An 不完全混合特征和及其应用的估计 s

Arpan Chandra Mazumder[a,1]，Giorgos Kapetanakis[b,*]，Sushant Kala[c]，Dhiren Kumar Basnet[a]

[a]特兹普尔大学数学科学系，印度阿萨姆邦特兹普尔，*784028*[b]色萨利大学数学系，拉米亚-雅典旧国道*3*公里处，*35100*，希腊拉米亚[c]数学科学研究所（*HBNI*）数学系，*CIT*校区，*IV Cross Road*，金奈，*600113*，印度

arXiv:2603.02118v1 [math.NT] 2 Mar 2026

摘要

设 q 为素数幂， $m>1$ 为任意整数。设$\mathbb{F}_{q^m}$ 为阶为 q^m 的有限域，且$\theta \in \mathbb{F}_{q^m}$ 满足$\mathbb{F}_{q^m}=\mathbb{F}_q(\theta)$。我们利用函数域方法，得到混合特征和 $\sum_{x\in\mathbb{F}_q}\chi(\theta+x)\psi(x)$ 的一个非平凡上界，其中 χ 和 ψ 分别是 $\mathbb{F}_{q^m}$ 和 $\mathbb{F}_q$上的乘法特征与加法特征。作为主要结果的应用，我们证明，对于固定的 m 以及满足某些条件的充分大的素数幂q，$\mathbb{F}_{q^m}/\mathbb{F}_q$ 对本原正规元具有弱直线性质。特别地，我们的结果强化了已有结果。

关键词：特征和，本原元，正规元，直线性质，平移性质，迹

2020 数学学科分类： 11T30, 11T23, 12E20

1. 引言

全文中，设 p 为素数， q 为 p 的幂， m 为正整数。用$\mathbb{F}_q$表示阶为 q 、特征为 p 的有限域，用 $\mathbb{F}_{q^m}$ 表示 $\mathbb{F}_q$ 的 m次扩域。乘法群 $\mathbb{F}_{q^m}^*$ 是循环群，该群的生成元称为 $\mathbb{F}_{q^m}$的本原元。称元素 $\theta\in\mathbb{F}_{q^m}$ 正规于 $\mathbb{F}_q$，如果它关于 $\mathbb{F}_q$的全部共轭元所成的集合，即集合 $\{\theta,\theta^q,\ldots,\theta^{q^{m-1}}\}$，构成 $\mathbb{F}_{q^m}$ 在 $\mathbb{F}_q$上的一组基。称元素 $\theta\in\mathbb{F}_{q^m}$ 为本原正规元，如果它既是本原元，又正规于 $\mathbb{F}_q$。

设 $\mathbb{F}_{q^m}$ 是 $\mathbb{F}_q$上的 m 次扩张。若 $\mathbb{F}_{q^m}=\mathbb{F}_q(\theta)$，则称元素 $\theta\in\mathbb{F}_{q^m}$ 为扩张$\mathbb{F}_{q^m}/\mathbb{F}_q$的生成元。对 $\mathbb{F}_{q^m}/\mathbb{F}_q$的任一生成元 θ，我们称集合 $\{\theta+x:\ x\in\mathbb{F}_q\}$为 θ 在 $\mathbb{F}_q$ 上的平移集（因为从几何上看，该集合可解释为 $\mathbb{F}_q$的一个平移）。对任一特定扩张$\mathbb{F}_{q^m}/\mathbb{F}_q$，我们将如下问题称为平移问题：对 $\mathbb{F}_{q^m}$ 的每一个生成元 θ，是否存在 $\mathbb{F}_{q^m}$ 中具有某种类型且形如 $\theta+x$的元素，其中 $x\in\mathbb{F}_q$；若答案为肯定，则称扩张$\mathbb{F}_{q^m}/\mathbb{F}_q$对该类元素具有平移性质（$TP$）。

同样，对于 $\mathbb{F}_{q^m}/\mathbb{F}_q$ 和 $\alpha\in\mathbb{F}_{q^m}^*$的任意生成元 θ，我们称集合 $\{\alpha(\theta+x):\ x\in\mathbb{F}_q\}$ 为 θ和 α 在 $\mathbb{F}_q$ 上的直线（因为该集合可以解释为 $\mathbb{F}_{q^m}$ 中的一条直线）。对于任意给定的扩张 $\mathbb{F}_{q^m}/\mathbb{F}_q$，我们将以下问题称为直线问题：对于每个 $\alpha\in\mathbb{F}_{q^m}^*$ 以及 $\mathbb{F}_{q^m}$ 的每个生成元 θ，是否存在 $\mathbb{F}_{q^m}$ 中某种特定类型、且形式为 $\alpha(\theta+x)$ 的元素，其中$x\in\mathbb{F}_q$? 如果答案为肯定，我们就说扩张 $\mathbb{F}_{q^m}/\mathbb{F}_q$ 对这类元素具有直线性质（LP）。

最后，若在上述设定中我们只考虑 $\alpha\in\mathbb{F}_q^*$这一情形，则称之为弱直线问题，并称扩张 $\mathbb{F}_{q^m}/\mathbb{F}_q$对这类元素具有弱直线性质（$WLP$），

*通讯作者电子邮箱：arpan10@tezu.ernet.in（Arpan Chandra Mazumder）、kapetanakis@uth.gr（GiorgosKapetanakis）、sushant@imsc.res.in（Sushant Kala）、dbasnet@tezu.ernet.in（Dhiren Kumar Basnet）[1]第一作者获得 DST INSPIRE 奖学金资助，资助编号为 DST/INSPIRE Fellowship/2021/IF210206。

分别。因此，一旦我们注意到 $\alpha = 1$ 对应于平移性质，且条件$\alpha \in \mathbb{F}_{q^m}^m$、 $\alpha \in \mathbb{F}_q^*$ 和 $\alpha = 1$ 的强度依次递增，显然

$$LP \Rightarrow WLP \Rightarrow TP.$$

值得注意的是，Rúa [1, 2] 成功地将有限域扩张中本原元的平移性质与半域中本原元的存在联系起来；半域是一种具有乘法单位元的有限非结合除环。这引发了人们对有限域扩张中平移性质（及其推广）的进一步关注。

1937年，Davenport [3] 给出了如下界

$$\left| \sum_{x \in \mathbb{F}_p} \chi(\theta + x) \right| \ll p^{1 - \frac{1}{2(m+1)}}$$

其中， χ 是 $\mathbb{F}_q$的非平凡乘法特征标， $m > 1$ 是任意整数，且 $\mathbb{F}_q = \mathbb{F}_{p^m} = \mathbb{F}_p(\theta)$。由此可知，在（充分大的）素域上的扩张具有本原元的平移性质。1953年，Carlitz [4] 将上述结果推广至任意有限域扩张（不一定是素域上的扩张）。以下是本原元研究中的一项经典结果。

定理 1.1 (Davenport-Carlitz)。设 $m > 1$ 为整数。存在某个 $TP(m)$，使得对于每个素数幂 $q > TP(m)$，扩张 $\mathbb{F}_{q^m}/\mathbb{F}_q$都具有本原元的平移性质。

1989 年，Katz [5] 给出了以下估计，适用于一类特征和；这些特征和是 Chung [6]构造的某些图的邻接矩阵的特征值。

定理 1.2 (Katz)。设 χ 是 $\mathbb{F}_{q^m}^*$ 上的任意非平凡乘法特征，且 θ 在 $\mathbb{F}_{q^m}$中是一个生成元$\mathbb{F}_{q^m}/\mathbb{F}_q$。那么

$$\left| \sum_{x \in \mathbb{F}_q} \chi(\theta + x) \right| \leq (m-1)q^{1/2}.$$

此外，Cohen [7]于 2010 年利用这一结果，证明了定理 1.1 的一个自然推广。

定理 1.3 (Cohen)。设 $m > 1$ 是一个整数。存在某个 $LP(m)$，使得对于每个素数幂 $q > LP(m)$，扩张 $\mathbb{F}_{q^m}/\mathbb{F}_q$ 都具有本原元的直线性质。

最近，Cohen 和 Kapetanakis [8] 将定理 1.1 和 1.3 推广到了 r-本原元，即 $\mathbb{F}_{q^m}$ 中乘法阶为 $(q^m - 1)/r$ 的元素，其中必然有 $r \mid q^m - 1$。

定理 1.4 (Cohen-Kapetanakis)。设 $m > 1$ 和 r 为整数。存在某个 $LP_r(m)$，使得对于每个满足性质 $r \mid q^m - 1$的素数幂 $q > LP_r(m)$，扩张 $\mathbb{F}_{q^m}/\mathbb{F}_q$ 都具有关于 r-本原元的直线性质。至于关于 r-本原元的平移性质，对于某个 $TP_r(m) \leq LP_r(m)$，同样的结论也成立。

受上述关于有限域上本原元直线性质和平移性质的一系列杰出结果，以及作为这些结果理论基础的特征和估计的启发，我们研究本原正规元的直线性质和平移性质。为此，注意到 Davenport [3] 和 Katz [5]的结果只涉及乘法特征。然而，由于正规性是 $\mathbb{F}_{q^m}$的加法结构的一种性质，我们将遇到混合特征和估计，也就是说，其中还会出现加法特征。

1990年，Perel'muter 和 Shparlinski [9] 证明，若 θ 是扩张 $\mathbb{F}_{p^m}/\mathbb{F}_p$ 的生成元且$a \in \mathbb{F}_p$，则

$$\left| \sum_{t \in \mathbb{F}_p} \chi(\theta + t) \exp(2\pi i a t/p) \right| \leq m p^{1/2}, \tag{1.1}$$

其中 χ 是$\mathbb{F}_{p^m}$上的非平凡乘法特征。请注意，上述结果适用于素域上的有限域扩张；尽管 $\psi(t) = \exp(2\pi iat/p)$ 是一种加法特征，但它并非任意的加法特征。

2014年，Fu 和 Wan [10] 得到了如下结果。

定理1.5 (Fu-Wan)。取 f、$g \in \mathbb{F}_{q^m}(x)$ 为最简形式。此外，令 $D_1 = \deg(f)$，$D_2 = \max(\deg(g),0)$，D_3 为 g的分母的次数，D_4 为 g 的分母中与 f的分子和分母均互素部分的次数。设 χ 是 $\mathbb{F}_{q^m}$ 上的乘法特征，ψ 是 $\mathbb{F}_q$上的非平凡加法特征。若 $\mathrm{Tr}_{q^m/q}(g)$ 不具有如下形式：对某个 $r \in \mathbb{F}_q(x)$而言为 $r^q - r$，则

$$\left| \sum_{t\in\mathbb{F}_q, f(t)\neq 0,\infty, g(t)\neq\infty} \chi(f(t))\psi(\mathrm{Tr}_{q^m/q}(g(t))) \right| \leq (m(D_1 + D_3 + D_4) + D_2 - 1)q^{1/2}.$$

因此可以得到：给定 θ 为 $\mathbb{F}_{q^m}/\mathbb{F}_q$的一个生成元，$\chi$ 为 $\mathbb{F}_{q^m}$上的乘法特征，且 ψ 为 $\mathbb{F}_q$上的非平凡加法特征，则

$$\left| \sum_{t\in\mathbb{F}_q} \chi(\theta + t)\psi(t) \right| \leq mq^{1/2}. \tag{1.2}$$

然而，值得指出的是，Fu 和 Wan [10], 在定理1.5的证明中采用了 ℓ-进上同调理论，而 Perel'muter 和 Shparlinski [9], 在公式（1.1）的证明中使用了更为简单的函数域论证。综上所述，本文的目标首先是使用更为简单的函数域论证证明公式（1.2）（同时涵盖 χ 非平凡且 ψ 平凡的情形），具体如下。

定理 1.6. 设 χ 为$\mathbb{F}_{q^m}$ 的乘法特征，ψ 为 $\mathbb{F}_q$的加法特征，且二者不全为平凡特征。此外，设 θ 为扩张 $\mathbb{F}_{q^m}/\mathbb{F}_q$的生成元。则式(1.2)成立。

在此我们强调，ψ 为平凡而 χ 非平凡的情形已由定理 1.2 涵盖。我们的方法本质上推广了这一结果，同时更为简单、更为初等。此外值得注意的是，定理 1.6 最近在 [11]中被用于对 Morgan-Mullen 猜想[12]的最新攻关。

随后，我们利用定理 1.6 来探讨扩张 $\mathbb{F}_{q^m}/\mathbb{F}_q$ 是否对本原正规元具有直线性质。具体而言，我们得到如下结果。

定理1.7. 固定一个素数 m。存在整数 $WLPN(m)$，使得对每一个模 m本原的素数幂$q \geq WLPN(m)$，扩张$\mathbb{F}_{q^m}/\mathbb{F}_q$对本原正规元具有弱直线性质。对于某些 $TPN(m) \leq WLPN(m)$，关于本原正规元的平移性质，同样成立。

本文的组织结构如下。第2节介绍后文将用到的背景知识。在第3节中，我们将式（1.1）的混合特征和估计推广到所有素数幂 q，同时考虑 χ 为平凡特征的情形，从而得到定理 1.6。在第4节中，我们应用这一界证明定理4.2，即定理1.7的一个技术性推广。在第5节中，我们利用定理4.2得到定理1.7。最后，我们在第6节讨论本工作的可能推广。

2. 预备知识

本节介绍建立我们的结果所必需的背景信息。有关本节前三个小节中所述事实的更多细节和详细证明，感兴趣的读者可参阅权威教科书，例如 [13, 14] 。

2.1. 迹函数

我们先定义扩张 $\mathbb{F}_{q^m}/\mathbb{F}_q$ 的迹，即函数

$$\mathrm{Tr}_{q^m/q}:\mathbb{F}_{q^m}\to\mathbb{F}_q; x\mapsto\sum_{i=0}^{m-1}x^{q^i}.$$

众所周知，迹函数是满射、 $\mathbb{F}_q$-线性的，并且具有传递性，也就是说，对于 a， $b\in\mathbb{F}_q$ 和x， $y\in\mathbb{F}_{q^m}$，有

$$\mathrm{Tr}_{q^m/q}(ax+by)=a\,\mathrm{Tr}_{q^m/q}(x)+b\,\mathrm{Tr}_{q^m/q}(y)$$

并且，若有限域塔为 $\mathbb{F}_q\subseteq\mathbb{F}_{q^n}\subseteq\mathbb{F}_{q^m}$，那么对于 $x\in\mathbb{F}_{q^m}$,

$$\mathrm{Tr}_{q^m/q}(x)=\mathrm{Tr}_{q^n/q}\left(\mathrm{Tr}_{q^m/q^n}(x)\right).$$

注2.1。 在 直线的语境下，迹函数的行为非常容易预测。为了解这一点， ，取函数

$$\mathrm{Tr}_{q^m/q}:\{\alpha(\theta+x),x\in\mathbb{F}_q\}\to\mathbb{F}_q; a\mapsto\mathrm{Tr}_{q^m/q}(a)$$

并注意到 $\mathrm{Tr}^{q^m/m}(\alpha(\theta+x))=\mathrm{Tr}^{q^m/m}(\alpha\theta)+x\mathrm{Tr}^{q^m/m}(\alpha)$。因此，若 $\mathrm{Tr}^{q^m/q}(\alpha)\neq 0$，它就是一个双射；否则它是常值函数。换言之，具有指定迹的元素的直线性质是平凡的，因此无法与正规性等其他性质有意义地结合起来。

2.2. 有限域特征

在我们的研究中，本原元和正规元的特征函数起着重要作用。要表示这些函数，需要有限阿贝尔群的特征这一概念。

定义 2.2. 设 $\mathbb{G}$ 是一个有限阿贝尔群。群 $\mathbb{G}$ 的特征 χ 是从 $\mathbb{G}$ 到 $\mathbb{S}^1$ 的同态，其中 $\mathbb{S}^1:=\{z\in\mathbb{C}:|z|=1\}$ 是模长为 1 的复数乘法群，即对于所有 a_1， $a_2\in\mathbb{G}$，都有 $\chi(a_1a_2)=\chi(a_1)\chi(a_2)$。特殊特征 $\chi_0:\mathbb{G}\to\mathbb{S}^1$ 定义为对所有 $a\in\mathbb{G}$ 均有 $\chi_0(a)=1$，称为 $\mathbb{G}$ 的平凡特征。

在有限域 $\mathbb{F}_{q^m}$ 中有两种主要的群结构：一种是加法群 $\mathbb{F}_{q^m}$ ，另一种是乘法群 $\mathbb{F}^*_{q^m}$。因此，对应这两种群结构，我们有两类特征：一种是 $\mathbb{F}_{q^m}$ 上的任意加法特征，记作 ψ ；另一种是 $\mathbb{F}^*_{q^m}$ 上的任意乘法特征，记作 χ。 $\mathbb{F}_{q^m}$ 的典范特征定义为

$$\psi_1:\mathbb{F}_{q^m}\to\mathbb{S}^1;\ a\mapsto e^{2\pi i\,\mathrm{Tr}_{q^m/p}(a)/p},$$

且它是 $\mathbb{F}_{q^m}$上的一个加法特征，而 $\mathbb{F}_{q^m}$ 的所有加法特征都具有如下形式：

$$\psi_c:\mathbb{F}_{q^m}\to\mathbb{S}^1;\ a\mapsto\psi_1(ca),$$

其中 $c\in\mathbb{F}_{q^m}$为某个元素，参见 [13]中的定理 5.7。与 $\mathbb{F}^*_{q^m}$ 相关的乘法特征按照以下规则从 $\mathbb{F}^*_{q^m}$ 扩展到 $\mathbb{F}_{q^m}$ ：

$$\chi(0):=\begin{cases}0, & \text{if } \chi\neq\chi_0,\\ 1, & \text{if } \chi=\chi_0.\end{cases}$$

定义 2.3. </style}加法特征 $\psi\in\mathbb{F}_{q^m}$ 的 $\mathbb{F}_q$阶 </style}是 x^m-1 的首一 $\mathbb{F}_q$-除子 g，其次数最小，且满足 $\psi\circ g$ 是 $\widehat{\mathbb{F}_{q^m}}$的平凡特征，其中 $(\psi\circ g)(\alpha):=\psi(g\circ\alpha)$，并且 $g\circ\alpha=\sum_{i=0}^n a_i\alpha^{q^i}$ 若对任意 $\alpha\in\mathbb{F}_{q^m}$， $g(x)=\sum_{i=0}^n a_ix^i$ ，记作 $\mathrm{Ord}_q(\psi)$。

众所周知，若 $z \mid q^m - 1$，则恰有 $\phi(z)$ 个阶为 z 的乘法特征，其中 ϕ 表示欧拉φ函数，而乘法特征的阶 按自然方式定义。同样，若 $g \mid x^m - 1$，则恰有 $\Phi(g)$ 个 $\mathbb{F}_q$-阶加性特征标，其中 Φ 表示环 $\mathbb{F}_q[x]$ 中的欧拉函数。

在接下来的章节中，我们将进一步探讨 $\mathbb{F}_{q^m}$ 的加法特征的性质。下面的引理将会派上用场。

引理 2.4。 设 ψ 是 $\mathbb{F}_{q^m}$ 的一个加法特征。 ψ 在 $\mathbb{F}_q$, $\psi|_{\mathbb{F}_q}$ 中的限制是 $\mathbb{F}_q$ 的一个加法特征。此外，以下各项等价:

1. $\psi|_{\mathbb{F}_q}$ 是 $\mathbb{F}_q$ 的平凡加法特征。
2. 存在某个 $c \in \mathbb{F}_{q^m}$，使得 $\mathrm{Tr}^{q^m/q}(c) = 0$。
3. $\mathrm{Ord}_q(\psi) \mid \frac{x^m-1}{x-1}$.

证明。 显然， $\psi|_{\mathbb{F}_q}$ 是 $\mathbb{F}_q$ 的一个加法特征。进一步，假设 $\psi = \psi_c$。现在我们来证明 (1) $\iff$ (2)。取某个 $a \in \mathbb{F}_q$。于是

$$\psi(a) = \psi_c(a) = \psi_1(ca) = e^{2\pi i \,\mathrm{Tr}_{q^m/p}(ca)/p} = e^{2\pi i \,\mathrm{Tr}_{q/p}(\mathrm{Tr}_{q^m/q}(ca))/p} = e^{2\pi i \,\mathrm{Tr}_{q/p}\left(\mathrm{Tr}_{q^m/q}(c)\cdot a\right)/p}.$$

换言之，将其视为 $\mathbb{F}_q$ 的一个特征时， $\psi|_{\mathbb{F}_q} = \psi_{\mathrm{Tr}_{q^m/q}(c)}$，结论得证。最后，我们来考察等价关系 (2) $\iff$ (3)。我们有

$$\begin{aligned}
\mathrm{Ord}_q(\psi_c) \mid (x^m-1)/(x-1) &\iff \text{for every } a \in \mathbb{F}_{q^m},\ \psi_c(\mathrm{Tr}_{q^m/q}(a)) = 1 \\
&\iff \text{for every } a \in \mathbb{F}_{q^m},\ \psi_1(c\,\mathrm{Tr}_{q^m/q}(a)) = 1 \\
&\iff \text{for every } b \in \mathbb{F}_q,\ \mathrm{Tr}_{q^m/p}(cb) = 0 \\
&\iff \text{for every } b \in \mathbb{F}_q,\ \mathrm{Tr}_{q/p}\left(\mathrm{Tr}_{q^m/q}(cb)\right) = 0 \\
&\iff \text{for every } b \in \mathbb{F}_q,\ \mathrm{Tr}_{q/p}\left(b\,\mathrm{Tr}_{q^m/q}(c)\right) = 0 \\
&\iff \mathrm{Tr}_{q^m/q}(c) = 0.
\end{aligned}$$

□

2.3. 自由性

有限域元素在乘法结构和代数结构上的自由性概念，在本研究中发挥着至关重要的作用。

定义2.5。 设 $e \mid q^m - 1$，则称元素 $\alpha \in \mathbb{F}_{q^m}^*$ 为 e-自由，如果对于某个$y \in \mathbb{F}_{q^m}^*$， $d \mid e$ 且 $\alpha = y^d$蕴含 $d = 1$。由定义可知，元素 $\alpha \in \mathbb{F}_{q^m}^*$ 是本原元素，当且仅当它是一个 $(q^m - 1)$-自由元素。

$\mathbb{F}_{q^m}$ 的加法群在以下规则下构成一个 $\mathbb{F}_q[x]$-模

$$f \circ \alpha := \sum_{i=0}^{n} a_i \alpha^{q^i},$$

对于 $\alpha \in \mathbb{F}_{q^m}$，其中 $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}_q[x]$。对于 $\alpha \in \mathbb{F}_{q^m}$， α 的-阶 是满足 $g \circ \alpha = 0$ 的最小次数首一 $\mathbb{F}_q$-除子 g，它是$x^m - 1$ 的除子，记为 $\mathrm{Ord}_q(\alpha)$。

定义2.6。 对于 $g \mid x^m - 1$，如果 $\alpha \in \mathbb{F}_{q^m}$ 对于某个 $\beta \in \mathbb{F}_{q^m}$ 和 $h \mid g$， $\alpha = h \circ \beta$ 蕴含 $h = 1$，则称元素 $\alpha \in \mathbb{F}_{q^m}$ 为 g-自由 。根据定义，显然，当且仅当元素 $\alpha \in \mathbb{F}_{q^m}$ 是（$x^m - 1$）-自由时，它是正规的。显然， $x^m - 1$ 可以自由地替换为其 p-根 $g_0 := x^{m_0} - 1$，其中 m_0 满足 $m = m_0 p^a$；这里 a 是非负整数，且 $\gcd(m_0, p) = 1$。

对于任意 $e \mid q^m-1$， $\mathbb{F}_{q^m}^*$ 中 e-自由元的特征函数可表示如下。

$$\rho_e : \mathbb{F}_{q^m}^* \to \{0,1\}; \alpha \mapsto \epsilon(e) \sum_{d \mid e} \left(\frac{\mu(d)}{\phi(d)} \sum_{(d)} \chi_d(\alpha) \right), \tag{2.1}$$

其中 $\epsilon(e) := \phi(e)/e$， μ 是默比乌斯函数，而 χ_d 表示 $\mathbb{F}_{q^m}^*$ 中任意一个阶为 d 的特征，内和遍历所有阶为 d 的特征。

类似地，对于任意 $g \mid x^m - 1$， $\mathbb{F}_{q^m}$ 中 g-自由元的特征函数可以表示如下:

$$\kappa_g : \mathbb{F}_{q^m} \to \{0,1\}; \alpha \mapsto \varepsilon(g) \sum_{f \mid g} \left(\frac{\mu'(f)}{\Phi(f)} \sum_{(f)} \psi_f(\alpha) \right), \tag{2.2}$$

其中 $\varepsilon(g) := \Phi(g)/q^{\deg(g)}$， ψ_f 表示 $\widehat{\mathbb{F}_{q^m}}$ 中任意一个 $\mathbb{F}_q$-阶特征 f，而 μ' 是默比乌斯函数的类似物，其定义如下:

$$\mu'(g) := \begin{cases} (-1)^s, & \text{if } g \text{ is the product of } s \text{ distinct irreducible monic polynomials,} \\ 0, & \text{otherwise,} \end{cases}$$

内和遍历所有阶为 f 的 $\mathbb{F}_q$ 阶加法特征。

$\mathbb{F}_{q^m}$ 中一类与我们有关的元素是 $(x^m-1)/(x-1)$-自由元。不难验证，这些元素不属于 $\mathbb{F}_{q^m}/\mathbb{F}_q$ 的任何中间扩张；而当 $p \mid m$ 时，它们恰好是正规于 $\mathbb{F}_q$ 的元素。此外，若 m 是一个素数，且 q 是 模本原 m，即它生成群 $\mathbb{Z}_m^*$，那么这些元素很容易刻画如下。

引理2.7. 设 m 是素数，且 q 模 m本原。那么， $\mathbb{F}_{q^m}$ 中满足$(x^m-1)/(x-1)$自由的元素，恰好是不属于 $\mathbb{F}_{q^m}/\mathbb{F}_q$任何中间扩张的元素。

证明. 设 $g(x) := (x^m-1)/(x-1)$。对 m的限制，结合 [13], 中的定理2.45和2.47可得 g 不可约，因此

$$x^m - 1 = g(x)(x-1)$$

这是 x^m-1的素分解。现在，取一个 g自由的 $a \in \mathbb{F}_{q^m}$。根据 [15] 中的定理5.4， $g \mid \mathrm{Ord}_q(a)$，也就是说，$\mathrm{Ord}_q(a) = g$ 或 $\mathrm{Ord}_q(a) = x^m-1$。所需结论得证。 □

2.4. 除子与类群

设 F/K 是一个域扩张，且对于某个 $x \in F$， x 在 K 上是超越元，并且 $F/K(x)$是有限的。在这种情况下， F/K （或简称 F）称为 K上的一元函数域。特别地，函数域 $K(x)/K$ 称为有理函数域；若 K 是有限的，即对于某个素数幂 q，有 $K = \mathbb{F}_q$，则函数域 F/K 称为全局函数域。

函数域 F/K 的一个离散赋值环 是一个环 $K \subsetneq \mathcal{O} \subsetneq F$，满足性质 $a \in \mathcal{O}$ 或 $a^{-1} \in \mathcal{O}$，对所有 $a \in F$ 均成立。可以证明，离散赋值环是一个局部环，也就是说，它有唯一的极大理想，且该理想是主理想。此外，函数域 F/K 的离散赋值环 $\mathcal{O}$ 的极大理想 $\mathfrak{p}$ 称为 F/K 的一个位；并且，若 $\mathfrak{p} = t\mathcal{O}$，则每个 $z \in F^*$ 都有唯一的表示形式 $z = t^{\nu_\mathfrak{p}(z)}u$，其中 $\nu_\mathfrak{p}(z) \in \mathbb{Z}$ 且 $u \in \mathcal{O}^*$。此外，可以看出，尽管上述的t 并不唯一，数值 $\nu_\mathfrak{p}(z)$却与其选择无关。另外，

$$\begin{aligned} \mathcal{O} &= \{z \in F : \nu_\mathfrak{p}(z) \geq 0\} \cup \{0\}, \\ \mathcal{O}^* &= \{z \in F : \nu_\mathfrak{p}(z) = 0\} \text{ and} \\ \mathfrak{p} &= \{z \in F : \nu_\mathfrak{p}(z) > 0\}. \end{aligned}$$

上述事实表明， F/K的位与离散赋值环之间存在一一对应关系，因此“赋值环 $\mathcal{O}$的位”或“位 $\mathfrak{p}$的赋值环”这样的说法是有意义的。最后，注意到，由于 $\mathfrak{p}$

是 $\mathcal{O}$的一个极大理想，环 $\mathcal{O}/\mathfrak{p}$ 是一个域，因此数值 $[\mathcal{O}/\mathfrak{p}\colon K]$ 是有定义的，称为位 $\mathfrak{p}$ 的次数，记作 $\deg(\mathfrak{p})$。已知位 $\mathfrak{p}$ 的次数是有限的。

F 的一个重要函数族是离散赋值。具体而言，F 的离散赋值 是一个函数

$$\nu : F \to \mathbb{Z} \cup \{\infty\}; a \mapsto \nu(a),$$

使得对所有 $a,\ b \in F$,

1. $\nu(a) = \infty \iff a = 0$, 2. $\nu(ab) = \nu(a) + \nu(b)$, 3. $\nu($ $a + b) \geq \min\{\nu(a)\ \nu(b)\}$,

4. 存在某个 $c \in F$，使得 $\nu(c) = 1$ 并且

5. 对所有 $d \in K^*$，$\nu(d) = 0$。

特别地，若 $\mathfrak{p}$ 是函数域 F/K 的一个位，则上述定义的函数 $\nu_{\mathfrak{p}}$ 按规则 $\nu_{\mathfrak{p}}(0) = \infty$扩展到零后，是一个称为 $\mathfrak{p}$-阶的离散赋值。

F/K 的位生成的自由阿贝尔群称为除子群，记作 $\mathrm{Div}(F)$，其元素称为除子，通常表示为形式和，不过我们将采用乘法记号。除子群的单位元是除子 $1_{\mathrm{Div}(F)} := \prod_{\mathfrak{p}} \mathfrak{p}^0$，其中乘积遍历 F/K 的各个位。此外，除子 $D = \prod_{\mathfrak{p}} \mathfrak{p}^{d_{\mathfrak{p}}}$ 的次数自然定义为 $\deg(D) := \sum_{\mathfrak{p}} d_{\mathfrak{p}} \deg(\mathfrak{p})$，其中 $d_{\mathfrak{p}} \in \mathbb{Z}$，且几乎所有的 $d_{\mathfrak{p}}$ 都为零。除子 $D = \prod_{\mathfrak{p}} \mathfrak{p}^{d_{\mathfrak{p}}}$ 的支撑是集合

$$\mathrm{supp}(D) := \{\mathfrak{p} : d_{\mathfrak{p}} \neq 0\}$$

它总是 F/K 的位集的有限子集。一类特殊的除子是主除子，即形如以下形式的除子

$$[a] = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(a)},$$

其中 $a \in F^*$，且乘积遍历 F/K 的各个位。显然，$\mathrm{Div}(F)$ 中的主除子构成 $\mathrm{Div}(F)$ 的一个子群，称为主除子群，记作 $\mathrm{Prin}(F)$，而商群

$$\mathrm{Cl}(F) := \mathrm{Div}(F)/\mathrm{Prin}(F)$$

称为 F 的 除子类群，而该群中属于同一类的两个除子称为线性等价。在 $\mathrm{Div}(F)$ 中定义了一种自然的偏序，除子 $D \geq 1_{\mathrm{Div}\, F}$（即 $D = \prod_{\mathfrak{p}} p^{d_{\mathfrak{p}}}$，其中对所有 $\mathfrak{p}$ 都有 $d_{\mathfrak{p}} \geq 0$）称为整，而整除子的半群记作 $\mathrm{Int}(F)$。

接下来，我们将注意力转向有理函数域 $K(x)/K$。根据以上讨论，该函数域的每个位都会导出一个离散赋值。然而，众所周知，在这种情况下，离散赋值只有两种类型:

1. 对每个不可约的 $\pi \in K[x]$，映射

$$\nu_\pi : K(x) \to \mathbb{Z} \cup \{\infty\}; f \mapsto \nu_\pi(f),$$

其中 $\nu_\pi(0) = \infty$，并且对于 $f \neq 0$，$\nu_\pi(f) = n$，其中 n 是满足 $f = \pi^n g/h$ 的唯一整数，其中g, $h \in K[x]$ 与 π 互素，是 $K(x)$ 的一个离散赋值。

2. 映射

$$\nu_\infty : K(x) \to \mathbb{Z} \cup \{\infty\}; f \mapsto \nu_\infty(f),$$

其中 $\nu_\infty(0) = \infty$ 且，对于 $f \neq 0$, $\nu_\infty(f) = -\deg(f)$ 是 $K(x)$ 上的离散赋值 .

$K(x)$ 的位恰好是位 $\mathfrak{p}_\pi := \langle \pi \rangle$，其中 $\pi \in K[x]$ 是一个首一不可约多项式，称为 $K(x)/K$ 的有限 位；而 $\mathfrak{p}_\infty$ 称为 $K(x)/K$ 的无限 位。此外，可以看出 $\deg(\mathfrak{p}_\pi) = \deg(\pi)$，且 $\deg(\mathfrak{p}_\infty) = 1$。最后，由上文可知，在有理函数域 $K(x)/K$ 中，某个 $f \in K[x]$（若 $f = \prod_\pi \pi^{f_\pi}$ 是其不可约分解）除了对应的主除子外，还对应除子

$$(f) = \prod_\pi \mathfrak{p}_\pi^{f_\pi} \in \mathrm{Int}(K(x)).$$

有关上述事实及其详细证明的更多内容，请感兴趣的读者参阅[16]第 1 章。

2.5. 模除子的特征

现在我们定义模一个整除子的特征。取某个 $I \in \mathrm{Int}(F)$。集合 $D_I := \{D \in \mathrm{Div}(F) : \mathrm{supp}(D) \cap \mathrm{supp}(I) = \emptyset\}$ 是 $\mathrm{Div}(F)$ 的一个子群，而集合

$$E_I := \{[a] : a \in F^* \text{ and } a \equiv 1 \pmod{I}\}$$

是 D_I的一个子群，称为 I的射线，其中同余意味着 $[a-1]/I \in \mathrm{Int}(F)$。从 $\mathrm{Int}(F)$ 到 $\mathbb{C}$的一个有限且对乘法封闭的子集的同态映射 X，若将其乘法地延拓到整个群 $\mathrm{Div}(F)$，则称为模 I的特征（或简称特征），如果

1. $G_X := \{D \in \mathrm{Div}(F) : X(D) \neq 0\} = D_I$ and
2. $E_I \subseteq G_X^1 := \{D \in \mathrm{Div}(F) : X(D) = 1\}$.

最后，如果一个特征在零次除子上不平凡，则称其为非奇异。有关这类特征的更多内容，请感兴趣的读者参阅 [9, 17] 及其中的参考文献。

3. 定理 1.6 的一个更简洁证明

受 [9], 的工作启发，我们将注意力转向整体有理函数域 $\mathbb{F}_q(x)/\mathbb{F}_q$。按照第 2.4 小节的讨论，这个函数域的位恰好是对应于 $\mathbb{F}_q$ 和 $\mathfrak{p}_\infty$ 的首一不可约多项式的位。特别地，次数为 1 的位恰好是对应于首一线性多项式和 $\mathfrak{p}_\infty$ 的位。此外，对于模 I 的非奇异特征 X， [17], 关于这一特殊函数域情形的结果给出了如下界

$$\left| \sum_{\deg \mathfrak{p}=1} X(\mathfrak{p}) \right| \leq (\deg(I) - 2)q^{1/2}. \tag{3.1}$$

现在，令 $g(x)$ 为 θ 在 $\mathbb{F}_q$ 上的极小多项式。我们如下定义模 $I = \mathfrak{p}_g \mathfrak{p}_\infty^2$ 的特征 X。取某个整 $\mathfrak{a} \in D_I$，并取首一多项式 $f_\mathfrak{a} \in \mathbb{F}_q[x]$，使得 $(f_\mathfrak{a}) = \mathfrak{a}$。显然，$g \nmid f_\mathfrak{a}$，因此 $f_\mathfrak{a}(\theta) \in \mathbb{F}_{q^m}^*$。于是 $\chi(f_\mathfrak{a}(\theta)) \neq 0$。接下来，令 $S_\mathfrak{a}$ 为 $f_\mathfrak{a}$ 的所有根之和（计重数）。显然， $S_\mathfrak{a} \in \mathbb{F}_q$，因此令

$$X(\mathfrak{a}) := \chi(f_\mathfrak{a}(\theta))\psi(-S_\mathfrak{a}).$$

由于对于 $\mathfrak{a}$， $\mathfrak{b} \in D_I$ 整除子，我们有 $f_{\mathfrak{a}\mathfrak{b}} = f_\mathfrak{a} f_\mathfrak{b}$，因此也有 $S_{\mathfrak{a}\mathfrak{b}} = S_\mathfrak{a} + S_\mathfrak{b}$，于是$X(\mathfrak{a}\mathfrak{b}) = X(\mathfrak{a})\ X(\mathfrak{b})$，所以可以将 X 的定义扩展到整个 D_I。

假设 $D \in E_I$，其中 $D = \mathfrak{a}/\mathfrak{b}$对于 $\mathfrak{a}$， $\mathfrak{b} \in E_I \cap \mathrm{Prin}(\mathbb{F}_q(x))$。由于 $D \in E_I$，我们有 D与 $1_{\mathrm{Div}(\mathbb{F}_q(x))}$线性等价，这意味着，参见 [16], 的推论 1.4.12，$\deg(D) = 0$。因此，$\deg(\mathfrak{a}) = \deg(\mathfrak{b})$，从而 $D = \mathfrak{a}/\mathfrak{b} = (f_\mathfrak{a})/(f_\mathfrak{b}) = (f_\mathfrak{a}/f_\mathfrak{b}) = [f_\mathfrak{a}/f_\mathfrak{b}]$。此外， $D \in E_I$ 意味着对于某个 $r(x)$，有 $D = [r(x)]$，且满足 $r(x) \equiv 1 \pmod{I}$。

由于 $r(x)$ 和 $f_{\mathfrak{a}}/f_{\mathfrak{b}}$ 生成相同的理想，它们相差一个 $\mathbb{F}_q$ 中的非零元素。因此，对于某个 $e \in \mathbb{F}_q^*$，$f_{\mathfrak{a}}/f_{\mathfrak{b}} \equiv e \pmod{I}$。现在，根据 I 的定义，我们得到 $\nu_\infty(f_{\mathfrak{a}}/f_{\mathfrak{b}} - e) \geq 2$ 以及 $\nu_g(f_{\mathfrak{a}}/f_{\mathfrak{b}} - e) \geq 1$。由于 $\deg(\mathfrak{a}) = \deg(\mathfrak{b})$，我们可以假设

$$f_{\mathfrak{a}} = x^k + a_1 x^{k-1} + \ldots + a_k \quad \text{and} \quad f_{\mathfrak{b}} = x^k + b_1 x^{k-1} + \ldots + b_k,$$

其中 $a_i's$ 和$b_i's$ 属于 $\mathbb{F}_q$。将 $f_{\mathfrak{a}}/f_{\mathfrak{b}}$ 形式地展开为关于 $1/x$ 的幂级数，得到

$$\frac{f_{\mathfrak{a}}}{f_{\mathfrak{b}}} - e = c_0 + c_1 \frac{1}{x} + c_2 \frac{1}{x^2} + \ldots,$$

其中 $c_0 = 1 - e$ 和 $c_1 = a_1 - b_1$。由于系数 a_1 和 b_1 分别等于 $f_{\mathfrak{a}}$和 $f_{\mathfrak{b}}$的根之和，因此由 $\nu_\infty(f_{\mathfrak{a}}/f_{\mathfrak{b}} - e) \geq 2$ 可得 $e = 1$ 和 $S_{\mathfrak{a}} = S_{\mathfrak{b}}$。此外，$\nu_g(f_{\mathfrak{a}}/f_{\mathfrak{b}} - e) \geq 1$推出 $f_{\mathfrak{a}}/f_{\mathfrak{b}} - e = g \cdot h_1/h_2$，其中 h_1，$h_2 \in \mathbb{F}_q[x]$ 和 $g \nmid h_2$。因此，给定 $e = 1$，由 $f_{\mathfrak{a}}(\theta) = f_{\mathfrak{b}}(\theta)$，可得$X(D) = 1$。于是，$X$ 是一个从 D_I 到复单位圆上的点的有限值同态，其核包含 E_I。对于所有其他除子 $\mathfrak{a}$，我们定义 $X(\mathfrak{a}) = 0$。

为明确 X 是非奇异特征，即它在零次除子子群上非平凡，我们考虑以下情形。

情形 I：χ 非平凡。在这种情形下，存在某个 $\beta \in \mathbb{F}_{q^m}^*$，使得 $\chi(\beta) \neq 1$，并且存在某个次数为 $\leq n$ 的 $f \in \mathbb{F}_q[x]$, 使得 $f(\theta) = \beta$。令 $f'(x) = x^{q^n-1} + f(x) - 1$。因此，$r'(x) := f'(x)/(x^{q^n-1} + g(x))$ 是一个零次有理函数，且满足 $r'(\theta) = \beta$。与 $r'(x)$ 对应的除子次数为零，且

$$X((r'(x))) = \chi(r'(\theta)) \cdot \psi(S_{(r'(x))}),$$

满足 $\chi(r'(\theta)) = \chi(\beta) \neq 1$。注意，由于 ψ 是 $\mathbb{F}_q$ 上的加法特征，乘积 $\chi(r'(\theta)) \cdot \psi(S_{(r'(x))})$ 不可能等于 1，因为 $\chi(r'(\theta))$ 的阶与 $\psi(S_{(r'(x))})$ 在 $\mathbb{C}^*$ 中的阶互素。这意味着 $X((r'(x))) \neq 1$，也就是说，X 是非奇异的。

情形 II：ψ是非平凡的。映射 $\mathbb{F}_q \times \mathbb{F}_q \to \mathbb{F}_q, (t, s) \mapsto t - s$是满射。这使我们可以选取$t_0, s_0 \in \mathbb{F}_q$，使得 $\psi(t_0 - s_0) \neq 1$ 非平凡。有理函数 $r'(x) = \frac{x-t_0}{x-s_0}$ 对应于一个次数为零的除子，并且 $\overline{\psi}(S_{(r'(x))}) \neq 1$。情形 I 末尾的阶数论证保证$X((r'(x))) \neq 1$，因此 X 是非奇异的。

我们已经证明 X 是非奇异的。现在，由于次数为一的位恰好是 $\mathfrak{p}_\infty$ 和 $\mathfrak{p}_{\pi_t}$，其中 $\pi_t(x) = x + t$，且已知 $X(\mathfrak{p}_\infty) = 0$ 并且 $\deg(I) = m + 2$，由 (3.1) 得，

$$\left| \sum_{t \in \mathbb{F}_q} \chi(\theta + t)\psi(t) \right| \leq mq^{1/2} \Rightarrow \left| \sum_{t \in \mathbb{F}_q} \chi(\theta + t)\psi(t) \right| \leq mq^{1/2}.$$

定理 1.6 的证明至此完成。

4. 本原正规元的弱直线性质

设 θ 是扩张 $\mathbb{F}_{q^m}/\mathbb{F}_q$ 的生成元，并设某个 $\alpha \in \mathbb{F}_q$ 满足 $\alpha\theta$ 是 g-自由，其中 $g(x) =(x^m - 1)/(x - 1)$。本节将重点讨论满足 $\alpha\theta$ 是 $(x^m - 1)/(x - 1)$-自由的直线，并证明当 q 足够大时，每条这样的直线都包含一个本原正规元。由此，我们将得到特定类型扩张的本原正规元弱直线性质。

因此，现在设 θ 是 $\mathbb{F}_{q^m}/\mathbb{F}_q$ 的生成元，且有 $\alpha \in \mathbb{F}_q$，使得 $\alpha\theta$ 是 $(x^m - 1)/(x - 1)$-自由，并令 $\mathfrak{N}_{\alpha,\theta}$ 为该直线上既本原又正规的元素个数。对我们的目的而言，只需证明 $\mathfrak{N}_{\alpha,\theta} \neq 0$。

引理 4.1。设 $\mathfrak{N}_{\alpha,\theta}$ 如上文所定义。那么

$$\mathfrak{N}_{\alpha,\theta} \geq \epsilon(q^m - 1)\varepsilon(x^m - 1) \left[\frac{q}{\varepsilon\left(\frac{x^m-1}{x-1}\right)} - W(q^m - 1)W(x^m - 1)q^{1/2} \right],$$

其中，对于 $g \in \mathbb{F}_q[x]$， $W(g)$表示 g在 $\mathbb{F}_q[x]$ 中的无平方因子首一因子的个数；对于$a \in \mathbb{Z}$， $W(a)$表示 a的正无平方因子的个数。

证明。 根据定义，我们有

$$\mathfrak{N}_{\alpha,\theta} = \sum_{x\in\mathbb{F}_q} \rho_{q^m-1}(\alpha(\theta+x))\kappa_{x^m-1}(\alpha(\theta+x)),$$

其中， ρ_{q^m-1} 和 κ_{x^m-1} 分别是本原元和正规元的特征函数。

利用 (2.1)) 和 (2.2)，我们得到，

$$\begin{aligned}\mathfrak{N}_{\alpha,\theta} &= \epsilon(q^m-1)\varepsilon(x^m-1)\sum_{x\in\mathbb{F}_q}\sum_{\substack{d|q^m-1\\ f|x^m-1}}\frac{\mu(d)\mu'(f)}{\phi(d)\Phi(f)}\sum_{(d),(f)}\chi_d(\alpha(\theta+x))\psi_f(\alpha(\theta+x))\\ &= \epsilon(q^m-1)\varepsilon(x^m-1)\sum_{\substack{d|q^m-1\\ f|x^m-1}}\frac{\mu(d)\mu'(f)}{\phi(d)\Phi(f)}\sum_{(d),(f)}\chi_d(\alpha)\psi_f(\alpha\theta)\sum_{x\in\mathbb{F}_q}\chi_d(\theta+x)\psi_f(\alpha x),\end{aligned}$$

因此，

$$\mathfrak{N}_{\alpha,\theta} = \epsilon(q^m-1)\varepsilon(x^m-1)[S_1+S_2+S_3], \tag{4.1}$$

其中， S_1 表示求和中对应于 $d=1$ 和 $f \mid (x^m-1)/(x-1)$的部分， S_2 表示对应于 $d=1$ 和 $f \nmid (x^m-1)/(x-1)$ 的部分，而 S_3 表示对应于 $d\neq 1$的部分。

关于 S_1，引理 2.4 推出，对于某个 $c \in \mathbb{F}_{q^m}$，有 $\psi_f(\alpha x) = \psi_c(\alpha x) = \psi_{c\alpha}(x)$，使得 $\mathrm{Tr}^{q^m/q}(c) = 0$。然而，$\mathrm{Tr}^{q^m/q}(c\alpha) = \alpha\,\mathrm{Tr}^{q^m/q}(c) = 0$。因此，引理 2.4 得出，对所有 $x \in \mathbb{F}_q$，均有 $\psi_f(\alpha x) = 1$。由此可得，对所有 $x \in \mathbb{F}_q$，均有 $\chi_1(\theta+x) = \psi_f(\alpha x) = 1$。因此，

$$S_1 = \sum_{f|(x^m-1)/(x-1)}\frac{\mu'(f)}{\Phi(f)}\sum_{(f)}\psi_f(\alpha\theta)\sum_{x\in\mathbb{F}_q}1 = \frac{q}{\varepsilon\left(\frac{x^m-1}{x-1}\right)}\cdot\kappa_{(x^m-1)/(x-1)}(\alpha\theta) = \frac{q}{\varepsilon\left(\frac{x^m-1}{x-1}\right)}, \tag{4.2}$$

因为 $\alpha\theta$ 是 $(x^m-1)/(x-1)$-自由的。

与上述情况类似，由引理 2.4 可知，在 S_2的情形下，我们得到 $\psi_f(\alpha x)$作为 $\mathbb{F}_q$的加法特征时是非平凡的。因此，

$$S_2 = \sum_{f\nmid(x^m-1)/(x-1)}\frac{\mu'(f)}{\Phi(f)}\sum_{(f)}\psi_f(\alpha\theta)\sum_{x\in\mathbb{F}_q}\psi_f(\alpha x)$$

而定理 1.6 表明，内层和的绝对值不超过 $mq^{1/2}$。再结合恰有 $\Phi(f)$ 个 $\mathbb{F}_q$-阶特征这一事实，可得，

$$|S_2| \le \left(W(x^m-1) - W\left(\frac{x^m-1}{x-1}\right)\right)mq^{1/2}. \tag{4.3}$$

最后，我们有

$$S_3 = \sum_{\substack{d|q^m-1,d\neq 1\\ f|x^m-1}}\frac{\mu(d)\mu'(f)}{\phi(d)\Phi(f)}\sum_{(d),(f)}\chi_d(\alpha)\psi_f(\alpha\theta)\sum_{x\in\mathbb{F}_q}\chi_d(\theta+x)\psi_f(\alpha x)$$

注意，在 S_3的情形下，乘法特征 $\chi_d(\theta+x)$ 是非平凡的，且定理 1.6 表明，内层和的绝对值不超过 $mq^{1/2}$。再结合以下事实：$\widehat{\ }$ $\widehat{\ }$在 $\mathbb{F}_{q^m}^*$ 中恰有 $\phi(d)$ 个 d 阶特征，且在 $\mathbb{F}_{q^m}$ 中恰有 $\Phi(f)$ 个 $\mathbb{F}_q$-阶特征，可得，

$$|S_3| \le (W(q^m-1)-1)W(x^m-1)mq^{1/2}. \tag{4.4}$$

结合 (4.1)、(4.2)、(4.3) 和 (4.4) 即可得到该结果。 □

由上可知，需要估计数值 $W(q^m-1)$ 和 $W(x^m-1)$。对于x^m-1，容易得到平凡上界

$$W(x^m-1) \le 2^m. \tag{4.5}$$

关于 $W(q^m-1)$，由 [18], 的定理13.12可知,

$$W(q^m-1) = o((q^m-1)^\delta)$$

对任意 $\delta > 0$，其中 o 表示小o记号。特别地，对固定整数 m,

$$W(q^m-1) = o(q^{1/4}). \tag{4.6}$$

结合 (4.5)、(4.6) 以及对每个 $g \in \mathbb{F}_q[x]$ 均有 $\varepsilon(g) < 1$ 这一事实，再应用引理 4.1，便可立即得到：当 q 足够大时，$\mathfrak{N}_{\alpha,\ \theta} \neq 0$。换言之，我们有如下结论。

定理4.2。固定整数 m。存在某个数 $\mathfrak{L}_m$，使得对每个素数幂 $q \ge \mathfrak{L}_m$，扩张 $\mathbb{F}_{q^m}/\mathbb{F}_q$ 中每条满足 $\alpha\theta$ 为 $(x^m-1)/(x-1)$-*free* 的直线都包含一个本原正规元。

5. 定理1.7的证明

本节简要说明定理4.2如何推出定理1.7。

设 $\mathbb{F}_{q^m}/\mathbb{F}_q$ 是一个扩张，使得 q 模 m 和 $q \ge \mathfrak{L}_m$ 本原。设 θ 是该扩张的一个生成元，并取某个 $a \in \mathbb{F}_q^*$。引理2.7表明，$\alpha\theta$ 是 $(x^m-1)/(x-1)$-自由的。由定理4.2可知，前述直线包含一个本原正规元。这就证明了定理1.7中关于弱直线性质的断言。关于平移性质的断言则显而易见。

6. 后续研究

本文最后简要讨论这一研究领域未来可能的发展方向。

一个值得探讨的方向是尝试利用函数域论证证明定理1.5（部分证明或在其完整的一般性下证明）。

另一个可能的方向是研究 $\alpha\theta$ 不是按第4节中的定义所说的 $(x^m-1)/(x-1)$-自由的情形，和/或尝试将定理1.7推广到（非弱）直线性质。仔细阅读引理 4.1 的证明，应能看出本文所作限制背后的技术原因。

另一个不同的研究方向是将本文的结果推广到存在 r-本原元和/或 k-正规元的情形，其中，如果某个 $\mathbb{F}_{q^m}$ 的 k-正规元的 $\mathbb{F}_q$-共轭元能生成一个维数为 $m-k$的 $\mathbb{F}_q$-向量空间，则称其为 $\mathbb{F}_q$ 上的 k-正规元。近期，r-本原元和 k-正规元的有效刻画分别在 [19] 和 [20],中建立，这些结果有望应用于这一情形。

从一个略有不同的角度来看，本文研究了集合 $\mathcal{A}_f := \{f(x) : x \in \mathbb{F}_q\}$中 $\mathbb{F}_{q^m}/\mathbb{F}_q$ 的本原正规元的存在性，其中 $f \in \mathbb{F}_q[x]$ 是线性的。在 [9], 中，作者研究素数次扩张 $\mathbb{F}_{p^m}/\mathbb{F}_p$，并考察 $\mathcal{A}_f$ 中本原元的存在性，其中要求 $f \in \mathbb{F}_p[x]$ 不可约。基于这一思路，我们认为，证明扩张 $\mathbb{F}_{q^m}/\mathbb{F}_q$ 在 $\mathcal{A}_f$中存在本原正规元（其中 $f \in \mathbb{F}_q[x]$不可约）是可行的，但并非易事。

最后，这一研究方向上一个引人关注的问题是，计算定理1.7中已证明渐近存在的那些数的确切值。沿着这一思路，1983年，Cohen [21] 证明了$TP(2) = LP(2) = 1$。2009年，[22], 同一位作者证明了 $TP(3) = 37$。2019年，Bailey等人 [23] 证明了 $LP(3) = 37$，并且 $73 \le TP(4) \le LP(4) \le 10282$。此外，2020年，Cohen和Kapetanakis [24] 证明了 $TP_2(2) = LP_2(2) = 41$。在定理1.7的背景下，鉴于在二次扩张 $\mathbb{F}_{q^2}/\mathbb{F}_q$ 中，所有本原元也都是正规于 $\mathbb{F}_q$的，事实 $LP(2) = 1$意味着 $LPN(2) = 1$。然而，计算某些数值 $TPN(m)$ 或 $WLPN(m)$（其中 $m \ge 3$如定理1.7所述）并非易事，这将把理论和计算方法推向极限。

7. 致谢

作者感谢Igor Shparlinski与我们进行了有益的交流，并提出了宝贵意见，尤其感谢他指出了 [9]。我们也感谢审稿人提出的深思熟虑的意见，并为改进稿件所付出的努力。

参考文献

[1] I. F. Rúa，《四维有限半体的本原性》，《有限域及其应用》33 (2015) 212–229。[2] I. F. Rúa，《阶为 2^{4e} 的本原半体》，《设计、编码与密码学》83 (2) (2017) 345–356。[3] H. Davenport，《有限域中的本原根》，《数学季刊》8 (1) (1937) 308–312。[4] L. Carlitz，《有限域中本原根的分布》，《数学季刊》4 (1) (1953) 4–10。[5] N. M. Katz，《特征和的一个估计》，美国数学会杂志 2 (2) (1989) 197–200。[6] F. R. K. Chung，《直径与特征值》，美国数学会杂志 2 (2) (1989) 187–196。[7] S. D. Cohen，《有限域扩张中直线上的本原元》，载于：D. P. Gary McGuire、Gary L. Mullen、I. E. Shparlinski（编），《有限域：理论与应用》，当代数学第 518 卷，美国数学会，罗得岛州普罗维登斯，2010 年，第 113–127 页。[8] S. D. Cohen、G. Kapetanakis，《具有直线或平移性质的有限域扩张中的 r-本原元》，《澳大利亚数学会杂志》111 (3) (2021) 313–319。[9] G. I. Perel’muter、I. E. Shparlinskii，《有限域中本原根的分布》，《俄罗斯数学评论》45 (1) (1990) 223–224。[10] L. Fu、D. Wan，《一类不完全特征和》，《数学季刊》65 (4) (2014) 1195–1211。[11] T. Garefalakis、G. Kapetanakis，《完全正规元的平移与 Morgan-Mullen 猜想》，已投稿发表，arXiv:2509 [math.NT], 2025。[12] I. H. Morgan、G. L. Mullen，《有限域的完全正规本原基生成元》，Utilitas Mathematica 49 (1996) 21–43。[13] R. Lidl、H. Niederreiter，《有限域》，第 2 版，数学及其应用百科全书第 20 卷，剑桥大学出版社，剑桥，1997。[14] G. L. Mullen、D. Panario，《有限域手册》，CRC出版社，博卡拉顿，2013。[15] S. Huczynska、G. L. Mullen、D. Panario、D. Thomson，《有限域上 k-正规元的存在性与性质》，《有限域及其应用》24 (2013) 170–183。[16] H. Stichtenoth，《代数函数域与编码》，第 2 版，数学研究生教材第 254 卷，施普林格，柏林海德堡，2009。[17] G. I. Perel’muter，《沿代数曲线的和的估计》，苏联科学院。《数学札记》5 (1969) 373–380。

[18] T. Apostol, 《解析数论导论》, Springer-Verlag, 纽约、海德堡、柏林, 1976。[19] S. D. Cohen、G. Kapetanakis、L. Reis, 《利用自由性证明曲线上 $\mathbb{F}_q$-本原点的存在性》, 《数学报告》360 (G6) (2022) 641–652。[20] G. Kapetanakis、L. Reis, 《有限域上阿廷-施赖尔曲线的正规点》, 《数学报告》365 (G6) (2025) 541–554。[21] S. D. Cohen, 《有限域二次扩张中的本原根》, 《伦敦数学学会杂志》27 (2) (1983) 221–228。[22] S. D. Cohen, 《有限域三次扩张的生成元》, 《组合学与数论杂志》1 (3) (2009) 189–202。[23] G. Bailey、S. D. Cohen、N. Sutherland、T. Trudgian, 《有限域三次和四次扩张中本原元存在性的结果》, 《计算数学》88 (316) (2019) 931–947。[24] S. D. Cohen、G. Kapetanakis, 《二次扩张中 2-本原元的平移性质与直线性质》, 《国际数论杂志》16 (9) (2020) 2029–2040。