Vol. 39 (2019)
No. 5

数 学 杂 志
J. of Math. (PRC)

A 2-DIMENSIONAL ANALOGUE OF SÁRKÖZY'S THEOREM IN FUNCTION FIELDS

LI Guo-quan, LIU Bao-qing, QIAN Kun, XU Gui-qiao
(*School of Mathematics Science, Tianjin Normal University, Tianjin 300387, China*)

Abstract: Let $\mathbb{F}_q[t]$ be the polynomial ring over the finite field $\mathbb{F}_q$ of q elements. For $N \in \mathbb{N}$, let $\mathbb{G}_N$ be the set of all polynomials in $\mathbb{F}_q[t]$ of degree less than N. Suppose that the characteristic of $\mathbb{F}_q$ is greater than 2 and $A \subseteq \mathbb{G}_N^2$. If $(d, d^2) \notin A - A = \{a - a' : a, a' \in A\}$ for any $d \in \mathbb{F}_q[t] \setminus \{0\}$, we prove that $|A| \le Cq^{2N} \frac{\log N}{N}$, where the constant C depends only on q. By using this estimate, we extend Sárközy's theorem in function fields to the case of a finite family of polynomials of degree less than 3.

Keywords: Sárközy's theorem; function fields; Hardy-Littlewood circle method
2010 MR Subject Classification: 11P55; 11T55
Document code: A **Article ID:** 0255-7797(2019)05-0656-21

1 Introduction

Let $\mathbb{N} = \{0, 1, 2, \cdots\}$ and write $\mathbb{N}_+$ for $\mathbb{N} \setminus \{0\}$. For a subset A of an additive group, we define the difference set $A - A = \{a - a' : a, a' \in A\}$. If A also is finite, we denote by $|A|$ its cardinality.

In the late 1970s, Furstenberg [1] and Sárközy [2] independently proved the following conclusion. If A is a subset of positive upper density of $\mathbb{Z}$, then there exist two distinct elements of A whose difference is a perfect square. The latter also provided an explicit estimate, but the former result is not quantitative. Sárközy's theorem was later improved by Pintz, Steiger and Szemerédi in [3], where they obtained the following theorem.

Theorem A There exists a constant $D > 0$ such that the following holds. Let $N \in \mathbb{N}_+$ and $A \subseteq \mathbb{N} \cap [1, N]$. If $(A - A) \cap \{n^2 : n \in \mathbb{N}_+\} = \emptyset$, then we have

$$|A| \le DN(\log N)^{-\frac{1}{12} \log\log\log\log N}.$$

Remark 1 Balog, Pelikán, Pintz and Szemerédi [4] showed that one may replace $\frac{1}{12}$ by $\frac{1}{4}$ in the above bound. This estimate is the current best known bound.

In 1996, by extending the ideas of Furstenberg, Bergelson and Leibman [5] established a far reaching qualitative result, the so-called Polynomial Szemerédi theorem. It is natural to ask for a quantitative version of the Polynomial Szemerédi theorem. Recently, Lyall and

* **Received date:** 2018-05-08 **Accepted date:** 2018-12-24
Foundation item: Supported by National Natural Science Foundation of China(11671271).
Biography: Li Guoquan (1969–), male, born at Yanzhou, Shandong, professor, major in analytic number theory and harmonic analysis.

Magyar [6] made some progress towards this problem. They first proved a higher dimensional analogue of Sárközy's theorem.

Theorem B For $k \in \mathbb{N}$ with $k \geq 2$, there exists a constant $D' > 0$ such that the following holds. Let $N \in \mathbb{N}_+$ and $A \subseteq \mathbb{N}^k \cap [1, N]^k$. If $(A - A) \cap \big\{(n, n^2, \cdots, n^k) : n \in \mathbb{Z} \setminus \{0\}\big\} = \emptyset$, then we have

$$|A| \leq D' N^k \Big(\frac{\log\log N}{\log N}\Big)^{\frac{1}{k-1}}.$$

Then by applying Theorem B, they established a quantitative result on the existence of polynomial configurations of the type in the Polynomial Szemerédi theorem in the difference set of sparse subsets of $\mathbb{Z}$.

Theorem C Let $l \in \mathbb{N}_+$ and $P_1, \cdots, P_l \in \mathbb{Z}[x]$ with $P_i(0) = 0$ for $i = 1, \cdots, l$. Suppose that $k = \max\limits_{1 \leq i \leq l} \deg P_i \geq 2$. Then there exists a constant $D'' > 0$ such that the following inequality holds: let $N \in \mathbb{N}_+$ and $A \subseteq \mathbb{N} \cap [1, N]$. If $\big\{P_1(n), \cdots, P_l(n)\big\} \nsubseteq A - A$ for any $n \in \mathbb{Z} \setminus \{0\}$, then we have

$$|A| \leq D'' N \Big(\frac{\log\log N}{\log N}\Big)^{\frac{1}{(k-1)l}}.$$

Remark 2 Theorems B and C were quoted from the revised version of [6], where the authors improved the main results in the original edition.

By taking $l = 1$, $P_1 = x^2$ and $k = 2$, Sárközy's theorem follows from Theorem C. Thus, we may consider Theorem C to be Sárközy's theorem for a family of polynomials.

Let $\mathbb{F}_q$ be the finite field of q elements. Let p denote the characteristic of $\mathbb{F}_q$. We denote by $\mathbb{A} = \mathbb{F}_q[t]$ the polynomial ring over $\mathbb{F}_q$ and write $\mathbb{A}^\times = \mathbb{F}_q[t] \setminus \{0\}$. For $N \in \mathbb{N}$, let $\mathbb{G}_N$ be the set of all polynomials in $\mathbb{A}$ of degree less than N.

By adapting part of the Pintz-Steiger-Szemerédi argument, Lê and Liu [7] obtained an analogue of Theorem A in function fields.

Theorem D If $p \geq 3$, then there exists a constant $D''' > 0$, depending only on q, such that the following holds: let $N \in \mathbb{N}$ with $N \geq 2$ and $A \subseteq \mathbb{G}_N$. If $(A - A) \cap \{d^2 : d \in \mathbb{A}^\times\} = \emptyset$, then we have

$$|A| \leq D''' q^N \frac{(\log N)^7}{N}.$$

In this paper, for the case $k = 2$, we consider the analogues of Theorems B and C in function fields. First, by closely following the approach of Lyall and Magyar, which is explained in detail by Rice [8], we prove a 2-dimensional version of Sárközy's theorem in function fields.

Theorem 1 If $p \geq 3$, then there exists a constant $C > 0$, depending only on q, such that the following holds: let $N \in \mathbb{N}$ with $N \geq 2$ and $A \subseteq \mathbb{G}_N^2$. If $(A - A) \cap \{(d, d^2) : d \in \mathbb{A}^\times\} = \emptyset$, then we have

$$|A| \leq C q^{2N} \frac{\log N}{N}.$$

By adapting the lifting argument in [6], we deduce the following analogue of Theorem C from Theorem 1.

Theorem 2 Let $l \in \mathbb{N}_+$ and $P_1, \cdots, P_l \in \mathbb{A}[x]$ with $P_i(0) = 0$ for $i = 1, \cdots, l$. Suppose that $\max\limits_{1\leq i\leq l} \deg P_i \leq 2$ and $p \geq 3$. Then there exists a constant $C' > 0$, depending only on $q, P_1, \cdots, P_l$, such that the following inequality holds: let $N \in \mathbb{N}$ with $N \geq 2$ and $A \subseteq \mathbb{G}_N$. If $\{P_1(d), \cdots, P_l(d)\} \nsubseteq A - A$ for any $d \in \mathbb{A}^\times$, then we have $|A| \leq C' q^N \left(\frac{\log N}{N}\right)^{\frac{1}{l}}$.

In particular, by taking $l = 1$ and $P_1 = x^2$ in Theorem 2, we obtain a slight improvement of Theorem D.

In the general cases $k \geq 3$, it is more difficult to establish a k-dimensional analogue of Theorem B in function fields. The main obstruction is that we are not able to obtain satisfactory exponential sum estimates on the minor arcs (for details of the circle method, see [9]), i.e., suitable generalizations of Proposition 10. We intend to return to this topic in the future.

2 Preliminaries

Let $\mathbb{K} = \mathbb{F}_q(t)$ be the field of fractions of $\mathbb{A}$. For $a, b \in \mathbb{A}$ with $b \neq 0$, we define $|\frac{a}{b}| = q^{\deg a - \deg b}$. Then $|\cdot|$ is a valuation on $\mathbb{K}$. The completion of $\mathbb{K}$ with respect to this valuation is $\mathbb{K}_\infty = \{\sum\limits_{i\leq r} c_i t^i : r \in \mathbb{Z} \text{ and } c_i \in \mathbb{F}_q\ (i \leq r)\}$, the field of formal Laurent series in $\frac{1}{t}$.

For $\omega = \sum\limits_{i\leq r} c_i t^i \in \mathbb{K}_\infty$, if $c_r \neq 0$, we define $\mathrm{ord}\omega = r$. Also, we adopt the convention that $\mathrm{ord} 0 = -\infty$. Thus, we have $|\omega| = q^{\mathrm{ord}\omega}$. We define $\{\omega\} = \sum\limits_{i\leq -1} c_i t^i$ to be the fractional part of ω and we write $[\omega]$ for $\sum\limits_{i\geq 0} c_i t^i$. Then it follows that $\omega = [\omega] + \{\omega\}$. We also write $\mathrm{res}\omega$ for c_{-1} which is said to be the residue of ω.

$\mathbb{K}_\infty$ is a locally compact field and $\mathbb{T} = \{\omega \in \mathbb{K}_\infty : \mathrm{ord}\omega \leq -1\}$ is a compact subring of $\mathbb{K}_\infty$. Let $d\omega$ be the Haar measure on $\mathbb{K}_\infty$ such that $\int_{\mathbb{T}} 1 d\omega = 1$.

Let $\mathrm{tr} : \mathbb{F}_q \to \mathbb{F}_p$ be the familiar trace map. For $c \in \mathbb{F}_q$, write $e_q(c) = \exp(\frac{2\pi\sqrt{-1}}{p}\mathrm{tr}(c))$. The exponential function $e : \mathbb{K}_\infty \to \mathbb{C}^\times$ is defined by $e(\omega) = e_q(\mathrm{res}\,\omega)$. Using this function, one can establish Fourier analysis in $\mathbb{A}$. In particular, $\mathbb{A}, \mathbb{K}, \mathbb{K}_\infty, \mathbb{T}$ play the roles of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{R}/\mathbb{Z}$, respectively.

For $\omega \in \mathbb{K}_\infty$ and $\gamma = (\gamma_1, \gamma_2), \gamma' = (\gamma_1', \gamma_2') \in \mathbb{K}_\infty^2$, write $\omega\gamma = (\omega\gamma_1, \omega\gamma_2)$ and $\gamma\gamma' = \gamma_1\gamma_1' + \gamma_2\gamma_2'$.

Let $f, g : \mathbb{A}^2 \to \mathbb{C}$ be functions with finite support sets. The Fourier transform $\hat{f} : \mathbb{T}^2 \to \mathbb{C}$ of f is defined by $\hat{f}(\alpha) = \sum\limits_{m\in\mathbb{A}^2} f(m)e(m\alpha)$. The convolution $f * g : \mathbb{A}^2 \to \mathbb{C}$ of f and g is defined by

$$f * g(n) = \sum_{m\in\mathbb{A}^2} f(m)g(n - m).$$

Then it follows that

$$\mathrm{supp} f * g \subseteq \mathrm{supp} f + \mathrm{supp} g \text{ and } \widehat{f * g}(\alpha) = \hat{f}(\alpha)\hat{g}(\alpha).$$

Let $d\alpha$ denote the product of Haar measures. For $m \in \mathbb{A}^2$, we have the orthogonal relation

$$\int_{\mathbb{T}^2} e(\alpha m) d\alpha = \begin{cases} 1, & \text{if } m = 0, \\ 0, & \text{otherwise.} \end{cases} \tag{2.1}$$

Lemma 1 For $M \in \mathbb{N}_+$ and $\omega \in \mathbb{K}_\infty$, we have

$$\sum_{d \in \mathbb{G}_M} e(\omega d) = \begin{cases} q^M, & \text{if } \mathrm{ord}\{\omega\} < -M, \\ 0, & \text{otherwise.} \end{cases}$$

Proof This is [10, Lemma 7].

Let $a, b \in \mathbb{A}$ with $b \neq 0$ and $\gcd(b, a) = 1$. For $m = (m_1, m_2) \in \mathbb{A}^2$, if $\gcd(b, m_1, m_2) = 1$, we define

$$G(\frac{a}{b}, m) = \sum_{d \in \mathbb{G}_{\mathrm{ord}b}} e(\frac{a}{b} m \overrightarrow{d}),$$

where $\overrightarrow{d} = (d, d^2)$.

For $N \in \mathbb{N}_+$, the exponential sum $S_N : \mathbb{T}^2 \to \mathbb{C}$ is defined by $S_N(\alpha) = \sum\limits_{d \in \mathbb{G}_N} e(\alpha \overrightarrow{d})$.

Lemma 2 Let $N \in \mathbb{N}_+$ and $\alpha = (\alpha_1, \alpha_2) \in \mathbb{T}^2$. Let $b \in \mathbb{A}^\times$ and $m = (m_1, m_2) \in \mathbb{A}^2$ with $\gcd(b, m_1, m_2) = 1$. Suppose that $\mathrm{ord}b \leq N$, $\left|\alpha_1 - \frac{m_1}{b}\right| < |b|^{-1}$ and $\left|\alpha_2 - \frac{m_2}{b}\right| < q^{1-N}|b|^{-1}$. Then we have

$$S_N(\alpha) = \frac{1}{|b|} G(\frac{1}{b}, m) S_N(\alpha - \frac{1}{b} m).$$

Proof Write $\beta = (\beta_1, \beta_2) = \alpha - \frac{1}{b} m$. Then

$$S_N(\alpha) = \sum_{t \in \mathbb{G}_{\mathrm{ord}b}} e(\frac{1}{b} m \overrightarrow{t}) \sum_{s \in \mathbb{G}_{N-\mathrm{ord}b}} e(\beta \overrightarrow{sb + t}).$$

Let $s \in \mathbb{G}_{N-\mathrm{ord}b}$ and $t \in \mathbb{G}_{\mathrm{ord}b}$. Note that

$$\mathrm{ord}(\beta_1(sb + t) - \beta_1 sb) = \mathrm{ord}\beta_1 + \mathrm{ord}t \leq (-\mathrm{ord}b - 1) + (\mathrm{ord}b - 1) = -2,$$

we have $e(\beta_1(sb + t)) = e(\beta_1 sb)$. Similarly, since

$$\begin{aligned} \mathrm{ord}(\beta_2(sb + t)^2 - \beta_2 s^2 b^2) &\leq \mathrm{ord}\beta_2 + \mathrm{ord}t + \max\{\mathrm{ord}t, \mathrm{ord}sb\} \\ &\leq (-N - \mathrm{ord}b) + (\mathrm{ord}b - 1) + (N - 1) \\ &= -2, \end{aligned}$$

it follows that $e(\beta_2(sb + t)^2) = e(\beta_2 s^2 b^2)$. Thus, we obtain

$$\begin{aligned} S_N(\alpha) &= \sum_{t \in \mathbb{G}_{\mathrm{ord}b}} e(\frac{1}{b} m \overrightarrow{t}) \sum_{s \in \mathbb{G}_{N-\mathrm{ord}b}} e(\beta \overrightarrow{sb}) \\ &= G(\frac{1}{b}, m) \sum_{s \in \mathbb{G}_{N-\mathrm{ord}b}} e(\beta \overrightarrow{sb}) \\ &= \frac{1}{|b|} G(\frac{1}{b}, m) \sum_{t \in \mathbb{G}_{\mathrm{ord}b}} \sum_{s \in \mathbb{G}_{N-\mathrm{ord}b}} e(\beta \overrightarrow{sb + t}) \\ &= \frac{1}{|b|} G(\frac{1}{b}, m) S_N(\beta). \end{aligned}$$

This completes the proof of the lemma.

Lemma 3 Let $r_1, r_2 \in \mathbb{N}$. Then for any $\alpha = (\alpha_1, \alpha_2) \in \mathbb{T}^2$, there exists $(b, m_1, m_2) \in \mathbb{A}^3$ with the following properties

(i) b is monic and $\mathrm{ord} b \le r_1 + r_2$;

(ii) $\gcd(b, m_1, m_2) = 1$;

(iii) $\mathrm{ord} m_j < \mathrm{ord} b$ and $\left|\alpha_j - \frac{m_j}{b}\right| < q^{-r_j}|b|^{-1}$ $(1 \le j \le 2)$.

Proof For $1 \le j \le 2$, let $\mathbb{T}_j = \left\{\omega \in \mathbb{T} : \mathrm{ord}\omega \le -r_j - 1\right\}$. Then $\mathbb{T}_j$ is a subgroup of $\mathbb{T}$. Also, $\left|\mathbb{T}/\mathbb{T}_j\right| = q^{r_j}$.

Note that $\left|\prod\limits_{j=1}^{2} \mathbb{T}/\mathbb{T}_j\right| = q^{r_1+r_2} < |\mathbb{G}_{r_1+r_2+1}|$, we can find two distinct elements d_1, d_2 of $\mathbb{G}_{r_1+r_2+1}$ such that

$$\big(\{d_1\alpha_1\} + \mathbb{T}_1, \{d_1\alpha_2\} + \mathbb{T}_2\big) = \big(\{d_2\alpha_1\} + \mathbb{T}_1, \{d_2\alpha_2\} + \mathbb{T}_2\big).$$

Write $b' = d_2 - d_1$. Then we have $b' \ne 0$ and $\mathrm{ord} b' \le r_1 + r_2$.

Let $m'_j = [b'\alpha_j]$. Then $\mathrm{ord} m'_j \le \mathrm{ord}(b'\alpha_j) = \mathrm{ord} b' + \mathrm{ord}\alpha_j < \mathrm{ord} b'$.

Since $\mathrm{ord}(b'\alpha_j - m'_j) = \mathrm{ord}\{b'\alpha_j\} = \mathrm{ord}(\{d_2\alpha_j\} - \{d_1\alpha_j\}) \le -r_j - 1$, we have

$$\left|\alpha_j - \frac{m'_j}{b'}\right| < q^{-r_j}|b'|^{-1}.$$

Let c be the leading coefficient of b' and let $a = \gcd(b', m'_1, m'_2)$. By taking $b = \frac{b'}{ac}$ and $m_j = \frac{m'_j}{ac}$, the lemma follows.

3 Estimate for $G(\frac{a}{b}, m)$

In this section, we obtain an estimate for $G(\frac{a}{b}, m)$. Our arguments run in parallel with the approach of Chen [11].

Lemma 4 Let $a_1, a_2, b_1, b_2 \in \mathbb{A}$ with $b_1, b_2 \ne 0$ and $\gcd(b_1, a_1) = \gcd(b_2, a_2) = 1$. Let $m = (m_1, m_2) \in \mathbb{A}^2$. Suppose that $\gcd(b_1, m_1, m_2) = \gcd(b_2, m_1, m_2) = 1$. If $\gcd(b_1, b_2) = 1$, then

$$G(\frac{a_1}{b_1}, m)G(\frac{a_2}{b_2}, m) = G(\frac{a_1b_2 + a_2b_1}{b_1b_2}, m).$$

Proof Since $\gcd(b_1, b_2) = 1$, $b_2 + b_1\mathbb{A}$ is invertible in the ring $\mathbb{H}_1 = \mathbb{A}/b_1\mathbb{A}$. Thus,

$$G(\frac{a_1}{b_1}, m) = \sum_{d+b_1\mathbb{A}\in\mathbb{H}_1} e(\frac{a_1}{b_1}m\,\overrightarrow{d}\,) = \sum_{d+b_1\mathbb{A}\in\mathbb{H}_1} e(\frac{a_1}{b_1}m\overrightarrow{b_2d}) = \sum_{d\in\mathbb{G}_{\mathrm{ord}b_1}} e(\frac{a_1}{b_1}m\overrightarrow{b_2d}).$$

Similarly, we have

$$G(\frac{a_2}{b_2}, m) = \sum_{d\in\mathbb{G}_{\mathrm{ord}b_2}} e(\frac{a_2}{b_2}m\overrightarrow{b_1d}).$$

Combining the above two equalities, it follows that

$$\begin{aligned} G(\frac{a_1}{b_1}, m)G(\frac{a_2}{b_2}, m) &= \sum_{d_1\in\mathbb{G}_{\mathrm{ord}b_1}, d_2\in\mathbb{G}_{\mathrm{ord}b_2}} e(\frac{a_1}{b_1}m\overrightarrow{b_2d_1})e(\frac{a_2}{b_2}m\overrightarrow{b_1d_2}) \\ &= \sum_{d_1\in\mathbb{G}_{\mathrm{ord}b_1}, d_2\in\mathbb{G}_{\mathrm{ord}b_2}} e(\frac{a_1b_2+a_2b_1}{b_1b_2}m\overrightarrow{b_1d_2+b_2d_1}) \\ &= \sum_{d\in\mathbb{G}_{\mathrm{ord}b_1b_2}} e(\frac{a_1b_2+a_2b_1}{b_1b_2}m\overrightarrow{d}). \end{aligned} \tag{3.1}$$

Equality (3.1) follows since $\gcd(b_1, b_2) = 1$.

Lemma 5 Let $a, b \in \mathbb{A}$ with $b \neq 0$ and $\gcd(b, a) = 1$. Let $m = (m_1, m_2) \in \mathbb{A}^2$. Suppose that $\gcd(b, m_1, m_2) = 1$. If $p \geq 3$ and b is irreducible, then we have

$$\left|G(\frac{a}{b}, m)\right| \leq |b|^{\frac{1}{2}}.$$

Proof Since b is irreducible and $\gcd(b, a) = 1$, it follows that $a \neq 0$. We divide into two cases.

Case 1 Suppose that $b \mid m_2$. Since $\gcd(b, m_1, m_2) = 1$, $b \nmid m_1$. By Lemma 1, we have

$$G(\frac{a}{b}, m) = \sum_{d\in\mathbb{G}_{\mathrm{ord}b}} e(\frac{am_1}{b}d) = 0.$$

Case 2 Suppose that $b \nmid m_2$. Since b is irreducible, $\mathbb{H} = \mathbb{A}/b\mathbb{A}$ is a field. Note that $|\mathbb{H}| = |b|$, we can find an isomorphism $T : \mathbb{F}_{|b|} \to \mathbb{H}$ of fields.

Consider $\psi : \mathbb{F}_{|b|} \to \mathbb{C}^\times$ defined by $\psi(c) = e(\frac{a}{b}T(c))$. It follows from Lemma 1 that

$$\sum_{c\in\mathbb{F}_{|b|}} \psi(c) = \sum_{d\in\mathbb{G}_{\mathrm{ord}b}} e(\frac{ad}{b}) = 0.$$

Thus, ψ is a non-trivial additive character of $\mathbb{F}_{|b|}$. Let $P(t) = \sum_{j=1}^{2} T^{-1}(m_j + b\mathbb{A})t^j$. Then P is a polynomial of degree 2 in $\mathbb{F}_{|b|}[t]$.

Note that

$$G(\frac{a}{b}, m) = \sum_{d\in\mathbb{G}_{\mathrm{ord}b}} \psi(P(T^{-1}(d + b\mathbb{A}))) = \sum_{c\in\mathbb{F}_{|b|}} \psi(P(c)),$$

by Weil's theorem in [12], we have $\left|G(\frac{a}{b}, m)\right| \leq |b|^{\frac{1}{2}}$.

Combining the above two cases, the lemma follows.

Lemma 6 Let $a, b \in \mathbb{A}$ with $b \neq 0$ and $\gcd(b, a) = 1$. Let $m = (m_1, m_2) \in \mathbb{A}^2$. Suppose that $\gcd(b, m_1, m_2) = 1$. If $p \geq 3$ and b is irreducible, then for any $r \in \mathbb{N}_+$, we have

$$\left|G(\frac{a}{b^r}, m)\right| \leq |b|^{\frac{r}{2}}.$$

Proof We will prove this lemma by induction on r.

For $r=1$, the lemma follows from Lemma 5.

Let $r\in\mathbb{N}$ with $r\geq 2$. Suppose that the lemma holds for all $r'\in\mathbb{N}_+$ with $r'<r$. We now prove that the statement is true for r.

Note that for $d\in\mathbb{G}_{\mathrm{ord}b^r}$, there exist $d_1\in\mathbb{G}_{\mathrm{ord}b^{r-1}}$ and $d_2\in\mathbb{G}_{\mathrm{ord}b}$ such that $d=d_2b^{r-1}+d_1$. This observation allows us to obtain

$$G(\frac{a}{b^r},m)=\sum_{d_1\in\mathbb{G}_{\mathrm{ord}b^{r-1}}}e(\frac{a}{b^r}m\overrightarrow{d_1})\sum_{d_2\in\mathbb{G}_{\mathrm{ord}b}}e\big(\frac{a}{b}(m_1+2m_2d_1)d_2\big). \tag{3.2}$$

There are two cases.

Case 1 Suppose that $b\mid m_2$. Since $b\nmid m_1$, by Lemma 1, we have

$$\sum_{d_2\in\mathbb{G}_{\mathrm{ord}b}}e\big(\frac{a}{b}(m_1+2m_2d_1)d_2\big)=\sum_{d_2\in\mathbb{G}_{\mathrm{ord}b}}e(\frac{am_1}{b}d_2)=0.$$

By (3.2), we have

$$G(\frac{a}{b^r},m)=0.$$

Case 2 Suppose that $b\nmid m_2$. Then there exists unique $d_0\in\mathbb{G}_{\mathrm{ord}b}$ such that

$$m_1+2m_2d_0\equiv 0\ (\mathrm{mod}\ b).$$

For any $d_1\in\mathbb{G}_{\mathrm{ord}b^{r-1}}$, it follows from Lemma 1 that

$$\sum_{d_2\in\mathbb{G}_{\mathrm{ord}b}}e\big(\frac{a}{b}(m_1+2m_2d_1)d_2\big)=\begin{cases}|b|, & \text{if } d_1\equiv d_0\ (\mathrm{mod}\ b),\\ 0, & \text{otherwise.}\end{cases}$$

Write

$$\Lambda=\big\{d\in\mathbb{G}_{\mathrm{ord}b^{r-1}}:d\equiv d_0\ (\mathrm{mod}\ b)\big\}.$$

By (3.2), we have

$$G(\frac{a}{b^r},m)=\sum_{d_1\in\Lambda}|b|e(\frac{a}{b^r}m\overrightarrow{d_1}).$$

If $r=2$, then

$$|G(\frac{a}{b^r},m)|=\big||b|e(\frac{a}{b^2}m\overrightarrow{d_0})\big|=|b|^{\frac{r}{2}}.$$

If $r\geq 3$, then

$$G(\frac{a}{b^r},m)=\sum_{d\in\mathbb{G}_{\mathrm{ord}b^{r-2}}}|b|e\big(\frac{a}{b^r}m\overrightarrow{db+d_0}\big). \tag{3.3}$$

Let $m_1'=\frac{m_1+2m_2d_0}{b}$, then $m_1'\in\mathbb{A}$. Write $m'=(m_1',m_2)$. Note that

$$m\overrightarrow{db+d_0}-m\overrightarrow{d_0}=b^2m'\overrightarrow{d},$$

we deduce from (3.3) that

$$G(\frac{a}{b^r},m)=|b|e\big(\frac{a}{b^r}m\overrightarrow{d_0}\big)G(\frac{a}{b^{r-2}},m').$$

By the induction hypothesis, it follows that

$$\big|G(\frac{a}{b^r},m)\big| = |b|\big|G(\frac{a}{b^{r-2}},m')\big| \le |b|^{\frac{r}{2}}.$$

By combining the above two cases, we complete the proof of the lemma.

Proposition 7 Let $a,b\in\mathbb{A}$ with $b\ne 0$ and $\gcd(b,a)=1$. Let $m=(m_1,m_2)\in\mathbb{A}^2$. Suppose that $\gcd(b,m_1,m_2)=1$. If $p\ge 3$, then we have

$$\big|G(\frac{a}{b},m)\big| \le |b|^{\frac{1}{2}}.$$

Proof Without loss of generality, we assume that $a\ne 0$ and $\mathrm{ord}b\ge 1$. Also, b is monic. There exist $\iota, j_1,\cdots,j_\iota\in\mathbb{N}_+$ and distinct monic irreducible polynomials $\sigma_1,\cdots,\sigma_\iota$ in $\mathbb{A}$ such that $b=\prod\limits_{i=1}^{\iota}\sigma_i^{j_i}$. We prove the lemma by induction on ι.

For $\iota=1$, the lemma follows from Lemma 6.

Let $\iota\in\mathbb{N}$ with $\iota\ge 2$. Suppose that the lemma is true for $\iota-1$. We now prove that the claim holds for ι. Since $\gcd(b,a)=1$, we can find $a_l, a'\in\mathbb{A}^\times$ such that

$$\frac{a}{\prod_{i=1}^{\iota}\sigma_i^{j_i}} = \frac{a_l}{\sigma_l^{j_l}} + \frac{a'}{\prod_{i=1}^{\iota-1}\sigma_i^{j_i}} \text{ and } \gcd(\sigma_l^{j_l},a_l)=\gcd(\prod_{i=1}^{\iota-1}\sigma_i^{j_i},a')=1.$$

By Lemmas 4 and 6, we have

$$\big|G(\frac{a}{\prod_{i=1}^{\iota}\sigma_i^{j_i}},m)\big| = \big|G(\frac{a_l}{\sigma_l^{j_l}},m)\big|\Big|G(\frac{a'}{\prod_{i=1}^{\iota-1}\sigma_i^{j_i}},m)\Big| \le |\sigma_l|^{\frac{j_l}{2}}\Big|G(\frac{a'}{\prod_{i=1}^{\iota-1}\sigma_i^{j_i}},m)\Big|.$$

By the induction hypothesis, the proposition follows.

4 Estimates for S_N

For the present, we fix $N\in\mathbb{N}_+$ and $A\subseteq\mathbb{G}_N\times\mathbb{G}_{2N}$ with $|A|=\delta q^{3N}$. Throughout this section, we assume that the following hypothesis holds.

Hypothesis A $p\ge 3,\ (A-A)\cap\{\overrightarrow{d}: d\in\mathbb{A}^\times\}=\emptyset$ and $\delta\ge q^{1-\frac{N}{12}}$.

Take $\theta\in\mathbb{N}_+$ with $q^{-\theta}<\delta\le q^{1-\theta}$. Then $N\ge 12\theta$. Write $M=N-6\theta$.

The characteristic function $1_A:\mathbb{A}^2\to\mathbb{R}$ of A is defined by

$$1_A(m)=\begin{cases}1, & \text{if } m\in A,\\ 0, & \text{otherwise.}\end{cases}$$

Write $\Gamma_N=\mathbb{G}_N\times\mathbb{G}_{2N}$. We define the balanced function $f_A:\mathbb{A}^2\to\mathbb{R}$ of A to be $f_A=1_A-\delta 1_{\Gamma_N}$.

Let $b\in\mathbb{A}^\times$ with b monic. Write

$$\mathcal{A}_b=\big\{(a_1,a_2)\in\mathbb{A}^2:\gcd(b,a_1,a_2)=1,\ \mathrm{ord}a_j<\mathrm{ord}b\ (1\le j\le 2)\big\}.$$

For $(a_1,a_2)\in\mathcal{A}_b$, we define the Farey arc $F(b,a_1,a_2)$ to be

$$F(b,a_1,a_2)=\Big\{(\alpha_1,\alpha_2)\in\mathbb{T}^2:|\alpha_j-\frac{a_j}{b}|<q^{-jM}|b|^{-1}\ (1\le j\le 2)\Big\}.$$

Also, we define

$$F_b = \bigcup_{(a_1,a_2)\in\mathcal{A}_b} F(b,a_1,a_2).$$

We say $F(b,a_1,a_2)$ is major if $\mathrm{ord} b \le 2\theta+3$ and minor if $\mathrm{ord} b > 2\theta+3$. Let

$$\mathcal{B} = \{b \in \mathbb{A}^\times : b \text{ monic},\ \mathrm{ord} b \le 2\theta+3\}.$$

We define the major arcs $\mathfrak{M}$ and the minor arcs $\mathfrak{m}$ as follows:

$$\mathfrak{M} = \bigcup_{b\in\mathcal{B}} F_b \text{ and } \mathfrak{m} = \mathbb{T}^2 \setminus \mathfrak{M}.$$

Lemma 8 Let $b, b' \in \mathcal{B}$. Suppose that $(a_1,a_2)\in\mathcal{A}_b$ and $(a_1',a_2')\in\mathcal{A}_{b'}$. If $(b,a_1,a_2) \ne (b',a_1',a_2')$, then we have

$$F(b,a_1,a_2)\cap F(b',a_1',a_2') = \emptyset.$$

Proof To prove the lemma, we suppose the contrary. Then there exists

$$(\alpha_1,\alpha_2)\in F(b,a_1,a_2)\cap F(b',a_1',a_2').$$

Let $1\le j\le 2$. Since

$$\big|\frac{a_j}{b}-\frac{a_j'}{b'}\big| \le \max\big\{\big|\alpha_j-\frac{a_j}{b}\big|,\ \big|\alpha_j-\frac{a_j'}{b'}\big|\big\} < q^{-jM}\max\big\{|b|^{-1},|b'|^{-1}\big\},$$

it follows that

$$|a_jb'-a_j'b| < q^{-jM}\max\{|b|,|b'|\} \le q^{2\theta+3-M} \le q^{-\theta} < 1.$$

Thus $a_jb'=a_j'b$. Let $A_j, B_j \in \mathbb{A}$ with B_j monic such that

$$\gcd(B_j,A_j)=1 \text{ and } \frac{A_j}{B_j}=\frac{a_j}{b}=\frac{a_j'}{b'}.$$

It is easy to see that $b=\mathrm{lcm}(B_1,B_2)=b'$. It follows that $a_j=a_j'$. This leads to a contradiction, and the lemma follows.

Proposition 9 If $b\in\mathcal{B}$, then for any $\alpha\in F_b$, we have

$$|S_N(\alpha)| \le q^N|b|^{-1/2}.$$

Proof Write $(\alpha_1,\alpha_2)=\alpha$. Take $a=(a_1,a_2)\in\mathcal{A}_b$ such that $\alpha\in F(b,a_1,a_2)$. Since

$$|\alpha_2-\frac{a_2}{b}| < q^{-2M}|b|^{-1} \le q^{-N}|b|^{-1} \text{ and } \mathrm{ord} b \le 2\theta+3 < N,$$

by Lemma 2, we have

$$S_N(\alpha) = \frac{1}{|b|}G(\frac{1}{b},a)S_N(\alpha-\frac{1}{b}a).$$

It follows from Proposition 7 that

$$|S_N(\alpha)| \le |b|^{-\frac{1}{2}}|S_N(\alpha - \frac{1}{b}a)| \le |\mathbb{G}_N||b|^{-1/2}.$$

Proposition 10 For any $\alpha \in \mathfrak{m}$, we have

$$|S_N(\alpha)| \le \frac{\delta}{4}q^N.$$

Proof Write $\alpha = (\alpha_1, \alpha_2)$. By using Lemma 3 for $r_1 = 0$ and $r_2 = N$, we can find a monic polynomial b in $\mathbb{A}^\times$ and $a = (a_1, a_2) \in \mathbb{A}^2$ such that

$$\mathrm{ord} b \le N,\ \gcd(b, a_1, a_2) = 1,\ \mathrm{ord} a_j < \mathrm{ord} b \text{ and } \big|\alpha_j - \frac{a_j}{b}\big| < q^{-(j-1)N}|b|^{-1}\ (1 \le j \le 2).$$

Write $\beta = (\beta_1, \beta_2) = \alpha - \frac{1}{b}a$. If $\mathrm{ord} b \ge 2\theta + 4$, by Lemma 2 and Proposition 7, we have

$$|S_N(\alpha)| \le |b|^{-1}|G(\frac{1}{b}, a)||S_N(\beta)| \le |b|^{-\frac{1}{2}}|S_N(\beta)| \le q^{-\theta-2}|\mathbb{G}_N| \le \frac{\delta}{4}q^N.$$

In the following, we assume that $\mathrm{ord} b \le 2\theta + 3$. Consider the following estimate

$$\begin{aligned} \big|S_N(\beta)\big|^2 &= \sum_{d,d' \in \mathbb{G}_N} e\big(\beta_1(d-d') + \beta_2(d+d')(d-d')\big) \\ &= \sum_{d,d' \in \mathbb{G}_N} e(\beta_1 d + \beta_2 dd') \\ &\le \sum_{d \in \mathbb{G}_N} \Big|\sum_{d' \in \mathbb{G}_N} e(\beta_2 dd')\Big|. \end{aligned}$$

For $d \in \mathbb{G}_N$, since

$$\mathrm{ord}(\beta_2 d) = \mathrm{ord}\beta_2 + \mathrm{ord} d \le (-N - \mathrm{ord} b - 1) + (N - 1) \le -2,$$

it follows that $\{\beta_2 d\} = \beta_2 d$. By Lemma 1, we have

$$\big|S_N(\beta)\big|^2 \le \sum_{d \in \mathbb{G}_N, \mathrm{ord}(\beta_2 d) < -N} q^N \le |\beta_2|^{-1}.$$

Combining Lemma 2 and Proposition 7 with the above inequality, it follows that

$$|S_N(\alpha)| \le |b|^{-1}|G(\frac{1}{b}, a)||S_N(\beta)| \le |b|^{-\frac{1}{2}}|S_N(\beta)| \le |b|^{-\frac{1}{2}}|\beta_2|^{-\frac{1}{2}}. \tag{4.1}$$

Since $\alpha \notin \mathfrak{M}$, there are two cases.

Case 1 Suppose that $|\beta_2| \ge q^{-2M}|b|^{-1}$. By (4.1), we have

$$|S_N(\alpha)| \le q^M = q^{N-6\theta} \le \frac{\delta}{4}q^N.$$

Case 2 Suppose that $|\beta_1| \ge q^{-M}|b|^{-1}$ and $|\beta_2| < q^{-2M}|b|^{-1}$.

If $\mathrm{ord}\beta_2 \geq 1-N+\mathrm{ord}\beta_1$, then by (4.1), we have

$$|S_N(\alpha)| \leq |b|^{-\frac{1}{2}}|\beta_1|^{-\frac{1}{2}}q^{\frac{N-1}{2}} \leq q^{\frac{M+N-1}{2}} \leq q^{N-3\theta} \leq \frac{\delta}{4}q^N.$$

Thus, it remains to estimate $|S_N(\alpha)|$ under the additional assumption $\mathrm{ord}\beta_2 \leq \mathrm{ord}\beta_1 - N$.

Write $L_1 = -\mathrm{ord}\beta_1$, then $1 \leq L_1 \leq M+\mathrm{ord}b$; write $L_2 = -\mathrm{ord}\beta_2$, then $L_2 \geq 1+2M+\mathrm{ord}b$; write $K = \lfloor\frac{L_1+N}{2}\rfloor$, since $L_1 \leq M+2\theta+3 < N$, we have $L_1 \leq K \leq N-1$.

For $j \in \mathbb{N}$, write $\mathcal{C}_j = \{d \in \mathbb{A} : \mathrm{ord}d = j\}$, then

$$S_N(\beta) = \sum_{d\in\mathbb{G}_K} e(\beta\overrightarrow{d}) + \sum_{j=K}^{N-1}\sum_{d\in\mathcal{C}_j} e(\beta\overrightarrow{d}).$$

Let $d \in \mathbb{G}_K$. By the assumption $\mathrm{ord}\beta_2 \leq \mathrm{ord}\beta_1 - N$, we have

$$\mathrm{ord}(\beta_2 d^2) = 2\mathrm{ord}d - L_2 \leq 2(K-1) + (-N-L_1) \leq -2.$$

It follows that $e(\beta_2 d^2) = 1$. Note that $\mathrm{ord}\{\beta_1\} = -L_1 \geq -K$, by Lemma 1, we have

$$\sum_{d\in\mathbb{G}_K} e(\beta\overrightarrow{d}) = \sum_{d\in\mathbb{G}_K} e(\beta_1 d) = 0.$$

Thus

$$S_N(\beta) = \sum_{I=K}^{N-1}\sum_{d\in\mathcal{C}_I} e(\beta\overrightarrow{d}). \tag{4.2}$$

Take the sequences $\{\mu_i\}_{i=-\infty}^{-L_1}$ and $\{\nu_j\}_{j=-\infty}^{-L_2}$ in $\mathbb{F}_q$ such that

$$\beta_1 = \sum_{i\leq -L_1} \mu_i t^i \text{ and } \beta_2 = \sum_{j\leq -L_2} \nu_j t^j.$$

Let $K \leq I \leq N-1$ and $d \in \mathcal{C}_I$. Take $c_0, c_1, \cdots, c_I \in \mathbb{F}_q$ with $c_I \neq 0$ such that $d = \sum\limits_{i=0}^{I} c_i t^i$. Then

$$\mathrm{res}(\beta\overrightarrow{d}) = \sum_{i=L_1-1}^{I} \mu_{-i-1}c_i + \sum_{l=L_2-1}^{2I} \nu_{-l-1} \sum_{0\leq i,j\leq I, i+j=l} c_i c_j.$$

For $0 \leq i,j \leq I$, if $i+j \geq L_2-1$, by the assumption $\mathrm{ord}\beta_2 \leq \mathrm{ord}\beta_1 - N$, we have

$$\min\{i,j\} \geq L_2 - 1 - I \geq (N+L_1) - 1 - (N-1) = L_1.$$

Thus, there exists the polynomial $Q_I(t_1, \cdots, t_{I-L_1+1})$ of $(I-L_1+1)$ variables over $\mathbb{F}_q$ such that

$$\mathrm{res}(\beta\overrightarrow{d}) = \mu_{-L_1}c_{L_1-1} + Q_I(c_{L_1}, c_{L_1+1}, \cdots, c_I).$$

Substituting this into the definition of the function $e(\cdot)$, and noting that $\mu_{-L_1} \neq 0$, we have

$$\sum_{d\in\mathcal{C}_I} e(\beta\overrightarrow{d}) = \sum_{j\neq L_1-1, 0\leq j\leq I-1}\ \sum_{c_j\in\mathbb{F}_q}\ \sum_{c_I\in\mathbb{F}_q^\times} e_q\big(Q_I(c_{L_1}, \cdots, c_I)\big) \sum_{c_{L_1-1}\in\mathbb{F}_q} e_q\big(\mu_{-L_1}c_{L_1-1}\big) = 0.$$

It follows from (4.2) that $S_N(\beta)=0$. Finally, by Lemma 2, we have $S_N(\alpha)=0$.

Combining the above two cases, we complete the proof of the proposition.

5 Density Increment

In this section, we continue to fix $N\in\mathbb{N}_+$ and $A\subseteq\Gamma_N$ with $|A|=\delta q^{3N}$. Also, we assume that Hypothesis A holds.

Lemma 11

$$\int_{\mathbb{T}^2}|\widehat{f_A}(\alpha)|^2|S_N(\alpha)|d\alpha\geq\frac{1}{2}\delta^2q^{4N}.$$

Proof Write $\mathrm{I}=\sum\limits_{d\in\mathbb{G}_N,m\in\mathbb{A}^2}f_A(m)f_A(m+\overrightarrow{d})$. By (2.1), we have

$$\mathrm{I}=\sum_{d\in\mathbb{G}_N,m,n\in\mathbb{A}^2}f_A(m)f_A(n)\int_{\mathbb{T}^2}e(\alpha(m+\overrightarrow{d}-n))d\alpha=\int_{\mathbb{T}^2}|\widehat{f_A}(\alpha)|^2S_N(\alpha)\mathrm{d}\alpha. \tag{5.1}$$

If $d\in\mathbb{G}_N$, then $\overrightarrow{d}\in\Gamma_N$. Thus $\Gamma_N+\overrightarrow{d}=\Gamma_N-\overrightarrow{d}=\Gamma_N$. It follows that $(A-A)\cap\{\overrightarrow{d}:d\in\mathbb{A}^\times\}=\emptyset$ from Hypothesis A. Thus

$$\begin{aligned}\mathrm{I}&=\sum_{m\in\mathbb{A}^2}1_A(m)-\delta\sum_{d\in\mathbb{G}_N,m\in\mathbb{A}^2}1_A(m)\Big(1_{\Gamma_N}(m+\overrightarrow{d})+1_{\Gamma_N}(m-\overrightarrow{d})\Big)\\&\quad+\delta^2\sum_{d\in\mathbb{G}_N,m\in\mathbb{A}^2}1_{\Gamma_N}(m)1_{\Gamma_N}(m+\overrightarrow{d})\\&=|A|-\delta\sum_{d\in\mathbb{G}_N}\Big(\big|A\cap(\Gamma_N-\overrightarrow{d})\big|+\big|A\cap(\Gamma_N+\overrightarrow{d})\big|\Big)+\delta^2\sum_{d\in\mathbb{G}_N}\big|\Gamma_N\cap(\Gamma_N-\overrightarrow{d})\big|\\&=|A|-2\delta|A|\big|\mathbb{G}_N\big|+\delta^2\big|\mathbb{G}_N\big|\big|\Gamma_N\big|\\&=-\delta^2q^{4N}\big(1-\frac{1}{\delta q^N}\big).\end{aligned}$$

By Hypothesis A, we have $\delta q^N\geq q^{1+\frac{11N}{12}}\geq 2$. It follows that

$$\mathrm{I}\leq-\frac{1}{2}\delta^2q^{4N}. \tag{5.2}$$

Finally, by (5.1) and (5.2), we obtain

$$\int_{\mathbb{T}^2}|\widehat{f_A}(\alpha)|^2|S_N(\alpha)|d\alpha\geq|\mathrm{I}|\geq\frac{1}{2}\delta^2q^{4N}.$$

Lemma 12 There exists a monic polynomial b_0 in $\mathbb{G}_{2\theta+4}$ such that

$$\int_{F_{b_0}}|\widehat{f_A}(\alpha)|^2d\alpha\geq c\delta^3q^{3N},$$

where $0<c<1$ is a constant depending only on q.

Proof By Proposition 10, we have

$$\begin{aligned}\int_{\mathfrak{m}}|\widehat{f_A}(\alpha)|^2|S_N(\alpha)|d\alpha &\le \frac{\delta}{4}q^N\int_{\mathfrak{m}}|\widehat{f_A}(\alpha)|^2d\alpha\\ &\le \frac{\delta}{4}q^N\sum_{m\in\mathbb{A}^2}|f_A(m)|^2\\ &\le \frac{\delta^2}{4}q^{4N}.\end{aligned}$$

Write

$$\mathrm{II}=\int_{\mathfrak{M}}|\widehat{f_A}(\alpha)|^2|S_N(\alpha)|d\alpha.$$

Combining the above inequality with Lemma 11, it follows that

$$\mathrm{II}\ge\int_{\mathbb{T}^2}|\widehat{f_A}(\alpha)|^2|S_N(\alpha)|\mathrm{d}\alpha-\frac{\delta^2}{4}q^{4N}\ge\frac{\delta^2}{4}q^{4N}. \tag{5.3}$$

For $j\in\mathbb{N}$, write $\mathcal{O}_j=\{b\in\mathbb{A}^\times: b \text{ monic},\ \mathrm{ord}b=j\}$. By Lemma 8 and Proposition 9, we have

$$\mathrm{II}=\sum_{j=0}^{2\theta+3}\sum_{b\in\mathcal{O}_j}\int_{F_b}|\widehat{f_A}(\alpha)|^2|S_N(\alpha)|d\alpha\le\sum_{j=0}^{2\theta+3}q^{N-\frac{j}{2}}\sum_{b\in\mathcal{O}_j}\int_{F_b}|\widehat{f_A}(\alpha)|^2d\alpha.$$

Take a monic polynomial b_0 in $\mathbb{G}_{2\theta+4}$ such that

$$\int_{F_{b_0}}|\widehat{f_A}(\alpha)|^2\mathrm{d}\alpha=\max_{0\le j\le 2\theta+3,b\in\mathcal{O}_j}\int_{F_b}|\widehat{f_A}(\alpha)|^2\mathrm{d}\alpha.$$

It follows from the above inequality that

$$\mathrm{II}\le\int_{F_{b_0}}|\widehat{f_A}(\alpha)|^2\mathrm{d}\alpha\sum_{j=0}^{2\theta+3}\big|\mathcal{O}_j\big|q^{N-\frac{j}{2}}=\int_{F_{b_0}}|\widehat{f_A}(\alpha)|^2\mathrm{d}\alpha\sum_{j=0}^{2\theta+3}q^{N+\frac{j}{2}}.$$

Since $\delta\le q^{1-\theta}$, we can find a constant $c'>1$, depending only on q, such that

$$\mathrm{II}\le\frac{c'}{\delta}q^N\int_{F_{b_0}}|\widehat{f_A}(\alpha)|^2d\alpha.$$

By taking $c=\frac{1}{4c'}$, the lemma follows from (5.3).

Lemma 13 There exists $n_0\in\Gamma_N$ such that

$$|A\cap(n_0+b_0\Gamma_M)|\ge\delta(1+\frac{c}{2}\delta)q^{3M},$$

where $b_0\Gamma_M=\big\{b_0m: m\in\Gamma_M\big\}$.

Proof Write $P=b_0\Gamma_M$. Let $m=(m_1,m_2)\in\Gamma_M$ and $1\le j\le 2$. Since

$$\mathrm{ord}(b_0m_j)=\mathrm{ord}b_0+\mathrm{ord}m_j\le(2\theta+3)+(jM-1)\le jN-1,$$

we have $b_0 m \in \Gamma_N$. Thus, $P \subseteq \Gamma_N$. Also, we have

$$\mathrm{supp} f_A * 1_{-P} \subseteq \mathrm{supp} f_A + \mathrm{supp} 1_{-P} \subseteq \Gamma_N + (-P) = \Gamma_N.$$

For $n \in \Gamma_N$, we have

$$\begin{aligned} f_A * 1_{-P}(n) &= \sum_{m \in \mathbb{A}^2} 1_A(m) 1_P(m-n) - \delta \sum_{m \in \mathbb{A}^2} 1_{\Gamma_N}(m) 1_P(m-n) \\ &= |A \cap (n+P)| - \delta \big|\Gamma_N \cap (n+P)\big| \\ &= |A \cap (n+P)| - \delta |P|. \end{aligned} \tag{5.4}$$

If there exists $n_0 \in \Gamma_N$ such that $f_A * 1_{-P}(n_0) \geq \delta|P|$, then

$$|A \cap (n_0 + P)| = f_A * 1_{-P}(n_0) + \delta|P| \geq 2\delta|P| \geq \delta(1 + \frac{c}{2}\delta) q^{3M}.$$

Thus, in the following, we assume that $f_A * 1_{-P}(n) \leq \delta|P|$ for all $n \in \Gamma_N$. It follows from (5.4) that

$$\big|f_A * 1_{-P}(n)\big| \leq \delta|P|. \tag{5.5}$$

Let $\alpha = (\alpha_1, \alpha_2) \in F_{b_0}$. Take $a = (a_1, a_2) \in \mathcal{A}_{b_0}$ such that $\alpha \in F(b_0, a_1, a_2)$. Since

$$\begin{aligned} \mathrm{ord}\big(m_j(b_0\alpha_j - a_j)\big) &= \mathrm{ord} m_j + \mathrm{ord} b_0 + \mathrm{ord}(\alpha_j - \frac{a_j}{b_0}) \\ &\leq (jM - 1) + \mathrm{ord} b_0 + (-jM - \mathrm{ord} b_0 - 1) = -2, \end{aligned}$$

we have $e(b_0 m_j \alpha_j) = e(m_j a_j) = 1$. Thus, $\widehat{1_{-P}}(\alpha) = |P|$. It follows from (5.5) that

$$\begin{aligned} \int_{F_{b_0}} |\widehat{f_A}(\alpha)|^2 d\alpha &= \frac{1}{|P|^2} \int_{F_{b_0}} |\widehat{f_A * 1_{-P}}(\alpha)|^2 d\alpha \\ &\leq \frac{1}{|P|^2} \sum_{n \in \mathbb{A}^2} |f_A * 1_{-P}(n)|^2 \\ &\leq \frac{\delta}{|P|} \sum_{n \in \mathbb{A}^2} |f_A * 1_{-P}(n)|. \end{aligned}$$

By Lemma 12, we have

$$\sum_{n \in \mathbb{A}^2} |f_A * 1_{-P}(n)| \geq c\delta^2 q^{3(M+N)}.$$

Note that $\sum\limits_{n \in \mathbb{A}^2} f_A(n) = 0$, we have

$$\sum_{n \in \mathbb{A}^2} \big(f_A * 1_{-P}\big)_+(n) \geq \frac{c}{2}\delta^2 q^{3(M+N)}.$$

Take $n_0 \in \Gamma_N$ such that

$$f_A * 1_{-P}(n_0) = \max_{n \in \Gamma_N} f_A * 1_{-P}(n).$$

By (5.4), we have

$$|A\cap(n_0+P)|=\delta|P|+f_A*1_{-P}(n_0)\geq\delta|P|+\frac{1}{|\Gamma_N|}\sum_{n\in\mathbb{A}^2}\big(f_A*1_{-P}\big)_+(n)\geq\delta(1+\frac{c}{2}\delta)q^{3M}.$$

Proposition 14 There exist $N'\in\mathbb{N}_+$ and $A'\subseteq\Gamma_{N'}$ with $|A'|=\delta' q^{3N'}$ such that
(i) $(A'-A')\cap\big\{\overrightarrow{d}:d\in\mathbb{A}^\times\big\}=\emptyset$;
(ii) $\delta'\geq\delta(1+\frac{c}{2}\delta)$;
(iii) $N'\geq N-11\log_q\big(\frac{q}{\delta}\big)$, where $\log_q x=\log x/\log q$.

Proof Write $L=\mathrm{ord}b_0$ and $T=|b_0|$. Then $0\leq L\leq 2\theta+3$. By taking $N'=M-L$, property (iii) follows. Take $d_1,\cdots,d_T\in\mathbb{G}_M$ and $d_1',\cdots,d_T'\in\mathbb{G}_{2M-L}$ such that

$$\mathbb{G}_M=\bigcup_{i=1}^T\big(d_i+\mathbb{G}_{N'}\big)\text{ and }\mathbb{G}_{2M-L}=\bigcup_{i=1}^T\big(d_i'+\mathbb{G}_{2N'}\big).\tag{5.6}$$

For $d\in\mathbb{G}_L$ and $1\leq i,j\leq T$, write

$$\Upsilon_{d,i,j}=n_0+(0,b_0d)+\overrightarrow{b_0}\odot(d_i,d_j')+\overrightarrow{b_0}\odot\Gamma_{N'},$$

where

$$\overrightarrow{b_0}\odot(d_i,d_j')=(b_0d_i,b_0^2d_j')\text{ and }\overrightarrow{b_0}\odot\Gamma_{N'}=\big\{\overrightarrow{b_0}\odot m:m\in\Gamma_{N'}\big\}.$$

Let $m=(m_1,m_2)\in\Gamma_M$. Take $d\in\mathbb{G}_L$ and $d'\in\mathbb{G}_{2M-L}$ such that $m_2=d+b_0d'$. By (5.6), we can find $1\leq i,j\leq T$ such that $(m_1,d')\in(d_i,d_j')+\Gamma_{N'}$. Then we have

$$n_0+b_0m=n_0+(0,b_0d)+\overrightarrow{b_0}\odot(m_1,d')\in\Upsilon_{d,i,j}.$$

Thus, we see that

$$n_0+b_0\Gamma_M=\bigcup_{d\in\mathbb{G}_L,1\leq i,j\leq T}\Upsilon_{d,i,j}.$$

Take $d_0\in\mathbb{G}_L$ and $1\leq i_0,j_0\leq T$ such that

$$\big|A\cap\Upsilon_{d_0,i_0,j_0}\big|=\max_{d\in\mathbb{G}_L,1\leq i,j\leq T}\big|A\cap\Upsilon_{d,i,j}\big|.$$

By Lemma 13, we have

$$\big|A\cap\Upsilon_{d_0,i_0,j_0}\big|\geq\frac{1}{T^3}\sum_{d\in\mathbb{G}_L,1\leq i,j\leq T}\big|A\cap\Upsilon_{d,i,j}\big|=\frac{1}{T^3}|A\cap(n_0+b_0\Gamma_M)|\geq\delta(1+\frac{c}{2}\delta)q^{3N'}.$$

Consider the bijection $f:\Gamma_{N'}\to\Upsilon_{d_0,i_0,j_0}$ defined by

$$f(t)=n_0+(0,b_0d_0)+\overrightarrow{b_0}\odot(d_{i_0},d_{j_0}')+\overrightarrow{b_0}\odot t.$$

By taking $A'=f^{-1}(A\cap\Upsilon_{d_0,i_0,j_0})$, property (ii) follows. To prove property (i), we suppose the contrary. Then there exist $t_1,t_2\in A'$ and $d\in\mathbb{A}^\times$ such that $t_2-t_1=\overrightarrow{d}$. It follows that

$$f(t_2)-f(t_1)=\overrightarrow{b_0}\odot\overrightarrow{d}=\overrightarrow{b_0d}\in A-A,$$

which contradicts Hypothesis A. This completes the proof of the proposition.

6 Proof of Theorem 1

Proposition 15 If $p \geq 3$, then there exists a constant $C_1 > 0$, depending only on q, such that the following inequality holds. Let $N \in \mathbb{N}$ with $N \geq 2$ and $A \subseteq \mathbb{G}_N \times \mathbb{G}_{2N}$. If $(A - A) \bigcap \left\{ \overrightarrow{d} : d \in \mathbb{A}^\times \right\} = \emptyset$, then we have

$$|A| \leq C_1 q^{3N} \frac{\log N}{N}.$$

Remark 3 Note that $d \in \mathbb{G}_N \Leftrightarrow d^2 \in \mathbb{G}_{2N}$, the form of Proposition 15 is more natural than of Theorem 1.

Proof Write $|A| = \delta q^{3N}$. If $\delta \leq q^{1-\frac{N}{12}}$, then by taking

$$C_1 = \sup_{N \geq 2} q^{1-N/12} \frac{N}{\log N},$$

the proposition follows. Thus in the following, we assume that $\delta \geq q^{1-\frac{N}{12}}$.

Now, we recursively define a sequence of triples (N_i, A_i, δ_i) with $N_i \in \mathbb{N}_+,\ A_i \subseteq \Gamma_{N_i}$ and $|A_i| = \delta_i q^{3N_i}$ as follows. Take $(N_0, A_0, \delta_0) = (N, A, \delta)$. Let $i \in \mathbb{N}$. Suppose that (N_i, A_i, δ_i) is defined. If $\delta_i < q^{1-\frac{N_i}{12}}$, we stop the definition. If $\delta_i \geq q^{1-\frac{N_i}{12}}$, by Proposition 14, we can find $N_{i+1} \in \mathbb{N}_+$ and $A_{i+1} \subseteq \Gamma_{N_{i+1}}$ with $|A_{i+1}| = \delta_{i+1} q^{3N_{i+1}}$ such that

(i) $(A_{i+1} - A_{i+1}) \cap \left\{ \overrightarrow{d} : d \in \mathbb{A}^\times \right\} = \emptyset$;

(ii) $\delta_{i+1} \geq \delta_i (1 + \frac{c}{2} \delta_i)$;

(iii) $N_{i+1} \geq N_i - 11 \log_q \left(\frac{q}{\delta_i} \right)$.

Write $c' = \frac{c}{2}$. It follows from (ii) that $\delta_{i+1} - \delta_i \geq c' \delta^2$. Since $\delta_{i+1} \leq 1$, this process produces a finite sequence $\left\{ (N_i, A_i, \delta_i) \right\}_{i=1}^{J}$. Then for any $0 \leq i \leq J-1$, the triple $(N_{i+1}, A_{i+1}, \delta_{i+1})$ satisfies the above conditions (i)–(iii). Also, we have

$$\delta_J < q^{1-\frac{N_J}{12}}. \tag{6.1}$$

Claim 1 For $j \in \mathbb{N}$, write $I_j = \lceil \frac{1}{2^j c' \delta} \rceil$. If $i \geq \sum_{l=0}^{j} I_l$, then $\delta_i \geq 2^{j+1} \delta$.

Proof We prove the claim by induction on j. For $j = 0$, we have $I_j \geq \frac{1}{c' \delta}$. It follows from (ii) that

$$\delta_i \geq \delta_0 + c' i \delta_0^2.$$

Thus if $i \geq I_0$, then $\delta_i \geq 2\delta$.

Suppose that the claim holds for j. We now prove that the statement is true for $j+1$. Write $k = \sum_{l=0}^{j} I_l$. Let $i > k$. By (ii), we have $\delta_i \geq \delta_k + (i-k) c' \delta_k^2$. Thus, if $i \geq \sum_{l=0}^{j+1} I_l$, it follows from the induction hypothesis that

$$\delta_i \geq 2^{j+1} \delta + c' I_{j+1} (2^{j+1} \delta)^2 \geq 2^{j+2} \delta.$$

This completes the proof of the claim.

Take $j_0 \in \mathbb{N}$ such that $2^{j_0}\delta \le 1 < 2^{j_0+1}\delta$. Then we have

$$J < \sum_{0 \le i \le j_0} I_i \le \frac{2}{c'\delta} \sum_{i \in \mathbb{N}} 2^{-i} = \frac{4}{c'\delta}.$$

It follows from (iii) that

$$N_J \ge N - 11J \log_q \big(\frac{q}{\delta}\big) \ge N - \frac{44}{c'\delta} \log_q \big(\frac{q}{\delta}\big).$$

By (6.1), we have

$$\delta \le \delta_J \le q^{1-\frac{N}{12}} \big(\frac{q}{\delta}\big)^{\frac{11}{3c'\delta}}.$$

Thus, there exists a constant $C_1 > 1$, depending only on q, such that

$$2N \le \frac{C_1}{\delta} \log \frac{C_1}{\delta}.$$

Note that the function $x \log x$ on $[1, +\infty)$ is increasing, and the proposition follows since

$$\frac{2N}{\log 2N} \log \big(\frac{2N}{\log 2N}\big) \le 2N.$$

Proof of Theorem 1 Write $|A| = \delta q^{2N}$. If $N \le 7$, by taking $C = \frac{7}{\log 7}$, the theorem follows. In the following, we assume that $N \ge 8$. Write

$$N' = \big\lfloor \frac{N}{4} \big\rfloor, \ S = q^{N-N'} \text{ and } T = q^{N-2N'}.$$

For $1 \le i \le S$ and $1 \le j \le T$, take $d_i, d'_j \in \mathbb{G}_N$ such that

$$\mathbb{G}_N = \bigcup_{i=1}^{S} (d_i + \mathbb{G}_{N'}) = \bigcup_{j=1}^{T} (d'_j + \mathbb{G}_{2N'}).$$

Then, we have

$$\mathbb{G}_N^2 = \bigcup_{1 \le i \le S, 1 \le j \le T} (d_i + \mathbb{G}_{N'}) \times (d'_j + \mathbb{G}_{2N'}) = \bigcup_{1 \le i \le S, 1 \le j \le T} \big((d_i, d'_j) + \Gamma_{N'}\big).$$

Write

$$A_{i,j} = A \bigcap \big((d_i, d'_j) + \Gamma_{N'}\big).$$

Take $1 \le i_0 \le S$ and $1 \le j_0 \le T$ such that

$$\big|A_{i_0,j_0}\big| = \max_{1 \le i \le S, 1 \le j \le T} \big|A_{i,j}\big|.$$

Write $A' = A_{i_0,j_0}$. Then we have $(A' - A') \bigcap \big\{ \overrightarrow{d} : d \in \mathbb{A}^\times \big\} = \emptyset$ and

$$|A'| \ge \frac{1}{ST} \sum_{1 \le i \le S, 1 \le j \le T} |A_{i,j}| \ge \frac{1}{ST} \Big| \bigcup_{1 \le i \le S, 1 \le j \le T} A_{i,j} \Big| = \frac{1}{ST} |A| = \delta q^{3N'}.$$

Define $f:\Gamma_{N'}\to(d_{i_0},d'_{j_0})+\Gamma_{N'}$ to be $f(m)=(d_{i_0},d'_{j_0})+m$. Then f is a bijection. Take $B=f^{-1}(A')$. Since $B-B=A'-A'$, we have $(B-B)\bigcap\left\{\overrightarrow{d}:d\in\mathbb{A}^{\times}\right\}=\emptyset$. It follows from Proposition 15 that

$$|B|\le C_1q^{3N'}\frac{\log N'}{N'}\le C_1\frac{N}{N/4-1}q^{3N'}\frac{\log N}{N}.$$

Note that $N\ge 8$ and $\delta\le|B|q^{-3N'}$, by taking $C=8C_1$, the theorem follows.

7 Proof of Theorem 2

For $1\le s\le l$, take $c_{s1},c_{s2}\in\mathbb{A}$ such that $P_s(x)=c_{s1}x+c_{s2}x^2$. Write $\mathcal{P}=\left(c_{sj}\right)_{1\le s\le l,1\le j\le 2}$. Denote by r the rank of the matrix $\mathcal{P}$. Then $1\le r\le 2$. Thus, we divide into two case.

Case 1 Suppose that $r=2$. Without loss of generality, we assume that $\left(c_{11},c_{12}\right)$ and $\left(c_{21},c_{22}\right)$ are linearly independent. Write $\mathcal{R}=\left(c_{ij}\right)_{1\le i,j\le 2}$, $e_1=(1,0)$ and $e_2=(0,1)$. For $1\le i\le 2$, take $\xi'_i\in\mathbb{K}^2$ such that $\mathcal{R}\xi'_i=e_i$. When $l\ge 3$, take $\mathcal{D}=\left(d'_{tj}\right)_{1\le t\le l-2,1\le j\le 2}$ such that

$$\left(c_{t'j}\right)_{3\le t'\le l,1\le j\le 2}=\mathcal{D}\mathcal{R}.$$

Take $S\in\mathbb{N}$ with $S\ge 4$ and $D\in\mathbb{A}^{\times}$ such that

$$D,c_{ij}\in\mathbb{G}_S,\ \xi_i=D\xi'_i\in\mathbb{G}_S^2\ \ (1\le i,j\le 2).$$

If $l\ge 3$, we also require

$$d_{tj}=Dd'_{tj}\in\mathbb{G}_S\ (1\le t\le l-2,1\le j\le 2).$$

If $N\le S$, by taking $C'=\left(\frac{S}{\log S}\right)^{\frac{1}{l}}$, the theorem follows. Thus, we assume that $N\ge S+1$.

Claim 2 For $m\in\mathbb{G}_S^2$, write $B'_m=\left\{b\in\mathbb{G}_{N+S}^2:\mathcal{R}b+m\in A^2\right\}$. Then there exists $\underline{m}\in\mathbb{G}_S^2$ such that

$$\left|B'_{\underline{m}}\right|\ge q^{-2S}|A|^2.$$

Proof Let $a=(a_1,a_2)\in A^2$. For $1\le i\le 2$, take $a'_i\in\mathbb{G}_{N-\mathrm{ord}D}$ and $a''_i\in\mathbb{G}_{\mathrm{ord}D}$ such that $a_i=Da'_i+a''_i$. Write $b=\sum\limits_{i=1}^{2}a'_i\xi_i$ and $m'=(a''_1,a''_2)$. Then we have

$$b\in\mathbb{G}_{N+S}^2,\ m'\in\mathbb{G}_S^2\text{ and }\mathcal{R}b=a-m'.$$

It follows that $a\in\mathcal{R}\left(\mathbb{G}_{N+S}^2\right)+m'$. Thus, we see that

$$A^2\subseteq\bigcup_{m\in\mathbb{G}_S^2}\Big(\mathcal{R}\left(\mathbb{G}_{N+S}^2\right)+m\Big).\tag{7.1}$$

Take $\underline{m}\in\mathbb{G}_S^2$ such that $\left|B'_{\underline{m}}\right|=\max\limits_{m\in\mathbb{G}_S^2}\left|B'_m\right|$. By (7.1), we have

$$\left|B'_{\underline{m}}\right|\ge\frac{1}{q^{2S}}\sum_{m\in\mathbb{G}_S^2}\left|B'_m\right|\ge\frac{1}{q^{2S}}\Big|\bigcup_{m\in\mathbb{G}_S^2}\Big(\left(\mathcal{R}\left(\mathbb{G}_{N+S}^2\right)+m\right)\cap A^2\Big)\Big|=\frac{1}{q^{2S}}|A^2|.$$

This completes the proof of the claim.

Claim 3 Suppose that $l \geq 3$. For $m \in \mathbb{G}_{N+3S}^{l-2}$, write $B''_m = \big\{b \in B'_{\underline{m}} : \mathcal{DR}b + m \in A^{l-2}\big\}$. Then there exists $\underline{m'} \in \mathbb{G}_{N+3S}^{l-2}$ such that

$$\big|B''_{\underline{m'}}\big| \geq q^{-(l-2)N-(3l-4)S}|A|^l.$$

Proof Let $n \in \mathbb{A}^{l-2}$ and $b \in B'_{\underline{m}}$. If $n + \mathcal{DR}b \in A^{l-2}$, then $n \in \mathbb{G}_{N+3S}^{l-2}$. Thus

$$\sum_{n \in \mathbb{G}_{N+3S}^{l-2}} \sum_{b \in B'_{\underline{m}}} 1_{A^{l-2}}\big(n + \mathcal{DR}b\big) = \sum_{b \in B'_{\underline{m}}} \sum_{n \in \mathbb{A}^{l-2}} 1_{A^{l-2}}\big(n + \mathcal{DR}b\big) = |B'_{\underline{m}}||A|^{l-2}. \tag{7.2}$$

Take $\underline{m'} \in \mathbb{G}_{N+3S}^{l-2}$ such that $\big|B''_{\underline{m'}}\big| = \max\limits_{m \in \mathbb{G}_{N+3S}^{l-2}} \big|B''_m\big|$. Then we have

$$\big|B''_{\underline{m'}}\big| \geq \frac{1}{q^{(l-2)(N+3S)}} \sum_{m \in \mathbb{G}_{N+3S}^{l-2}} |B''_m| = \frac{1}{q^{(l-2)(N+3S)}} \sum_{m \in \mathbb{G}_{N+3S}^{l-2}} \sum_{b \in B'_{\underline{m}}} 1_{A^{l-2}}\big(m + \mathcal{DR}b\big).$$

The claim follows from (7.2) and Claim 2.

Write

$$\overline{m} = \begin{cases} \underline{m}, & \text{if } l = 2, \\ (\underline{m}, \underline{m'}), & \text{if } l \geq 3. \end{cases}$$

Define $B = \big\{b \in \mathbb{G}_{N+S}^2 : \mathcal{P}b + \overline{m} \in A^l\big\}$. Then by Claims 2 and 3, we have

$$|B| \geq q^{-(l-2)N-(3l-4)S}|A|^l. \tag{7.3}$$

Suppose that there exists $d \in \mathbb{A}$ suth that $b' - b = \overrightarrow{d}$ for some $b, b' \in B$. Since

$$\mathcal{P}\overrightarrow{d} = \mathcal{P}b' - \mathcal{P}b \in A^l - A^l,$$

we have

$$\big\{P_1(d), \cdots, P_l(d)\big\} \subseteq (A - A),$$

from which it follows that $d = 0$. Thus, we obtain

$$(B - B)\bigcap\big\{\overrightarrow{d} : d \in \mathbb{A}^\times\big\} = \emptyset.$$

By Theorem 1, we have

$$|B| \leq Cq^{2(N+S)}\frac{\log(N+S)}{N+S} \leq Cq^{2(N+S)}\frac{\log N}{N}.$$

By taking $C' = C^{\frac{1}{l}}q^{\frac{(3l-2)S}{l}}$, the theorem follows from (7.3).

Case 2 Suppose that $r = 1$. Without loss of generality, we assume that $\mathcal{R} = \big(c_{11}, c_{12}\big) \neq 0$. Take $\xi' \in \mathbb{K}^2$ such that $\mathcal{R}\xi' = 1$. When $l \geq 2$, take $\mathcal{D} = \big(d'_1, \cdots, d'_{l-1}\big)$ such that $\big(c_{t'j}\big)_{2 \leq t' \leq l, 1 \leq j \leq 2} = \mathcal{DR}$.

Take $S \in \mathbb{N}$ with $S \geq 4$ and $D \in \mathbb{A}^{\times}$ such that

$$D, c_{1j} \in \mathbb{G}_S \ (1 \leq j \leq 2),\ \xi = D\xi' \in \mathbb{G}_S^2.$$

If $l \geq 2$, we also require

$$d_t = Dd_t' \in \mathbb{G}_S \ (1 \leq t \leq l-1).$$

If $N \leq S$, by taking $C' = \left(\frac{S}{\log S}\right)^{\frac{1}{l}}$, the theorem follows. Thus we assume that $N \geq S+1$.

Claim 4 For $m \in \mathbb{G}_S$, write $B_m' = \left\{b \in \mathbb{G}_{N+S}^2 : \mathcal{R}b + m \in A\right\}$. Then there exists $\underline{m} \in \mathbb{G}_S$ such that

$$\left|B_{\underline{m}}'\right| \geq q^{N-S}|A|.$$

Proof Let $a \in A$. Take $a' \in \mathbb{G}_{N-\mathrm{ord}D}$ and $a'' \in \mathbb{G}_{\mathrm{ord}D}$ such that $a = Da' + a''$. Write $b = a'\xi$. Then we have

$$b \in \mathbb{G}_{N+S}^2,\ a'' \in \mathbb{G}_S \text{ and } \mathcal{R}b = a - a''.$$

It follows that $a \in \mathcal{R}\left(\mathbb{G}_{N+S}^2\right) + a''$. Thus, we see that

$$A \subseteq \bigcup_{m \in \mathbb{G}_S} \Big(\mathcal{R}\left(\mathbb{G}_{N+S}^2\right) + m\Big). \tag{7.4}$$

For $m \in \mathbb{G}_S$, write $A_m = A \bigcap \left(\mathcal{R}\left(\mathbb{G}_{N+S}^2\right) + m\right)$. For each $a \in A_m$, we fix a $\hat{a} \in \mathbb{G}_{N+S}^2$ such that $\mathcal{R}\hat{a} + m = a$. Since

$$\left\{\hat{a} + d(-c_{12}, c_{11}) : a \in A_m,\ d \in \mathbb{G}_N\right\} \subseteq B_m',$$

it follows that $|B_m'| \geq q^N |A_m|$. Take $\underline{m} \in \mathbb{G}_S$ such that $\left|B_{\underline{m}}'\right| = \max\limits_{m \in \mathbb{G}_S} \left|B_m'\right|$. By (7.4), we have

$$\left|B_{\underline{m}}'\right| \geq \frac{1}{q^S} \sum_{m \in \mathbb{G}_S} \left|B_m'\right| \geq q^{N-S} \sum_{m \in \mathbb{G}_S} \left|A_m\right| \geq q^{N-S} \Big|\bigcup_{m \in \mathbb{G}_S} A_m\Big| = q^{N-S}|A|.$$

This completes the proof of the claim.

Claim 5 Suppose that $l \geq 2$. For $m \in \mathbb{G}_{N+3S}^{l-1}$, write $B_m'' = \left\{b \in B_{\underline{m}}' : \mathcal{D}\mathcal{R}b + m \in A^{l-1}\right\}$. Then there exists $\underline{m'} \in \mathbb{G}_{N+3S}^{l-1}$ such that

$$\left|B_{\underline{m'}}''\right| \geq q^{-(l-2)N-(3l-2)S}|A|^l.$$

Proof The claim follows from the similar argument as in Claim 3.

Write

$$\overline{m} = \begin{cases} \underline{m}, & \text{if } l = 1, \\ (\underline{m}, \underline{m'}), & \text{if } l \geq 2. \end{cases}$$

Define $B = \left\{b \in \mathbb{G}_{N+S}^2 : \mathcal{P}b + \overline{m} \in A^l\right\}$. Then by Claims 4 and 5, we have

$$|B| \geq q^{-(l-2)N-(3l-2)S}|A|^l. \tag{7.5}$$

By using similar arguments as in Case 1, we obtain $|B| \leq Cq^{2(N+S)\frac{\log N}{N}}$. By taking $C' = C^{\frac{1}{l}} q^{3S}$, the theorem follows from (7.5).

Combining the above two cases, the proof of the theorem is completed.

References

[1] Furstenberg H. Ergodic behavier of diagonal measures and a theorem of Szemerédi on arithmetic progressions[J]. J. d'Analyse Math., 1977, 31: 204–256.

[2] Sárközy A. On difference sets of sequences of integers III[J]. Acta. Math. Hungar., 1978, 31: 355–386.

[3] Pintz J, Steiger W L, Szemerédi E. On sets of natural numbers whose difference set contains no squares[J]. J. London Math. Soc., 1988, 37: 219–231.

[4] Balog A, Pelikán J, Pintz J, Szemerédi E. Difference sets without κ-th powers[J]. Acta Math. Hung., 1994, 65: 165–187.

[5] Bergelson V, Leibman A. Polynomial extensions of van der Waerden's and Szemerédi's theorems[J]. J. Amer. Math. Soc., 1996, 9: 725–753.

[6] Lyall N, Magyar Á. Polynomials configurations in difference sets[J]. J. Number Theory, 2009, 129: 439–450.

[7] Lê T H, Liu Y R. On sets of polynomials whose difference set contains no squares[J]. Acta. Arith., 2013, 161: 127–143.

[8] Rice A J. Improvements and extensions of two theorems of Sárközy[D]. Georgia: University of Georgia, 2012.

[9] Vaughan R C. The Hardy-Littlewood method[M]. Cambridge: Cambridge University Press, 1997.

[10] Kubota R. Waring's problem for $\mathbb{F}_q[x]$[J]. Diss. Math., 1974, 117: 1–60.

[11] Chen J R. On Professor Hua's estimate of exponential sums[J]. Sci. Sinica., 1977, 20: 711–719.

[12] Weil A. On some exponential sums[J]. Proc. Nat. Acad. Sci. U.S.A., 1948, 34: 47–62.

函数域中Sárközy定理的2-维相似品

李国全,刘宝庆,钱 锟,许贵桥

(天津师范大学数学科学学院, 天津 300387)

摘要: $\mathbb{F}_q[t]$为含有q个元的有限域$\mathbb{F}_q$上的多项式环. 对$N\in\mathbb{N}$, 设$\mathbb{G}_N$为由$\mathbb{F}_q[t]$中一切次数严格小于N的多项式所形成的集合. 假定$\mathbb{F}_q$的特征严格大于2, 并且$A\subseteq\mathbb{G}_N^2$. 如果对任何$d\in\mathbb{F}_q[t]\setminus\{0\}$都有$(d,d^2)\notin A-A=\{a-a':a,a'\in A\}$. 本文证明了$|A|\leq Cq^{2N}\frac{\log N}{N}$, 此处常数$C$只依赖于$q$. 应用这个估计, 本文把函数域中的Sárközy定理推广到了次数严格小于3的多项式的有限族的情形.

关键词: Sárközy定理; 函数域; Hardy-Littlewood圆法

MR(2010)**主题分类号**: 11P55; 11T55 **中图分类号**: O156