arXiv:2301.04063v1 [math.NT] 10 Jan 2023

有限域中丢番图 m-元组的数量

IGOR E. SHPARLINSKI

Abstract. 我们采用一种新的论证，改进了有限域中丢番图 m-元组数量的渐近公式中的误差项。该渐近公式由 A. Dujella 和 M. Kazalicki（2021年）以及 N. Mani 和 S. Rubinstein-Salzedo（2021年）给出。

1. Introduction

1.1. 动机与设定。我们回顾丢番图 m-元组的经典定义：它是一个向量 $(a_1, \dots, a_m) \in \mathbb{N}^m$，满足所有平移后的乘积 $a_i a_j + 1$, $1 \leqslant i < j \leqslant m$ 都是完全平方数。

经过多位作者的一系列中间成果，关于丢番图五元组集合有限性的这一长期猜想，最终在 Dujella 的一项杰出工作中得以证明[3], ；他还证明了丢番图六元组不存在。最近，He、Togb´e 和 Ziegler [8] 证明了丢番图五元组不存在，另见[1]。自然而然，这些结果促使人们研究这一概念在其他代数域中的推广，例如有理数集合或曲线上的点，也包括许多其他方向，参见 [2,5,6,11]及其中的参考文献。这一概念也很容易推广到有限域的情形，参见 [4,7,13]。

设 q 是一个奇素数幂，并设 $\mathbb{F}_q$ 是含有 q 个元素的有限域。

对于 $r \in \mathbb{F}_q^*$，我们称一个 m-元组 $(a_1, \dots, a_m) \in \mathbb{F}_q^m$构成有限域 $\mathbb{F}_q$ 中带有平移量 r 的丢番图 m-元组，若所有 $m(m-1)/2$ 平移后的乘积 $a_i a_j + r$ 在 $\mathbb{F}_q$中都是完全平方数。

注 1.1. 我们注意到，通常会将零值从抽取 a_1、.....、 a_m 的定义域中排除。不过，在下面的计数结果中，这并无影响，同时还能简化记号。特别是，在 $\mathbb{F}_q$ 上这类 m 元组中含有一个零

2020 年数学主题分类。11D09、11D79、11L40。关键词和短语。丢番图 m-元组、有限域、特征和。

项（其数量至多为 mq^{m-1}）的总数可以并入渐近公式的误差项中。

令 $N_r(m,q)$ 表示有限域 m 中具有平移量 $\mathbb{F}_q$ 的互异丢番图 r-元组的数量。Dujella 和 Kazalicki 已证明 [4]，对于 $r = 1$ 以及素数 p，有

$$N_1(m,p) = 2^{-m(m-1)/2}p^m + o(p^m). \tag{1.1}$$

利用 Dujella 和 Kazalicki 的一些想法，[4], Mani 和 Rubinstein-Salzedo [13, 定理 5。1] 给出了 $N_r(2,q)$ 和 $N_r(3,q)$ 的显式公式，而 $m \geqslant 4$ 则给出了比（1.1）更精确的渐近公式

$$N_r(m,q) = 2^{-m(m-1)/2}q^m + O\left(q^{m-1/2}\right), \tag{1.2}$$

其中隐含常数可能依赖于 m，该结论对任意 $r \in \mathbb{F}_q^*$ 都成立（并且很容易看出，对任意奇素数幂 q 也成立，而不只是对素数 $q = p$，如 [13] 中所述）。我们还注意到，界（1.2）可在 Dujella 和 Kazalicki 的初始方法中推出 [4]，只需使用 Lang-Weil 界的一个版本 [12]。

1.2. 新的界。 这里我们将证明，通过一些简单的论证，可以改进（1.2）中的误差项界。

定理 1.2. 对于固定的 $m \geqslant 4$，一致地对所有 $r \in \mathbb{F}_q^*$，我们有

$$N_(m,q) = 2^{-m(m-1)/2}q^m + O\left(q^{m-1}\right),$$

其中，隐含常数可以依赖于 m。

与 [13] 一样，我们的证明基于对多项式的乘法特征和应用 Weil 界；例如，参见 [9,定理 11.23]。

2. Proof of Theorem 1.2

2.1. 初步变换。由于满足某个条件的 m-元组 $(a_1, \ldots, a_m)$ 有 $O(q^{m-1})$ 种选择，或者对于某个 $1 \leqslant i \leqslant m$ 满足 $a_i = 0$ 的情形有相应选择，因此，依照 [13], 的论证，我们写作

$$N_r(m,q) = 2^{-m(m-1)/2} \sum_{a_1,\ldots,a_m \in \mathbb{F}_q^*} \prod_{1 \leqslant i < j \leqslant m} \left(1 + \chi\left(a_i a_j + r\right)\right) + O\left(q^{m-1}\right),$$

其中 χ 是 $\mathbb{F}_q$的二次特征，我们请参阅 [9, 第 3] 章，了解特征的相关背景。因此

$$N_r(m,q) = 2^{-m(m-1)/2}q^m + \sum_{\substack{\boldsymbol{\varepsilon}\in\{0,1\}^{m(m-1)/2}\\ \boldsymbol{\varepsilon}\neq\mathbf{0}}} R(\boldsymbol{\varepsilon}) + O\left(q^{m-1}\right), \tag{2.1}$$

其中，对于 $\boldsymbol{\varepsilon} = (\varepsilon_{i,\,j})_{1\leqslant i<j\leqslant m} \in \{0,1\}^m$

$$R(\boldsymbol{\varepsilon}) = \sum_{a_1,\dots,a_m\in\mathbb{F}_q^*} \prod_{1\leqslant i<j\leqslant m} \chi\left(a_ia_j + r\right)^{\varepsilon_{i,j}}. \tag{2.2}$$

现在固定 $\boldsymbol{\varepsilon} \in \{0,1\}^{m(m-1)/2}$，使得 $\boldsymbol{\varepsilon} \neq \mathbf{0}$，并估计 $R(\boldsymbol{\varepsilon})$。重新对变量 a_1、……、a_m 编号后可知，不失一般性，我们可以假设

$$\varepsilon_{1,2} = 1. \tag{2.3}$$

现在根据指数 $\varepsilon_{i,\,j}$ 是否为零，考虑以下两种情形，其中 $2 \leqslant i < j \leqslant m$。

2.2. 消失指数 $\varepsilon_{i,\,j}$，其中 $2 \leqslant i < j \leqslant m$。假设

$$\varepsilon_{i,j} = 0, \qquad \text{for all } 2 \leqslant i < j \leqslant m. \tag{2.4}$$

于是可知，在条件（2.4）下，（R（$\boldsymbol{\varepsilon}$）在（2.2）中的表达式可简化为

$$\begin{aligned} R(\boldsymbol{\varepsilon}) &= \sum_{a_1,\dots,a_m\in\mathbb{F}_q^*} \prod_{2\leqslant j\leqslant m} \chi\left(a_1a_j + r\right)^{\varepsilon_{1,j}} \\ &= \sum_{a_1\in\mathbb{F}_q^*} \prod_{2\leqslant j\leqslant m} \sum_{a_j\in\mathbb{F}_q^*} \chi\left(a_1a_j + r\right)^{\varepsilon_{1,j}}. \end{aligned}$$

因此，将关于 a_3，……，a_m 的和粗略估计为 $q-1$，并回顾我们的假设（2.3），可得

$$|R(\boldsymbol{\varepsilon})| \leqslant (q-1)^{m-2} \sum_{a_1\in\mathbb{F}_q^*} \left| \sum_{a_2\in\mathbb{F}_q^*} \chi\left(a_1a_2 + r\right) \right|.$$

显然，对于每个 $a_1 \in \mathbb{F}_q^*$，我们都有

$$\begin{aligned} \sum_{a_2\in\mathbb{F}_q^*} \chi\left(a_1a_2 + r\right) &= \sum_{a\in\mathbb{F}_q^*} \chi\left(a + r\right) \\ &= \sum_{a\in\mathbb{F}_q} \chi(a) - \chi(1) = \sum_{a\in\mathbb{F}_q} \chi(a) - 1 = -1. \end{aligned}$$

因此我们得到

$$|R(\boldsymbol{\varepsilon})| \leqslant (q-1)^{m-1} \tag{2.5}$$

在这种情况下。

2.3. 非零指数 $\varepsilon_{i,j}$ 满足 $2 \leqslant i < j \leqslant m$。现在我们假设

$$\varepsilon_{i,j} \neq 0, \qquad \text{for some } 2 \leqslant i < j \leqslant m. \tag{2.6}$$

我们将 $R(\boldsymbol{\varepsilon})$ 写作

$$R(\boldsymbol{\varepsilon}) = \sum_{a_1,\ldots,a_m \in \mathbb{F}_q^*} \prod_{2 \leqslant j \leqslant m} \chi\left(a_1 a_j + r\right)^{\varepsilon_{1,j}} \prod_{2 \leqslant i < j \leqslant m} \chi\left(a_i a_j + r\right)^{\varepsilon_{i,j}}.$$

注意，对任意 $b \in \mathbb{F}_q^*$，映射

$$(a_1, a_2, \ldots, a_m) \mapsto (a_1/b, a_2 b, \ldots, a_m b)$$

是 $\mathbb{F}_p^m$ 上的一个置换。因此

$$R(\boldsymbol{\varepsilon}) = (p-1)^{-1} \sum_{b \in \mathbb{F}_q^*} \sum_{a_1,\ldots,a_m \in \mathbb{F}_q^*} \prod_{2 \leqslant j \leqslant m} \chi\left(a_1 a_j + r\right)^{\varepsilon_{1,j}} \prod_{2 \leqslant i < j \leqslant m} \chi\left(a_i a_j b^2 + r\right)^{\varepsilon_{i,j}},$$

现在我们将其重新整理为

$$R(\boldsymbol{\varepsilon}) = (q-1)^{-1} \sum_{a_2,\ldots,a_m \in \mathbb{F}_q^*} S(a_2, \ldots, a_m) T(a_2, \ldots, a_m),$$

其中

$$S(a_2, \ldots, a_m) = \sum_{a_1 \in \mathbb{F}_q^*} \chi\left(\prod_{2 \leqslant j \leqslant m} \left(a_1 a_j + r\right)^{\varepsilon_{1,j}}\right),$$

$$T(a_2, \ldots, a_m) = \sum_{b \in \mathbb{F}_q^*} \chi\left(\prod_{2 \leqslant i < j \leqslant m} \left(a_i a_j b^2 + r\right)^{\varepsilon_{i,j}}\right).$$

我们现在考察多项式

$$F_{a_2,\ldots,a_m}(X) = \prod_{2 \leqslant j \leqslant m} \left(a_j X + r\right)^{\varepsilon_{1,j}},$$

$$G_{a_2,\ldots,a_m}(X) = \prod_{2 \leqslant i < j \leqslant m} \left(a_i a_j X^2 + r\right)^{\varepsilon_{i,j}}.$$

由于我们的假设（2.3）和（2.6），这两个多项式的次数均为正。

此外，显然，满足以下条件的 $(m-1)$ 元组 $(a_2, \ldots, a_m) \in \mathbb{F}_q^{m-1}$ 至多有 $O(q^{m-2})$ 种选择：多项式 $F_{a_2,\ldots,a_m}(X)$ 和 $G_{a_2,\ldots,a_m}(X)$ 中至少有一个在 $\mathbb{F}_q$ 的代数闭包中是完全平方。在这种情况下，我们对两个和 $S(a_2, \ldots, a_m)$

和 $T(a_2,\dots,a_m)$ 进行平凡估计，得 $q-1$。因此，这类和对 $R(\varepsilon)$ 的贡献为

$$A = O\left((q-1)^{-1}q^{m-2}(q-1)^2\right) = O(q^{m-1}). \tag{2.7}$$

对于 $(a_2,\dots,a_m) \in \mathbb{F}_q^{m-1}$的其他取值，根据 Weil 界，例如参见 [9,定理 11。23], 我们有

$$S(a_2,\dots,a_m), T(a_2,\dots,a_m) = O(q^{1/2}).$$

因此，这些和对 $R(\varepsilon)$ 的贡献为

$$B = O\left((q-1)^{-1}q^{m-1}\left(q^{1/2}\right)^2\right) = O(q^{m-1}). \tag{2.8}$$

结合 (2.7) 和 (2.8)，我们得到

$$R(\varepsilon) = A + B = O(q^{m-1}) \tag{2.9}$$

在此情形下。

2.4. 证明的结束。 将界 (2.5) 和 (2.9) 代入 (2.1) 后即可立即得到所需结果。

3. Comments

不难看出，所有隐含常数都可以显式求出。因此，我们可以利用这一论证估计满足以下条件的最小 q （关于 m）：对于所有 $r \in \mathbb{F}_q^*$, $N_r(m,q) > 0$。不过，对于这个问题，Dujella 和 Kazalicki 的归纳方法 [4, 定理 17]似乎更有效。

既然我们有多元特征和，自然也可以尝试通过采用某种形式的德利涅界来改进定理 1.2，例如参见 [10]。遗憾的是，我们的多项式具有高维奇异点集，这似乎妨碍了这种方法。

Acknowledgement

作者谨此感谢 Andrej Dujella 提出的若干非常有益的意见和建议。

本研究得到了澳大利亚研究理事会的资助（Discovery 项目 DP200100355）。

References

[1]N. C. Bonciocat、M. Cipu 和 M. Mignotte, 《不存在丢番图$D(-1)$-四元组》, 《伦敦数学会杂志》**105** (2022) 63–99。1[2] A. B. Dixit、S. Kim、M. Ra m Murty, 《广义丢番图 m-元组》, 《美国数学会会刊》**150** (2022), 1455–1465。1[3] A. Dujella, 《丢番图五元组只有有限多个》, 《纯粹与应用数学杂志》**566** (2004), 183–214。1

[4] A. Dujella 和 M. Kazalicki, 《有限域中的丢番图 m 元组与模形式》, 《数论研究》7 (2021), 论文编号 3, 1–24。1, 2, 5[5] A. Dujella、M. Kazalicki、M. Miki´c 和 M. Szikszai, 《存在无穷多个有理丢番图六元组》, 《国际数学研究通知》2017 (2017), 490–508。1[6] S. Gupta, 《虚二次域中的 $D(-1)$ 元组》, 《匈牙利数学学报》164 (2021), 556–569。1[7] T. Hammonds、S. Kim、S. J. Miller、A. Nigam、K. Onghai、D. Saikia 和 L. M. Sharma, 《有限域中的 k-丢番图 m-元组》, 《国际数论杂志》, 即将出版。1[8] B. He、A. Togb´e 和 V. Ziegler, 《不存在丢番图五元组》, 《美国数学会会刊》371 (2019), 6665–6709。1[9] H. Iwaniec 和 E. Kowalski, 《解析数论》, 美国数学会, 普罗维登斯, 罗得岛州, 2004年。2, 3, 5[10] N. M. Katz, 《非奇异乘法特征和的估计》, 《国际数学研究通知》2002 (2002), 333–349。5[11] M. Kazalicki 和 B. Naskr̨ecki, 《丢番图三元组与 $K3$ 曲面》, 《数论杂志》236 (2022), 41–70。1[12] S. Lang 和 A. Weil, 《有限域中代数簇的点数》, 《美国数学杂志》76 (1954年), 819–827。2[13] N. Mani 和 S. Rubinstein-Salzedo, 《 $\mathbb{Z}_p$上的丢番图元组》, 《算术学报》197 (2021), 331–351。1, 2

School of Mathematics and Statistics, University of New SouthWales, Sydney NSW 2052, Australia电子邮箱：igor.shparlinski@unsw.edu.au