)=0$, 所以对任意 3 个互不相同的 $u,a,b\in\mathbb{F}_q$, 有 $\phi_u(a)\neq\phi_u(b)$. 根据引理 2.1 可知, $\phi_u(x)$ 是有限域 $\mathbb{F}_q$ 上的一个置换多项式. 否则,

$$\#\{\phi_u(a)\mid a\in\mathbb{F}_q\}\leqslant q-\left\lceil\frac{q-1}{\deg(\phi_u(x))}\right\rceil\leqslant q-2,$$

与 $\phi_u(x)$ 是 $\mathbb{F}_q\setminus\{u\}$ 上的单射矛盾.

注意到引理 2.1 的证明使用了数论中 p- 进提升的技巧, 这里给这种特殊情形一个简单的证明.

因为当 a 历遍 $\mathbb{F}_q\setminus\{u\}$ 时, $q-1$ 个值 $\phi_u(a)$ 互不相同, 于是假设 w 是 $\mathbb{F}_q$ 中剩下的那个值, 即

$$\{\phi_u(a)\mid a\in\mathbb{F}_q\setminus\{u\}\}\cup\{w\}=\mathbb{F}_q,$$

则有

$$w+\sum_{a\in\mathbb{F}_q\setminus\{u\}}\phi_u(a)=0. \tag{2.2}$$

又因为多项式 $\phi_u(x)$ 的次数满足 $\deg(\phi_u(x))=\deg(f)-1\leqslant q-2$, 所以

$$\sum_{a\in\mathbb{F}_q}\phi_u(a)=0,$$

即

$$f'(u)+\sum_{a\in\mathbb{F}_q\setminus\{u\}}\phi_u(a)=0. \tag{2.3}$$

比较等式 (2.2) 和 (2.3), 可得 $w=f'(u)$, 于是 $\phi_u(x)$ 是有限域 $\mathbb{F}_q$ 上的一个置换多项式. 再根据定理 2.1 知, 多项式 $f(x)$ 只包含有偶数次数项, 这与题设矛盾. 从而定理 1.1 得证. □

注 2.1 结合定理 2.1 的第一个结论和定理 1.1 的证明, 不难发现该证明给出了结论 1.1 的一个新的证明.

推论 1.1 的证明 当 q 是奇数时, 推论 1.1 是结论 1.1 的特殊情形, 故只需要在偶特征的情形下证明推论 1.1. 对任意 $(a_4, a_5, \ldots, a_k) \in \mathbb{F}_q^{k-3}$, 令

$$g(x_1, x_2, x_3) := h(x_1, x_2, x_3, a_4, a_5, \ldots, a_k),$$

则 $g(x_1, x_2, x_3)$ 是一个 m 次完全对称多项式, 其首项为 $a_m h_m(x_1, x_2, x_3)$. 由题设知 m 是奇数, 故根据定理 1.1, 有 $N_q^*(g) \geqslant 6$, 更有 $N_q(g) \geqslant 6$. 从而 $N_q(h) \geqslant 6q^{k-3}$. □

定理 1.2 的证明 下面对 m 分别为奇数和偶数来证明. 首先, 若 m 是奇数, 利用推论 1.1, 有

$$N_q(h) \geqslant 6q^{k-3} = 6q \times q^{k-4} > 6(q-1)q^{k-4}.$$

其次, 若 m 是偶数, 则

$$\begin{aligned}
&h(x_1, x_2, \ldots, x_k)\\
&\quad = a_m h_m(x_1, x_2, \ldots, x_k) + a_{m-1} h_{m-1}(x_1, x_2, \ldots, x_k)\\
&\qquad + \sum_{e \leqslant m-2} a_e h_e(x_1, x_2, \ldots, x_k)\\
&\quad = a_m \Bigg(h_m(x_1, x_2, x_3) + h_{m-1}(x_1, x_2, x_3) h_1(x_4, x_5, \ldots, x_k)\\
&\qquad + \sum_{e \leqslant m-2} h_e(x_1, x_2, x_3) h_{m-e}(x_4, x_5, \ldots, x_k) \Bigg)\\
&\qquad + a_{m-1} \Bigg(h_{m-1}(x_1, x_2, x_3) + \sum_{e \leqslant m-2} h_e(x_1, x_2, x_3) h_{m-1-e}(x_4, x_5, \ldots, x_k) \Bigg)\\
&\qquad + \sum_{e \leqslant m-2} a_e h_e(x_1, x_2, \ldots, x_k)\\
&\quad = a_m h_m(x_1, x_2, x_3) + h_{m-1}(x_1, x_2, x_3)(a_m h_1(x_4, x_5, \ldots, x_k) + a_{m-1}) + g(x_1, x_2, \ldots, x_k)\\
&\quad = a_m h_m(x_1, x_2, x_3) + h_{m-1}(x_1, x_2, x_3)(a_m(x_4 + x_5 + \cdots + x_k) + a_{m-1}) + g(x_1, x_2, \ldots, x_k),
\end{aligned}$$

其中 $g(x_1, x_2, \ldots, x_k)$ 是关于 $\{x_1, x_2, x_3\}$ 的次数不超过 $m-2$ 的完全对称多项式. 令

$$S := \{(a_4, a_5, \ldots, a_k) \in \mathbb{F}_q^{k-3} \mid a_m(x_4 + x_5 + \cdots + x_k) + a_{m-1} \neq 0\}.$$

因为 $a_m \neq 0$, 所以 $\#S = q^{k-3} - q^{k-4}$. 注意到, 对任意 $(a_4, a_5, \ldots, a_k) \in S$, 关于 x_1、x_2 和 x_3 的完全对称多项式 $h(x_1, x_2, x_3) := h(x_1, x_2, x_3, a_4, a_5, \ldots, a_k)$ 的次数为 m, 并且 $m-1$ 次项系数不为 0. 因为 $m-1$ 为奇数, 从而根据定理 1.1, 可得 $N_q(h(x_1, x_2, x_3)) \geqslant 6$. 于是,

$$N_q(h) \geqslant 6 \cdot \#S \geqslant 6(q^{k-3} - q^{k-4}) = 6(q-1)q^{k-4}.$$

至此, 完成了定理 1.2 的证明. □

推论 1.2 的证明 若 $m = 1$, 由题设 $1 \leqslant q-3$ 可知 $q \geqslant 4$. 此时,

$$N_q(h) = q^{k-1} = q^3 \cdot q^{k-4} > 24q^{k-4}.$$

若 $m \geqslant 2$, 由题设 $2 \leqslant m \leqslant q-3$ 得知 $q \geqslant 5$. 此时, 由定理 1.2, 有

$$N_q(h) \geqslant 6(q-1)q^{k-4} \geqslant 24q^{k-4}.$$

从而, 推论 1.2 得证. □

参考文献

1 Zhang J, Wan D. Rational points on complete symmetric hypersurfaces over finite fields. Discrete Math, 2020, 343: 112072
2 Ball S. On sets of vectors of a finite vector space in which every subset of basis size is a basis. J Eur Math Soc (JEMS), 2012, 3: 733–748
3 Ball S, De Beule J. On sets of vectors of a finite vector space in which every subset of basis size is a basis II. Des Codes Cryptogr, 2012, 65: 5–14
4 Ball S, Lavrauw M. Arcs in finite projective spaces. arXiv:1908.10772, 2019
5 Seroussi G, Roth R M. On MDS extensions of generalized Reed-Solomon codes. IEEE Trans Inform Theory, 1986, 32: 349–354
6 Zhang J, Fu F W, Liao Q Y. Deep holes of generalized Reed-Solomon codes (in Chinese). Sci Sin Math, 2013, 43: 727–740 [张俊, 符方伟, 廖群英. 广义 Reed-Solomon 码的深洞. 中国科学: 数学, 2013, 43: 727–740]
7 Li J, Wan D. On the subset sum problem over finite fields. Finite Fields Appl, 2008, 14: 911–929
8 Wan D. A p-adic lifting lemma and its applications to permutation polynomials. In: Finite Fields, Coding Theory, and Advances in Communications and Computing. Lecture Notes in Pure and Applied Mathematics, vol. 141. New York: Marcel Dekker, 1992, 209–216

Complete symmetric polynomials over finite fields have many rational zeros

Daqing Wan & Jun Zhang

Abstract Counting zeros of polynomials over finite fields is one of the most important topics in arithmetic algebraic geometry. In this paper, we consider the problem for complete symmetric polynomials. The homogeneous complete symmetric polynomial of degree m in the k-variables $\{x_1, x_2, \ldots, x_k\}$ is defined as

$$h_m(x_1, x_2, \ldots, x_k) := \sum_{1 \leqslant i_1 \leqslant i_2 \leqslant \cdots \leqslant i_m \leqslant k} x_{i_1} x_{i_2} \cdots x_{i_m}.$$

A complete symmetric polynomial of degree m over $\mathbb{F}_q$ in the k-variables $\{x_1, x_2, \ldots, x_k\}$ is defined as

$$h(x_1, \ldots, x_k) := \sum_{e=0}^{m} a_e h_e(x_1, x_2, \ldots, x_k),$$

where $a_e \in \mathbb{F}_q$ and $a_m \neq 0$. We are interested in counting the number of zeros and the number of zeros with pairwise distinct coordinates of a complete symmetric polynomial, respectively. Let

$$N_q(h) := \#\{(a_1, \ldots, a_k) \in \mathbb{F}_q^k \mid h(a_1, \ldots, a_k) = 0\}$$

denote the number of $\mathbb{F}_q$-rational points on the affine hypersurface defined by $h(x_1, \ldots, x_k) = 0$. Let

$$N_q^*(h) := \#\{(a_1, \ldots, a_k) \in \mathbb{F}_q^k \mid h(a_1, \ldots, a_k) = 0 \text{ and } a_i \neq a_j, \forall\, i \neq j\}$$

denote the number of $\mathbb{F}_q$-rational points on the affine hypersurface defined by $h(x_1, \ldots, x_k) = 0$ with the additional condition that the coordinates are distinct. In the paper Zhang and Wan (2020), the authors showed the lower bound $N_q(h) \geqslant 6q^{k-3}$ if q is odd, $k \geqslant 3$ and $1 \leqslant m \leqslant k-3$ and conjectured $N_q(h) \geqslant 24q^{k-4}$ if q is even, $k \geqslant 4$ and $1 \leqslant m \leqslant k-4$. The key ingredient in the proof of the lower bound is to prove $N_q^*(h(x_1, x_2, x_3)) \geqslant 6$ for odd q, $k = 3$ and $1 \leqslant m \leqslant q-3$ which does not hold for even q in general. In this paper, we deal with the even characteristic case. The main new results are the following (suppose $\mathbb{F}_q$ is a finite field with characteristic 2):

(1) Let $h(x_1, x_2, x_3) := \sum_{e=0}^{m} a_e h_e(x_1, x_2, x_3) \in \mathbb{F}_q[x_1, x_2, x_3]$ be a complete symmetric polynomial of degree m with $1 \leqslant m \leqslant q-3$. If $a_{e_0} \neq 0$ for some odd e_0, then $N_q^*(h) \geqslant 6$.

(2) Let $h(x_1,\ldots,x_k)$ be a complete symmetric polynomial in $k \geqslant 3$ variables over $\mathbb{F}_q$ of degree m with $1 \leqslant m \leqslant q-3$. If m is odd, then $N_q(h) \geqslant 6q^{k-3}$.

(3) Let $h(x_1,\ldots,x_k)$ be a complete symmetric polynomial in $k \geqslant 4$ variables over $\mathbb{F}_q$ of degree m with $1 \leqslant m \leqslant q-3$. Then $N_q(h) \geqslant 6(q-1)q^{k-4}$.

(4) As a consequence, Conjecture 1.7 in the paper [Zhang J, Wan D. Rational points on complete symmetric hypersurfaces over finite fields. Discrete Math, 2020, 343: 112072] is true. That is, for any complete symmetric polynomial $h(x_1,\ldots,x_k)$ in $k \geqslant 4$ variables over $\mathbb{F}_q$ of degree m with $1 \leqslant m \leqslant q-4$, we have $N_q(h) \geqslant 24q^{k-4}$.

Keywords **complete symmetric polynomial, rational zero, even characteristic**

MSC(2010) **11T06, 14G05**

doi: SSM-2020-0328