有限域上四次对角方程 $ax^4+by^4=c$ 解的存在性

黄宝盛[1]，吴荣军[2]，谭千蓉[3]，朱光艳[4]

(1. 四川大学数学学院，成都 610064；2. 西南民族大学数学学院，成都 610041；
3. 攀枝花学院数学与计算机学院，攀枝花 617000；4. 湖北民族大学教育学院，恩施 445000)

摘　要：设 F_q 是特征为 p 的有限域，d 为正整数. 对任意的 $a,b\in F_q^*$，$c\in F_q$，方程 $ax^d+by^d=c$ 在 F_q 上是否恒有解这一问题长期吸引着大量研究者的关注. 当 $d=2$ 时，Cauchy 给出了肯定结论. 当 $d=3$ 时，Skolem 证明，对任意的素数 $p\neq 7$，方程 $ax^3+by^3=c$ 在 F_p 上恒有解；Singh 证明，对任意的素数方幂 $q\neq 4$，方程 $ax^3+by^3=c$ 在 F_q 上恒有解. 本文研究 $d=4$ 的情形，给出了该方程解的存在性，即当 $q\neq 5,9,13,17,25,29$ 时，对任意的 $a,b\in F_q^*$，$c\in F_q$，方程 $ax^4+by^4=c$ 在 F_q 上恒有解.

关键词：有限域；四次对角方程；存在性

中图分类号：O156.2　　**文献标识码**：A　　DOI：10.19907/j.0490-6756.2022.011001

On the existence of solutions of diagonal quartic equation $ax^4+by^4=c$ over finite field

HUANG Bao-Sheng[1], *WU Rong-Jun*[2], *TAN Qian-Rong*[3], *ZHU Guang-Yan*[4]

(1. School of Mathematics, Sichuan University, Chengdu 610064, China;
2. School of Mathematics, Southwest Minzu University, Chengdu 610041, China;
3. School of Mathematics and Computers, Panzhihua University, Panzhihua 617000, China;
4. School of Education, Hubei Minzu University, Enshi 445000, China)

Abstract: Let F_q be a finite field with q elements, where q is a power of a prime p, and d be a positive number. Given any $a,b\in F_q^*$ and $c\in F_q$, the problem whether there is always a solution over F_p for the diagonal equation $ax^d+by^d=c$ has been attracting significant attention of scholars. When $d=2$, Cauchy gave an affirmative answer. When $d=3$, Skolem showed that for any $p\neq 7$, there are always solutions over F_p for $ax^3+by^3=c$ with $a,b\in F_p^*$ and $c\in F_p$; Singh extended the result to the general finite fields F_p for $q\neq 4$. In this paper, we mainly study the case for $d=4$. We prove that there always exist solutions for the diagonal quartic equation $ax^4+by^4=c$ over F_q when $q\neq 5,9,13,17,25,29$ for every $a,b\in F_q^*$ and $c\in F_q$.

Keywords: Finite field; Diagonal quartic equation; Existence

(2010 MSC 11D79, 11D72)

收稿日期：2021-05-07

基金项目：西南民族大学科研启动基金(RQD2021100)

作者简介：黄宝盛(1995－)，男，广西玉林人，硕士研究生，主要研究方向为数论. E-mail：1196274553@qq.com

通讯作者：吴荣军. E-mail：eugen_woo@163.com

1　引　言

有限域上方程解的存在性以及解的个数[1-16]一直是数学家们十分关心的问题. 关于这一问题的第一个重要的结果是 Lagrange[4] 给出的：有限域 F_p(p 为素数)上的 $n(n\geqslant 0)$ 次单变量多项式至多只有 n 个根. 这结论在一般的有限域 F_q(q 为素数方幂)上也成立[5]. 如下问题直接推动了有限域理论的发展.

问题　设 d 为正整数，q 为素数方幂. 那么对充分大的 q，以及任意的 $a,b\in F_q^*$ 与 $c\in F_q$，方程

$$ax^d+by^d=c$$

在有限域 F_q 上是否恒有解？

当 $a=b=1,d=2$ 时，答案是肯定的. 这就是有限域中熟知的结论[11]：F_q 中的元素都可以写成两个元素的平方和；当 $a=b=1$ 时，对一般的 d，Small[10] 给出了问题的肯定回答并确定了 q 的下界. 设 d 为正整数，F_q 为 q 元有限域，记 $\delta=\gcd(d,q-1)$. 若 $q>(\delta-1)^4$，则 F_q 中任意元素均可写成该域上的两个 d 次方幂之和.

对于一般的 $a,b\in F_q^*$，Cauchy，Skolem，Singh 等人先后研究过上述问题. 当 $d=2$ 时，Cauchy[2] 证明了如下结论：设 F_q 为 q 元有限域，$a,b\in F_q^*$，则对任意的 $c\in F_q$，方程 $ax^2+by^2=c$ 在 F_q 上恒有解. 当 $d=3$ 时，Skolem[9] 证明：对任意的素数 $p\neq 7$，方程 $ax^3+by^3=c$ 在 F_p 上恒有解，其中 $a,b\in F_p^*$，$c\in F_p$. 对素数方幂 $q=p^k$，Singh[8] 证明：对任意的素数方幂 $q\neq 4$，方程 $ax^3+by^3=c$ 在 F_q 上恒有解，其中 $a,b\in F_q^*$，$c\in F_q^*$.

近年来，Zhang 等[16] 研究了当 $c\in F_p^*$ 时方程 $x^3+y^3+z^3+w^3=c$ 在 F_p 上解的个数的显式表达式. Hong 等[3] 研究了两类方程 $x_1^3+\cdots+x_s^3=c$ 和 $x_1^3+\cdots+x_{s-1}^3+yx_s^3=0$ 在 F_q 上解的个数，推广了前人的结果. 此外，Zhao 等[14,15] 使用 Gauss 和以及 Jacobi 和的方法研究了当 $c\in F_q^*$ 时三类四次对角方程 $x^4+y^4=c$，$x^4+y^4+z^4=c$ 以及 $x^4+y^4+z^4+w^4=c$ 在 F_q 上解的个数，并给出解的个数的显式表达式.

本文主要研究有限域上二元四次对角方程解的存在性，即对 $a,b\in F_q^*$，$c\in F_q$，方程 $ax^4+by^4=c$ 在 F_q 上是否恒有解. 我们给出了该方程恒有解时 q 的所有取值. 通过引入 F_q 上的概率测度，研究 F_q 的某些特殊子集的测度，我们借助指数和工具证明了如下主要结论：

定理 1.1　设 $q\neq 5,9,13,17,25,29$. 对任意 $a,b\in F_q^*$，$c\in F_q$，方程 $ax^4+by^4=c$ 在 F_q 上恒有解.

2　预备知识

在本节中，我们定义一些记号并给出几个引理.

定义 2.1　设 p 为素数，k 为正整数. 令 $q=p^k$. 记 F_q 为 q 元有限域. 对任意 F_q 的子集 A，我们定义 A 在 F_q 上的概率测度为 $\mu_q(A)=|A|/q$，其中 $|A|$ 为集合 A 中元素的个数.

定义 2.2　设 $A\subset F_q$，记 1_A 为集合 A 的特征函数，对任意的 $x\in F_q$，定义

$$1_A(x)\coloneqq\begin{cases}1,\text{若 } x\in A,\\ 0,\text{否则}.\end{cases}$$

定义 2.3　设 f_1,f_2 是定义在 F_q 上的两个复值函数，定义它们的内积为

$$\langle f_1,f_2\rangle\coloneqq\frac{1}{q}\sum_{g\in F_q}f_1(g)\overline{f_2(g)},$$

其中 $\overline{f_2(g)}$ 是复数 $f_2(g)$ 的共轭.

定义 2.4　设 f 是 F_q 到 C 上的函数，定义它的范数为 $\|f\|\coloneqq\sqrt{\langle f,f\rangle}$. 由 Cauchy-Schwarz 不等式可得

$$|\langle f_1,f_2\rangle|\leqslant\|f_1\|\cdot\|f_2\|.$$

定义 2.5　对任意 $b\in F_q$，我们称映射 χ_b：$F_q\to\mathbf{C}$，$a\mapsto\zeta_p^{\mathrm{Tr}(ba)}$ 为有限域 F_q 上的加法特征，其中 ζ_p 为 p 次本原单位根. 特别地，χ_0 为有限域 F_q 上的平凡加法特征. 记 $\widehat{F_q}\coloneqq\{\chi_b|b\in F_q\}$ 为 F_q 上所有加法特征构成的集合.

定义 2.6　设 f 是 $F_q\to\mathbf{C}$ 的映射，则它的 Fourier 变换定义为 $\widehat{f}:\widehat{F_q}\to\mathbf{C}$，

$$\widehat{f}(\chi)=q\langle f,\overline{\chi}\rangle=\sum_{g\in F_q}f(g)\chi(g).$$

类似地，对任意的 $a\in F_q$，我们可以给出 Fourier 反演公式如下：

$$f(a)=\frac{1}{q}\sum_{\chi\in\widehat{F_q}}\widehat{f}(\overline{\chi})\chi(a)=\frac{1}{q}\sum_{\chi\in\widehat{F_q}}\widehat{f}(\chi)\chi(-a).$$

引理 2.7[1]　设 d 为正整数，q 为素数方幂，若 $\delta=\gcd(d,q-1)$，则

$$\{x^\delta|x\in F_q\}=\{x^d|x\in F_q\}.$$

证明　由于 $\{x^d|x\in F_q\}\subseteq\{x^\delta|x\in F_q\}$ 是显然的，因此我们只需证明 $\{x^\delta|x\in F_q\}\subseteq\{x^d|x\in F_q\}$.

由 Bézout 引理可知，存在 $u,v\in\mathbf{Z}$，使得 $\delta=u(q-1)+vd$. 那么对任意 $x\in F_q^*$，有 $x^\delta=x^{u(q-1)+vd}=(x^{q-1})^u(x^d)^v=(x^d)^v$. 因而，$\{x^\delta\,|\,x\in F_q\}\subseteq\{x^d\,|\,x\in F_q\}$.

引理 2.8[1]　设 $d\geqslant 2$ 为正整数，F_q 为有限域，$A=\{x^d\,|\,x\in F_q\}$，则 $\mu(A)>\dfrac{1}{d}$.

证明　设 $\delta=\gcd(d,q-1)$，$c\in F_q^*$. 若 $\delta=1$，由引理 2.7 知，$A=\{x^d\,|\,x\in F_q\}=\{x\,|\,x\in F_q\}=F_q$，结论成立. 若 $\delta\geqslant 2$，由有限域理论中熟知的结果(参见文献[7]定理 9.4.2)可知方程 $x^d=c$ 在 F_q^* 中有解当且仅当 $c^{\frac{q-1}{\delta}}=1$. 又 F_q^* 中恰有 $\dfrac{q-1}{\delta}$ 个元 c 使得 $c^{\frac{q-1}{\delta}}=1$，从而 F_q^* 中恰有 $\dfrac{q-1}{\delta}$ 个元 c 使得方程 $x^d=c$ 在 F_q^* 中有解，即 $|A|=\dfrac{q-1}{\delta}+1>\dfrac{q}{\delta}$，因而 $\mu(A)=\dfrac{|A|}{q}>\dfrac{1}{\delta}\geqslant\dfrac{1}{d}$.

引理 2.9[6]　设 F_q 为奇特征 p 的 q 元有限域，$q\equiv 1(\mathrm{mod}\ 4)$，$\mathfrak{g}$ 为 F_q^* 的生成元，χ_1 为 F_q 上本原加法特征. 记

$$T_{\chi_1}(u):=\sum_{v\in F_q}\chi_1(uv^4).$$

那么对任意 $i\in 1,\cdots,q-1$ 有 $T_{\chi_1}(\mathfrak{g}^i)$ 为方程

$$\begin{cases} x^4-6qx^2+8qsx+q^2-4qs^2=0, \\ \qquad \text{如果 } q\equiv 1(\mathrm{mod}\ 8), \\ x^4+2qx^2+8qsx+9q^2-4qs^2=0, \\ \qquad \text{如果 } q\equiv 5(\mathrm{mod}\ 8) \end{cases}$$

的根，其中 s 由如下条件唯一确定：

$$q=s^2+4t^2,\ q\equiv 1(\mathrm{mod}\ 4)$$

并且如果 $p\equiv 1(\mathrm{mod}\ 4)$，那么 $\gcd(s,p)=1$.

引理 2.10[1]　定义实算术函数 $\kappa(x)$：$\mathbf{Z}\to\mathbf{R}$ 为 $\kappa(x):=\dfrac{3}{\sqrt{x}}$. 则 κ 满足如下性质：

(i) 对任意的 $q=p^n$，$A_q,B_q\subseteq F_q$ 以及 F_q 上的四次多项式 $P(x)=cx^4(c\in F_q^*)$，有

$$\left|\frac{1}{q}\sum\nolimits_{g\in F_q}\mu(A_q\cap(B_q+P(g)))-\mu(A_q)\mu(B_q)\right|\leqslant\kappa(q).$$

(ii) $\lim\limits_{q\to\infty}\kappa(q)=0$.

特别地，在 $q\equiv 5(\mathrm{mod}\ 8)$ 的情形下，我们给出了 $\left|\dfrac{1}{q}\sum\nolimits_{g\in F_q}\mu(A_q\cap(B_q+P(g)))-\mu(A_q)\mu(B_q)\right|$ 一个更严格的估计，即

引理 2.11　当 $A_q=\{ax^4\,|\,x\in F_q\}$，$B_q=\{-by^4\,|\,y\in F_q\}$，$P(x)=cx^4$，$a,b,c\in F_q^*$ 且 $q=p^n\equiv 5(\mathrm{mod}\ 8)$时，引理 2.10 中的算术函数可以取

$$\kappa(x)=2.5526\,\frac{x+3}{4x^{3/2}}.$$

证明　为简便起见，记 $A=A_q$，$B=B_q$，$\mu(A)=\mu_q(A)$. 对任意的 $g,h\in F_q$，由定义 2.1 和 2.2 可得

$$\mu(A)=\frac{|A|}{q}=\frac{1}{q}\sum_{z\in F_q}1_A(z),$$

$$1_{A\cap B}(g)=1_A(g)\,1_B(g),$$

$$1_{A+g}(h)=1_A(h-g).$$

因而

$$\begin{aligned}&\frac{1}{q}\sum\nolimits_{g\in F_q}\mu(A\cap(B+P(g)))=\\&\quad\frac{1}{q^2}\sum_{g\in F_q}\sum_{h\in F_q}1_{A\cap(B+P(g))}(h)=\\&\quad\frac{1}{q^2}\sum_{g\in F_q}\sum_{h\in F_q}1_A(h)\,1_{B+P(g)}(h)=\\&\quad\frac{1}{q^2}\sum_{g\in F_q}\sum_{h\in F_q}1_A(h)\,1_B(h-P(g)).\end{aligned}$$

由 Fourier 反演公式可得

$$\begin{aligned}&\frac{1}{q^2}\sum_{g\in F_q}\sum_{h\in F_q}1_A(h)\,1_B(h-P(g))=\\&\quad\frac{1}{q^3}\sum_{g\in F_q}\sum_{h\in F_q}\sum_{\chi\in\widehat{F}_q}1_A(h)\,\widehat{1}_B(\chi)\chi(P(g)-h)=\\&\quad\frac{1}{q^3}\sum_{g,h\in F_q}\sum_{\chi\in\widehat{F}_q}1_A(h)\widehat{1}_B(\chi)\chi(P(g))\,\overline{\chi}(h)=\\&\quad\frac{1}{q^3}\sum_{g\in F_q,\chi\in\widehat{F}_q}\widehat{1}_B(\chi)\chi(P(g))\sum_{h\in F_q}1_A(h)\,\overline{\chi}(h)=\\&\quad\frac{1}{q^3}\sum_{g\in F_q,\chi\in\widehat{F}_q}\widehat{1}_B(\chi)\chi(P(g))\,\widehat{1}_A(\overline{\chi})=\\&\quad\frac{1}{q^3}\sum_{\chi\in\widehat{F}_q}\widehat{1_A}(\overline{\chi})\widehat{1_B}(\chi)\sum_{g\in F_q}\chi(P(g)).\end{aligned}$$

当 $\overline{\chi}=\chi_0$ 时，有

$$\widehat{1}_A(\chi_0)=\sum_{g\in F_q}1_A(g)\,\chi_0(g)=\sum_{g\in F_q}1_A(g)=|A|.$$

当 $\chi=\chi_0$ 时，同理可得 $\widehat{1_B}(\chi_0)=|B|$. 进一步地，我们有 $\sum\nolimits_{g\in F_q}\chi_0(P(g))=q$. 于是

$$\begin{aligned}&\frac{1}{q^3}\sum_{\chi\in\widehat{F}_q}\widehat{1}_A(\overline{\chi})\widehat{1}_B(\chi)\sum_{g\in F_q}\chi(P(g))=\\&\quad\frac{1}{q^3}\,\widehat{1}_A(\overline{\chi_0})\widehat{1}_B(\chi_0)\sum_{g\in F_q}\chi_0(P(g))+\\&\quad\frac{1}{q^3}\sum_{\chi\neq\chi_0}\widehat{1}_A(\overline{\chi})\widehat{1}_B(\chi)\sum_{g\in F_q}\chi(P(g))=\\&\quad\frac{1}{q^3}|A|\cdot|B|q+\end{aligned}$$

$$\frac{1}{q^3}\sum_{\chi\neq\chi_0}\widehat{1}_A(\overline{\chi})\widehat{1}_B(\chi)\sum_{g\in F_q}\chi(P(g))=$$
$$\mu(A)\mu(B)+$$
$$\frac{1}{q^3}\sum_{\chi\neq\chi_0}\widehat{1}_A(\overline{\chi})\widehat{1}_B(\chi)\sum_{g\in F_q}\chi(P(g)).$$

进而有

$$\left|\frac{1}{q}\sum_{g\in F_q}\mu(A_q\cap(B_q+P(g)))-\right.$$
$$\mu(A_q)\mu(B_q)|=$$
$$\left|\frac{1}{q^3}\sum_{\chi\neq\chi_0}\widehat{1}_A(\overline{\chi})\widehat{1}_B(\chi)\sum_{g\in F_q}\chi(P(g))\right|.$$

接下来我们对

$$\left|\frac{1}{q^3}\sum_{\chi\neq\chi_0}\widehat{1}_A(\overline{\chi})\widehat{1}_B(\chi)\sum_{g\in F_q}\chi(P(g))\right|$$

的上界进行估计. 不妨记该上界为 $\kappa(q)$. 由三角不等式,我们有

$$\left|\frac{1}{q^3}\sum_{\chi\neq\chi_0}\widehat{1}_A(\overline{\chi})\widehat{1}_B(\chi)\sum_{g\in F_q}\chi(P(g))\right|\leqslant$$
$$\frac{1}{q^3}\sum_{\chi\neq\chi_0}|\widehat{1}_A(\overline{\chi})||\widehat{1}_B(\chi)|\left|\sum_{g\in F_q}\chi(P(g))\right| \tag{1}$$

因

$$\sum_{\chi\in\widehat{F}_q}|\widehat{1}_A(\chi)|^2=q\langle\widehat{1}_A,\widehat{1}_A\rangle=$$
$$q^2\langle 1_A,1_A\rangle=q^2\mu(A),$$

由 Cauchy-Schwarz 不等式有

$$\sum_{\chi\neq\chi_0}|\widehat{1}_A(\overline{\chi})||\widehat{1}_B(\chi)|\leqslant$$
$$\sum_{\chi\in\widehat{F}_q}|\widehat{1}_A(\overline{\chi})||\widehat{1}_B(\chi)|\leqslant$$
$$\Big(\sum_{\chi\in\widehat{F}_q}|\widehat{1}_A(\overline{\chi})|^2\sum_{\chi\in\widehat{F}_q}|\widehat{1}_B(\chi)|^2\Big)^{1/2}=$$
$$(q^4\mu(A)\mu(B))^{1/2}\leqslant$$
$$q^2\left(\frac{q+3}{4q}\right)=\frac{q(q+3)}{4} \tag{2}$$

把式(2)代入式(1)可得

$$\frac{1}{q^3}\sum_{\chi\neq\chi_0}|\widehat{1}_A(\overline{\chi})||\widehat{1}_B(\chi)|\left|\sum_{g\in F_q}\chi(P(g))\right|\leqslant$$
$$\frac{(q+3)}{4q^2}\left|\sum_{g\in F_q}\chi(P(g))\right|.$$

接下来,我们给出 $\left|\sum_{g\in F_q}\chi(P(g))\right|$ 的一个上界. 给定有限域F_q到F_p上的任意非平凡加法特征 χ,均存在$h_\chi\in F_q^*$使得对任意 $g\in F_q$,有

$$\chi(P(g))=\chi_1(h_\chi P(g))=\chi_1(h_\chi cg^4).$$

对 $g\in F_q$求和,由引理 2.9 我们有

$$\sum_{g\in F_q}\chi(P(g))=T_{\chi_1}(h_\chi c).$$

于是,当 $q\equiv 5(\mathrm{mod}\ 8)$时,对任意$F_q$上的加法特征 χ,指数和 $\sum_{g\in F_q}\chi(P(g))$ 为方程

$$x^4+2qx^2+8qsx+9q^2-4qs^2=0$$

的根. 接下来我们估计 $\left|\sum_{g\in F_q}\chi(P(g))\right|$ 的上界. 由 Rouche 定理[17]可知,如果存在实数$\tilde{r}$,使得对任意$|x|=\tilde{r}$,不等式

$$|2qx^2+8qsx+9q^2-4qs^2|<\tilde{r}^4 \tag{3}$$

恒成立,那么方程$x^4+2qx^2+8qsx+9q^2-4qs^2=0$所有的根的模长都小于$\tilde{r}$.

接下来,我们求解满足上述条件的实数$\tilde{r}$的下界. 令$\tilde{r}=r\sqrt{q}$. 那么对任意复数 x 满足条件$|x|=\tilde{r}$,总可以表示为 $x=r\sqrt{q}\mathrm{e}^{\mathrm{i}\theta}$. 于是不等式(3)等价于

$$|2r^2q^2\mathrm{e}^{2\mathrm{i}\theta}+8rqs\sqrt{q}\mathrm{e}^{\mathrm{i}\theta}+9q^2-4qs^2|<r^4q^2 \tag{4}$$

注意到 $q=s^2+4t^2$,于是有$|s|\leqslant\sqrt{q}$. 从而

$$|2r^2q^2\mathrm{e}^{2\mathrm{i}\theta}+8rqs\sqrt{q}\mathrm{e}^{\mathrm{i}\theta}+9q^2-4qs^2|\leqslant$$
$$|2r^2q^2\mathrm{e}^{2\mathrm{i}\theta}|+|8rqs\sqrt{q}\mathrm{e}^{\mathrm{i}\theta}|+|9q^2-4qs^2|\leqslant$$
$$2r^2q^2+8rq^2+9q^2=(2r^2+8r+9)q^2 \tag{5}$$

可以解得,当 $r>2.55254$ 时,$2r^2+8r+9<r^4$成立. 结合式(4)与(5)可知当 $r=2.5526$ 时,不等式(3)成立. 综上所述,我们有

$$\Big|\sum_{g\in F_q}\chi(P(g))\Big|\leqslant 2.5526\sqrt{q}.$$

因而我们可以取

$$\kappa(q)=2.5526\,\frac{(q+3)}{4q^{3/2}}.$$

这样我们就完成了引理的证明.

引理 2.12[12]　设 p 为素数,$k=2t$,其中 t 为正整数. 令 $q=p^k$,F_q为 q 元有限域. 设 $a_1,a_2,\cdots,a_s\in F_q^*$,$s\geqslant 2$,$b\in F_q$,$d$ 是 $q-1$ 的因子且满足 $nd=q-1$. 记 N 为方程$a_1x_1^d+\cdots+a_sx_s^d=b$ 的解的个数. 若存在 t 的因子 r,满足$p^r\equiv -1(\mathrm{mod}\ d)$,则有

(i) 当 $b=0$ 时,

$$N=q^{s-1}+\varepsilon^s q^{\frac{s}{2}-1}(q-1)d^{-1}\sum_{j=0}^{d-1}(1-d)^{v(j)};$$

(ii) 当 $b\neq 0$ 时,

$$N=q^{s-1}-\varepsilon^{s+1}q^{\frac{s}{2}-1}\Big[(1-d)^{\theta(b)}q^{\frac{1}{2}}-$$
$$(q^{\frac{1}{2}}-\varepsilon)d^{-1}\sum_{j=0}^{d-1}(1-d)^{\tau(j)}\Big],$$

其中 $\varepsilon=(-1)^{\frac{t}{r}}$,

$$v(j):=|\{1\leqslant i\leqslant s\mid(\alpha^ja_i)^n=\varepsilon^{\frac{p^r+1}{d}}\lambda\}|,$$
$$\theta(b):=|\{1\leqslant i\leqslant s\mid(a_i)^n=(-b)^n\}|,$$
$$\tau(j)=|\{1\leqslant i\leqslant s\mid(a_i)^n=(\alpha^j)^n\}|,$$

这里 α 是F_q^*的生成元.

3　主要定理的证明

设 p 为 F_q 的特征，k 为 F_q 在素域 F_p 上的扩张次数. 结论成立等价于 $F_q\subseteq\{ax^4+by^4\,|\,x,y\in F_q\}$. 由于方程 $ax^4+by^4=0$ 在 F_q 上总有平凡解(0,0)，即 $0\in\{ax^4+by^4\,|\,x,y\in F_q\}$，我们只需证明 $F_q^*\subseteq\{ax^4+by^4\,|\,x,y\in F_q\}$. 下面我们分三种情形 $p=2$，$p=3$ 及 $p\geqslant5$ 分别讨论.

情形 1　$p=2$. 我们有

$$\gcd(4,q-1)=\gcd(4,2^k-1)=1.$$

由引理 2.7 可得 $\{x\,|\,x\in F_q\}=\{x^4\,|\,x\in F_q\}$. 换句话说，此时任意的 $x\in F_q$ 均可开四次方. 直接验证可知 $(a^{-1}c,0)$ 就是方程 $ax+by=c$ 的解. 从而方程 $ax^4+by^4=c$ 在 F_q 上也有解 $((a^{-1}c)^{\frac{1}{4}},0)$.

情形 2　$p=3$. 若 $k\equiv1 \pmod 2$，我们有 $\gcd(4,q-1)=\gcd(4,3^k-1)=2$. 由引理 2.7，$\{x^2\,|\,x\in F_q\}=\{x^4\,|\,x\in F_q\}$，即方程 $ax^4+by^4=c$ 解的个数不少于方程 $ax^2+by^2=c$ 解的个数，而后者在 F_q 上有解是已知结果，因而方程 $ax^4+by^4=c$ 在 F_q 上也有解. 若 $k\equiv0 \pmod 2$，任取 $c\in F_q^*$，设 N 是方程 $ax^4+by^4=c$ 解的个数，由引理 2.12，

$$N=q-\varepsilon^3\left[(-3)^{\theta(b)}\,q^{\frac{1}{2}}-\frac{1}{4}(q^{\frac{1}{2}}-\varepsilon)\sum\nolimits_{j=0}^{3}(-3)^{\tau(j)}\right],$$

其中 $|\varepsilon|=1$，$\theta(b)\geqslant0$，$\tau(j)\leqslant2$. 简单放缩有

$$N\geqslant q-(-3)^2q^{\frac{1}{2}}-4\times\frac{1}{4}(q^{\frac{1}{2}}+1)(-3)^2\geqslant q-18\,q^{\frac{1}{2}}-9.$$

令 $N>0$，解得 $q\geqslant342$. 因而，当 $q=3^{2t}$，$t\geqslant4$ 时，恒有 $q>342$，即该方程在 F_q 上有解. 经检验，当 $q=81$ 和 729 时，该方程在 F_q 上也有解. 综上，当 $q=3^{2t}$，$t\geqslant2$ 时方程 $ax^4+by^4=c$ 在 F_q 上恒有解.

情形 3　$p\geqslant5$. 若 $q\equiv3 \pmod 4$，则有 $\gcd(4,q-1)=2$. 与情形 2 的讨论类似知方程 $ax^4+by^4=c$ 在 F_q 上也有解. 若 $q\equiv1 \pmod 4$，我们分 $q\equiv1 \pmod 8$ 与 $q\equiv5 \pmod 8$ 两种情况讨论.

令算术函数

$$\kappa(q):=\begin{cases}\dfrac{3}{\sqrt{q}}, & \text{若 } q\equiv1 \pmod 8；\\[2mm] 2.5526\,\dfrac{(q+3)}{4\,q^{3/2}}, & \text{若 } q\equiv5 \pmod 8.\end{cases}$$

记 $A_q=\{ax^4\,|\,x\in F_q\}$，$B_q=\{-by^4\,|\,y\in F_q\}$. 对给定元素 $c\in F_q^*$，令 $P(x)=cx^4$. 若 $q\equiv5 \pmod 8$，我们断言当 $q>139$ 时，如下不等式成立

$$\mu(A_q)\mu(B_q)-\frac{1}{q}\mu(A_q\cap B_q)>\kappa(q)\tag{6}$$

由引理 2.8 可知，$\mu(A_q)>\dfrac{1}{4}$ 且 $\mu(B_q)>\dfrac{1}{4}$. 又当 $q>139$ 时，不等式 $\dfrac{1}{16}-\dfrac{1}{q}>\kappa(q)$ 成立，注意到 $\dfrac{1}{q}\mu(A_q\cap B_q)\leqslant\dfrac{1}{q}$，因而有

$$\kappa(q)+\frac{1}{q}\mu(A_q\cap B_q)<\frac{1}{4^2}<\mu(A_q)\mu(B_q),$$

即断言成立.

若 $q\equiv1 \pmod 8$，同理可得 $q>2335$ 时不等式(6)成立. 下面我们分别定义

$$S=\frac{1}{q}\sum\nolimits_{h\in F_q}\mu(A_q\cap(B_q+P(h))),$$

$$T=\frac{1}{q}\sum\nolimits_{h\in F_q^*}\mu(A_q\cap(B_q+P(h))).$$

由引理 2.10 和 2.11 可知

$$S-\mu(A_q)\mu(B_q)\geqslant-\kappa(q)$$

成立. 因此

$$\begin{aligned}T=&S-\frac{1}{q}\mu(A_q\cap B_q)=\\&(S-\mu(A_q)\mu(B_q))+\\&\left(\mu(A_q)\mu(B_q)-\frac{1}{q}\mu(A_q\cap B_q)\right)>\\&-\kappa(q)+\kappa(q)=0.\end{aligned}$$

因此时 $T>0$，则至少存在一个元素 $h\in F_q^*$ 使得 $\mu(A_q\cap(B_q+P(h)))>0$. 从而存在 $x_1,x_2\in F_q$ 使得 $ax_1^4=-bx_2^4+ch^4$. 进一步可得

$$c=a(x_1h^{-1})^4+b(x_2h^{-1})^4.$$

从而对任意的 $c\in F_q^*$，都有 $c\in\{ax^4+by^4\,|\,x,y\in F_q\}$.

综上，我们证明了当 $q\equiv1 \pmod 8$ 且 $q>2335$ 以及 $q\equiv5 \pmod 8$ 且 $q>139$ 时，$F_q\subseteq\{ax^4+by^4\,|\,x,y\in F_q\}$. 其他情形可借助 Magma 直接验证知若 $q\neq5,9,13,17,25,29$，方程 $ax^4+by^4=c$ 在 F_q 上恒有解. 至此，我们完整地给出了定理的证明.

参考文献：

[1]　Bergelson V, Best A, Iosevich A. Sums of powers in large finite fields: a mix of methods[EB/OL]. [2020-09-20]. https://arxiv.org/pdf/2009.09518.pdf.

[2]　Cauchy A. Recherches sur les nombres [J]. J Éc polytech Math, 1813, 9: 99.

[3]　Hong S F, Zhu C X. On the number of zeros of di-

agonal cubic forms over finite fields[J]. Forum Math，2021，33：697.

[4] Lagrange J L. Nouvelle méthode pour résoudre les problémes indéterminésen nombres entiers [J]. Mémoires Acad Roy Oeuvres，1868，2：655.

[5] Lidl R，Niederreiter H. Finite fields [M]. New York：Cambridge University Press，1997.

[6] Myerson G，On the number of zeros of diagonal cubicforms [J]. J Number Theory，1979，11：95.

[7] Roman S. Field theory [M]. New York：Springer-Verlag，2006.

[8] Singh S. Analysis of each integer as sum of two cubes in a finite integral domain [J]. Indian J Pure Appl Math，1973，6：29.

[9] Skolem T. Zwei Sätzeüber kubische Kongruenzen [J]. Norske Vid Selsk Forh，1937，10：89.

[10] Small C. Sums of powers in large finite fields [J]. Proc Amer Math Soc，1977，65：35.

[11] Weber H. Lehrbuch der algebra[M]. Chelsea：AMS，1899.

[12] Wolfmann J. The number of solutions of certain diagonal equations over finite fields [J]. J Number Theory，1992，42：247.

[13] Pérez M，Privitelli M. Estimates on the number of F_q-rational solutions of variants of diagonal equations over finite fields [J]. Finite Fields Th App，2020，68：101728.

[14] Zhao J Y，Zhao Y，Niu Y J. On the number of solutions of two-variable diagonal quartic equations over finite fields [J]. AIMS Math，2020，5：2979.

[15] Zhao J Y，Hong S F，Zhu C X. The number of rational points of certain quartic diagonal hypersurfaces over finite fields [J]. AIMS Math，2020，5：2710.

[16] Zhang W P，Hu J Y. The number of solutions of the diagonal cubic congruence equation mod p [J]. Math Rep，2018，20：73.

[17] Ahlfors L. Complex analysis [M]. New York：McGraw-Hill，1979.

引用本文格式：

中　文：黄宝盛，吴荣军，谭千蓉，等. 有限域上四次对角方程 $ax^4+by^4=c$ 解的存在性[J]. 四川大学学报：自然科学版，2022，59：011001.

英　文：Huang B S，Wu R J，Tan Q R，*et al*. On the existence of solutions of diagonal quartic equation $ax^4+by^4=c$ over finite field [J]. J Sichuan Univ：Nat Sci Ed，2022，59：011001.