ON SETS OF POLYNOMIALS WHOSE DIFFERENCE SET CONTAINS NO SQUARES

THÁI HOÀNG LÊ AND YU-RU LIU

Abstract. Let $\mathbb{F}_q[t]$ be the polynomial ring over the finite field $\mathbb{F}_q$, and let $\mathbb{G}_N$ be the subset of $\mathbb{F}_q[t]$ containing all polynomials of degree strictly less than N. Define $D(N)$ to be the maximal cardinality of a set $A \subseteq \mathbb{G}_N$ for which $A - A$ contains no squares of polynomials. By combining the polynomial Hardy-Littlewood circle method with the density increment technology developed by Pintz, Steiger and Szemerédi, we prove that $D(N) \ll q^N (\log N)^7/N$.

1. Introduction

In a series of papers, Sárközy [11, 12, 13] investigated the set of differences of a set of positive density in the integers. He proved the following theorem in [11], confirming a conjecture of Lovász:

Theorem 1. *If B is a subset of positive density of the integers, then there exist two distinct elements of B whose difference is a perfect square.*

For a set $H \subseteq \mathbb{N} = \{1, 2, \dots\}$ and $N \in \mathbb{N}$, we denote by $D(H, N)$ the maximal cardinality of a set $B \subseteq \{1, 2, \dots, N\}$ such that the difference set $B - B$ does not contain any element of H. Thus, if T is the set of non-zero squares, the above theorem says that $D(T, N) = o(N)$. Sárközy indeed gave an explicit upper bound for $D(T, N)$ by showing that

$$D(T, N) \ll N \frac{(\log \log N)^{2/3}}{(\log N)^{1/3}}.$$

At about the same time, by using ergodic theory, Furstenberg [2] independently proved that $D(T, N) = o(N)$, but his result is not quantitative. Recently, Green [3] and Lyall [8] provided greatly simplified proofs of Sárközy's theorem with weaker bounds. Even more recently, Green, Tao and Ziegler [14] gave yet another simple and elementary proof of Sárközy's theorem (though with weaker bounds). A sharper quantitative result was obtained by Pintz, Steiger and Szemerédi in [9], where they proved that

$$D(T, N) \ll N (\log N)^{-(1/12) \log \log \log \log N}.$$

Date: April 6, 2013.

2000 *Mathematics Subject Classification.* 11P55, 11T55.

Key words and phrases. Sáközy's theorem, function fields, circle method.

During the preparation of this paper, the first author was a member of the Institute for Advanced Study and visiting the University of Waterloo. He would like to thank the Institute for Advanced study for its support, and the University of Waterloo for its hospitality. The research of the second author is supported in part by an NSERC discovery grant.

This bound was later improved by Balog, Pelikán, Pintz and Szemerédi [1] with 1/12 being replaced by 1/4.

Various generalizations of Sárközy's theorem have been investigated. For example, Kamae and Mendès France [4] gave very general criteria for sets enjoying the same properties as the squares (known as *intersective sets*). For $l \in \mathbb{N}$ with $l \geq 2$, the aforementioned bound of Balog, Pelikán, Pintz and Szemerédi was valid with squares replaced by lth powers. Sárközy's [12] also estimated $D(H, N)$ with $H = \{p-1 : p \text{ prime}\}$. His theorem was later improved by Ruzsa and Sanders [10]. For more results on intersective sets, we refer the reader to the survey paper [6].

In [7], the first author and Spencer investigated a function field analog of Sárközy's theorem for shifted primes. Because of some improved exponential sum estimates, they obtained a result that is stronger than Ruzsa-Sander's bound. In this paper, we consider a function field analogue of Theorem 1. Let $\mathbb{F}_q[t]$ be the polynomial ring over the finite field $\mathbb{F}_q$, and let $\mathbb{G}_N$ be the subset of $\mathbb{F}_q[t]$ containing all polynomials of degree strictly less than N. We denote by $D(N)$ the maximal cardinality of a set $A \subseteq \mathbb{G}_N$ for which $A - A$ contains no squares of non-zero polynomials. Also, for $A \subseteq \mathbb{G}_N$, we denote by $|A|$ the cardinality of A. Define

$$U(A, N) = \sum_{\substack{f \in \mathbb{F}_q[t] \\ f \neq 0}} \left| \left\{ (a, a') \in A^2 \,|\, a - a' = f^2 \right\} \right|,$$

which represents the number of distinct pairs (a, a') in A^2 whose difference is a square. We first notice that if q is a power of 2, the map $f \mapsto f^2$ is linear. This observation allows us to provide simple estimates for $D(N)$ and $U(A, N)$ in this case. For a real number R, let $\lceil R \rceil$ be the smallest integer $\geq R$ and $\lfloor R \rfloor$ the largest integer $\leq R$.

Proposition 2. *Suppose that q is a power of 2.*
(1) *We have*

$$D(N) \leq q^{N/2}.$$

(2) *Let $A \subseteq \mathbb{G}_N$ with $|A| = \delta q^N$ and $\delta > q^{-N/2}$. We have*

$$U(A, N) \geq \delta^2 q^{\lceil 3N/2 \rceil} - \delta q^N.$$

Proof: For $a, a' \in \mathbb{G}_N$, we have $a - a' = f^2 \in \mathbb{G}_N$. We first notice that every square in $\mathbb{G}_N$ is of the form $x_0 + x_2 t^2 + \ldots + x_{2k} t^{2k}$, where $x_i \in \mathbb{F}_q$ and $k \leq \lfloor \frac{N-1}{2} \rfloor$. Let $M = \lfloor \frac{N}{2} \rfloor$. For every $x = (x_1, x_2, \ldots, x_M) \in \mathbb{F}_q^M$, the M-dimensional vector space over $\mathbb{F}_q$, let A_x be the set of all elements $a = a_0 + a_1 t + \ldots + a_{N-1} t^{N-1}$ in A such that $(a_1, a_3, \ldots, a_{2M-1}) = (x_1, x_2, \ldots, x_M)$.
(1) If

$$|A| > q^{N-M} \geq q^{N/2},$$

by the pigeonhole principle, there exists x such that A_x contains at least two distinct elements. Then the difference of these two elements is a non-zero square in $\mathbb{F}_q[t]$.
(2) Suppose that $A \subseteq \mathbb{G}_N$ with $|A| = \delta q^N$ and $\delta > q^{-N/2}$. From the above estimate, we

see that

$$U(A,N) \geq \sum_{x\in\mathbb{F}_q^M} |A_x|^2 - |A| \geq \frac{1}{q^M}|A|^2 - |A| = \delta^2 q^{\lceil 3N/2\rceil} - \delta q^N.$$

This completes the proof of the proposition.

Thus, throughout the rest of this paper, we assume that q is odd. By adapting part of the Pintz-Steiger-Szeméredi argument, we prove that

Theorem 3. *Suppose that q is not divisible by 2.*
(1) *There exists a constant C, depending only on q, such that*

$$D(N) \leq Cq^N \frac{(\log N)^7}{N}.$$

(2) *Let $A \subseteq \mathbb{G}_N$ with $|A| = \delta q^N$ and $\delta > C\frac{(\log N)^7}{N}$. There exists a constant C', depending only on q, such that*

$$U(A,N) \geq \delta^2 \exp\Big(- C'\frac{1}{\delta}(\log N)^7\Big) q^{3N/2}.$$

The paper is organized as follows. In Section 2, we will introduce basic notation and Fourier analysis in $\mathbb{F}_q[t]$. In Section 3, we will obtain some exponential sum estimates that are necessary for our arguments. Then we will prove Theorem 3 in Section 4. We remark here that since we will not implement the full strength of the Pintz-Steiger-Szemerédi argument in this paper, the above bound of $D(N)$ is not as strong as its integer analogue. However, our approach allows us to get a bound on $U(A,N)$, which is not possible using the method of Pintz-Steiger-Szemerédi. On the other hand, various arguments used to get the correct order of magnitude of $U(A,N)$, which is $q^{3N/2}$, give much weaker bounds for $D(N)$ than the one in Theorem 3. Thus, our bounds of $D(N)$ and $U(A,N)$ are something in between the two extremes. Also, although we work only with the squares, our approach can be easily extended to cover lth powers when $l < p$, the characteristic of $\mathbb{F}_q$, with a bound of the same strength. The cases when $l \geq p$ are more difficult. The main obstruction is that our approach involves the use of Weyl's differencing (see Lemma 9), which produces factors of $l!$ on certain exponential sums. Since these factors are zero when $l \geq p$, the standard application of the circle method is ineffective in providing non-trivial estimates. In our future paper, we intend to apply the recent work of the second author and Wooley on Vinogradov's mean value theorem in function fields to overcome the difficulty of small characteristics. We also plan to apply the approach of Pintz-Steiger-Szemerédi to obtain a bound of comparable strength to its integer analogue.

2. Preliminaries

We begin this section by introducing Fourier analysis for function fields. Let $\mathbb{K} = \mathbb{F}_q(t)$ be the field of fractions of $\mathbb{F}_q[t]$, and let $\mathbb{K}_\infty = \mathbb{F}_q((1/t))$ be the completion of $\mathbb{K}$ at ∞. Each element $\xi \in \mathbb{K}_\infty$ may be written in the form $\xi = \sum_{i\leq w} a_i(\xi)t^i$ for some $w \in \mathbb{Z}$ and $a_i(\xi) \in \mathbb{F}_q$ $(i \leq w)$. If $a_w(\xi) \neq 0$, we say that $\operatorname{ord}\xi = w$, and we write $\langle\xi\rangle$ for $q^{\operatorname{ord}\xi}$. We adopt the conventions that $\operatorname{ord} 0 = -\infty$ and $\langle 0\rangle = 0$. Also, we write $\{\xi\} = \sum_{i<0} a_i(\xi)t^i$ as the fractional part of ξ. It is often convenient to refer to $a_{-1}(\xi)$ as being the residue of ξ, denoted by $\operatorname{res}\xi$. For a real number R, we let $\widehat{R}$ denote q^R. Thus, for $x \in \mathbb{F}_q[t]$, we have $\langle x \rangle < \widehat{R}$ if and only if $\operatorname{ord} x < R$.

Let $\mathbb{T} = \{\xi \in \mathbb{K}_\infty \,|\, \operatorname{ord}\xi < 0\}$. Given any Haar measure $d\xi$ on $\mathbb{K}_\infty$, we normalize it in such a manner that $\int_{\mathbb{T}} 1 d\xi = 1$. We are now equipped to define the exponential function on $\mathbb{K}_\infty$. Suppose that the characteristic of $\mathbb{F}_q$ is p. Let $e(z)$ denote $e^{2\pi i z}$ and let $\operatorname{tr} : \mathbb{F}_q \to \mathbb{F}_p$ denote the familiar trace map. There is a non-trivial additive character $e_q : \mathbb{F}_q \to \mathbb{C}^\times$ defined for each $a \in \mathbb{F}_q$ by taking $e_q(a) = e(\operatorname{tr}(a)/p)$. This character induces a map $e : \mathbb{K}_\infty \to \mathbb{C}^\times$ by defining, for each element $\xi \in \mathbb{K}_\infty$, the value of $e(\xi)$ to be $e_q(\operatorname{res}\xi)$. For $\xi \in \mathbb{K}_\infty$, the exponential function satisfies the following orthogonal relation [5, Lemma 7]:

$$\sum_{\langle x \rangle < \widehat{N}} e(x\xi) = \begin{cases} \widehat{N}, & \text{if } \operatorname{ord}\{\xi\} < -N, \\ 0, & \text{if } \operatorname{ord}\{\xi\} \geq -N. \end{cases} \tag{1}$$

Let $\Phi : \mathbb{G}_N \to \mathbb{C}$. The *Fourier transform* $\widehat{\Phi} : \mathbb{T} \to \mathbb{C}$ *of* Φ is defined by

$$\widehat{\Phi}(\alpha) = \sum_{\langle x \rangle < \widehat{N}} \Phi(x) e(x\alpha).$$

If $\Phi, \Psi : \mathbb{G}_N \to \mathbb{C}$, then the *convolution* $\Phi * \Psi : \mathbb{G}_N \to \mathbb{C}$ *of* Φ *and* Ψ is defined by

$$\Phi * \Psi(x) = \sum_{\langle y \rangle < \widehat{N}} \Phi(y)\Psi(x-y).$$

Let $\gamma \in \mathbb{T}$ with $\operatorname{ord}\gamma = -N$. By (1), we have

$$\sum_{\langle x \rangle < \widehat{N}} \widehat{\Phi}(x\gamma)\overline{\widehat{\Psi}(x\gamma)} = \widehat{N} \sum_{\langle x \rangle < \widehat{N}} \Phi(x)\overline{\Psi(x)}, \tag{2}$$

where $\overline{\Psi(x)}$ is the complex conjugate of $\Psi(x)$. Then it follows that

$$\sum_{\langle x \rangle < \widehat{N}} |\widehat{\Phi}(x\gamma)|^2 = \widehat{N} \sum_{\langle x \rangle < \widehat{N}} |\Phi(x)|^2. \tag{3}$$

Also, for every $\alpha \in \mathbb{T}$, we have

$$\widehat{\Phi * \Psi}(\alpha) = \widehat{\Phi}(\alpha)\widehat{\Psi}(\alpha). \tag{4}$$

For a set $A \subseteq \mathbb{G}_N$, we denote by $A(x)$ the characteristic function of x. If $|A| = \delta\widehat{N}$, by (3), we have

$$\sum_{\langle x \rangle < \widehat{N}} |\widehat{A}(x\gamma)|^2 = \widehat{N}|A| = \delta\widehat{N}^2. \tag{5}$$

Finally, by (2), we have

$$\sum_{\langle x \rangle < \widehat{N}} A * A(-x)\Phi(x) = \frac{1}{\widehat{N}} \sum_{\langle x \rangle < \widehat{N}} |\widehat{A}(x\gamma)|^2 \widehat{\Phi}(x\gamma). \tag{6}$$

Notation For $r \in \mathbb{R}$, let $f(r)$ and $g(r)$ be functions of r. If $g(r)$ is positive and there exists a constant $C > 0$ such that $|f(r)| \leq Cg(r)$ for all r, we write $f(r) \ll g(r)$ or

$f(r) = O\big(g(r)\big)$. Throughout this paper, all implicit constants and constants denoted by C, C' or c_i depend at most on q.

3. Exponential sum estimates

For $\eta > 0$ and $a, g \in \mathbb{F}_q[t]$, define

$$\mathcal{M}_{a,g,\eta} = \big\{\alpha \in \mathbb{T} \,|\, \langle \alpha - a/g \rangle < \eta \big\}.$$

Let $R, M \in \mathbb{N}$ with $R < 2M/3$. We recall that for all $\alpha \in \mathbb{T}$, by Dirichlet's theorem in $\mathbb{F}_q[t]$ [5, Lemma 3], there exist $a, g \in \mathbb{F}_q[t]$ with g monic, $\langle a \rangle < \langle g \rangle$, $(a, g) = 1$, $\langle \alpha - a/g \rangle < \widehat{R} \langle g \rangle^{-1} \widehat{M}^{-2}$ and $\langle g \rangle \leq \widehat{M}^2 \widehat{R}^{-1}$. Let $\mathcal{M}_{a,g} = \mathcal{M}_{a,g,\widehat{R}\langle g \rangle^{-1}\widehat{M}^{-2}}$. Then we define the *major arcs* $\mathfrak{M}$ and the *minor arcs* $\mathfrak{m}$ as follows:

$$\mathfrak{M} = \bigcup_{\substack{\langle g \rangle \leq \widehat{R} \\ g \text{ monic} \\ \langle a \rangle < \langle g \rangle \\ (a,g)=1}} \mathcal{M}_{a,g} \qquad \text{and} \qquad \mathfrak{m} = \mathbb{T} \setminus \mathfrak{M}.$$

Also, we define

$$S_M(\alpha) = \sum_{\langle x \rangle < \widehat{M}} \langle x \rangle e(x^2 \alpha).$$

In this section, we will obtain some estimates of S_M on the major and minor arcs. Specific choices of M and R will be made in Section 4.

Lemma 4. *For $\alpha \in \mathcal{M}_{a,g} \subseteq \mathfrak{M}$, we have*

$$S_M(\alpha) = \frac{1}{\langle g \rangle} \sum_{\langle r \rangle < \langle g \rangle} e(r^2 a/g) S_M(\alpha - a/g) + O\big(\langle g \rangle^2\big).$$

Proof: Let $\beta = \alpha - a/g$. For $x \in \mathbb{F}_q[t]$, we write $x = yg + r$ with $y, r \in \mathbb{F}_q[t]$ and $\langle r \rangle < \langle g \rangle$. Since $\alpha \in \mathfrak{M}$, we have $\langle g \rangle \leq \widehat{R} < \widehat{M}$. Then

$$\begin{aligned} S_M(\alpha) &= \sum_{\langle x \rangle < \widehat{M}} \langle x \rangle e(x^2 a/g) e(x^2 \beta) \\ &= \sum_{\langle r \rangle < \langle g \rangle} \sum_{\langle y \rangle < \widehat{M} \langle g \rangle^{-1}} \langle yg + r \rangle e\big((yg+r)^2 a/g\big) e\big((yg+r)^2 \beta\big) \\ &= \sum_{\langle r \rangle < \langle g \rangle} e(r^2 a/g) \langle r \rangle e(r^2 \beta) + \sum_{\langle r \rangle < \langle g \rangle} e(r^2 a/g) \Bigg(\sum_{1 \leq \langle y \rangle < \widehat{M} \langle g \rangle^{-1}} \langle yg + r \rangle e\big((yg+r)^2 \beta\big) \Bigg). \end{aligned}$$

Notice that for $\langle y \rangle \geq 1$, we have $\langle yg + r \rangle = \langle yg \rangle$. Also, since $\widehat{R} < \widehat{M}^{2/3}$, we have

$$\big\langle (yg+r)^2 \beta - (yg)^2 \beta \big\rangle \leq \max\big\{\langle yg \rangle, \langle r^2 \rangle\big\} \langle \beta \rangle < \max\big\{\widehat{M} q^{-1}, \widehat{R}^2 q^{-2}\big\} \widehat{R} \langle g \rangle^{-1} \widehat{M}^{-2} \leq q^{-2}.$$

Thus, $e\big((yg+r)^2\beta\big) = e\big((yg)^2\beta\big)$. It follows that

$$\begin{aligned}\sum_{1\le\langle y\rangle<\widehat{M}\langle g\rangle^{-1}} \langle yg+r\rangle e\big((yg+r)^2\beta\big) &= \sum_{1\le\langle y\rangle\le\widehat{M}\langle g\rangle^{-1}} \langle yg\rangle e\big((yg)^2\beta\big)\\ &= \frac{1}{\langle g\rangle}\sum_{\langle r\rangle<\langle g\rangle}\sum_{1\le\langle y\rangle\le\widehat{M}\langle g\rangle^{-1}} \langle yg+r\rangle e\big((yg+r)^2\beta\big)\\ &= \frac{1}{\langle g\rangle}\sum_{\langle r\rangle<\langle g\rangle}\sum_{\langle y\rangle\le\widehat{M}\langle g\rangle^{-1}} \langle yg+r\rangle e\big((yg+r)^2\beta\big) + O\big(\langle g\rangle\big)\\ &= \frac{1}{\langle g\rangle} S_M(\beta) + O\big(\langle g\rangle\big).\end{aligned}$$

Combining the above two equalities, we have

$$S_M(\alpha) = O\big(\langle g\rangle^2\big) + \sum_{\langle r\rangle<\langle g\rangle} e(r^2a/g)\left(\frac{1}{\langle g\rangle}S_M(\beta) + O\big(\langle g\rangle\big)\right) = \frac{1}{\langle g\rangle}\sum_{\langle r\rangle<\langle g\rangle} e(r^2a/g)S_M(\beta) + O\big(\langle g\rangle^2\big).$$

This completes the proof of the lemma.

Lemma 5. *(major arcs estimate) For $\alpha\in\mathcal{M}_{a,g}\subseteq\mathfrak{M}$, we have*

$$S_M(\alpha) \ll \widehat{M}^2\langle g\rangle^{-1/2}.$$

Proof: Since $\sum_{\langle r\rangle<\langle g\rangle} e\big(r^2a/g\big) \ll \langle g\rangle^{1/2}$ [5, Lemma 22] and $S_M(\alpha - a/g) \ll \widehat{M}^2$, by Lemma 4, we have

$$S_M(\alpha) \ll \langle g\rangle^{-1}\langle g\rangle^{1/2}\widehat{M}^2 + \langle g\rangle^2 \ll \widehat{M}^2\langle g\rangle^{-1/2}.$$

The last inequality follows since $\langle g\rangle^{5/2} \le \widehat{R}^{5/2} < \widehat{M}^2$.

Lemma 6. *For $\alpha\in\mathcal{M}_{a,g}\subseteq\mathfrak{m}$, we have*

$$S_M(\alpha) = S_M(a/g).$$

Proof: Write $\alpha = a/g+\beta$. Then

$$S_M(\alpha) = S_M(a/g+\beta) = \sum_{\langle x\rangle<\widehat{M}} \langle x\rangle e(x^2a/g)e(x^2\beta).$$

Notice that for $\alpha\in\mathfrak{m}$, we have $\langle g\rangle > \widehat{R}$. Then

$$\langle x^2\beta\rangle < \widehat{M}^2q^{-2}\widehat{R}\langle g\rangle^{-1}\widehat{M}^{-2} < q^{-2}.$$

Thus, $e(x^2\beta) = 1$, and the lemma follows.

Lemma 7. *For $\widehat{M} < \langle g\rangle$, we have*

$$\sum_{\langle x\rangle<\widehat{M}} e(x^2a/g) \ll \langle g\rangle^{1/2}(\operatorname{ord} g)^{1/2}.$$

Proof: We have

$$\Big|\sum_{\langle x\rangle<\widehat{M}} e(x^2a/g)\Big|^2 = \sum_{\langle x\rangle<\widehat{M}}\sum_{\langle y\rangle<\widehat{M}} e\big((x+y)(x-y)a/g\big) \le \sum_{\langle u\rangle<\widehat{M}}\Big|\sum_{\langle v\rangle<\widehat{M}} e(uva/g)\Big|.$$

Since $(a,g)=1$ and $\widehat{M}<\langle g\rangle$, by (1), it follows that

$$\begin{aligned}\Big|\sum_{\langle x\rangle<\widehat{M}} e(x^2a/g)\Big|^2 &\ll \widehat{M} + \sum_{1\le\langle u\rangle<\langle g\rangle}\big\langle\{ua/g\}\big\rangle^{-1}\\ &= \widehat{M} + \sum_{1\le\langle z\rangle<\langle g\rangle}\big\langle z/g\big\rangle^{-1}\\ &\ll \langle g\rangle + \sum_{W=0}^{\operatorname{ord} g-1}\widehat{W}\langle g\rangle\widehat{W}^{-1}\\ &\ll \langle g\rangle \operatorname{ord} g.\end{aligned}$$

This completes the proof of the lemma.

Lemma 8. *(minor arcs estimate) For $\alpha\in\mathcal{M}_{a,g}\subseteq\mathfrak{m}$, we have*

$$S_M(\alpha)\ll \widehat{M}^2M^{1/2}\widehat{R}^{-1/2}.$$

Proof: By Lemma 6, we have $S_M(\alpha)=S_M(a/g)$. There are two cases:
(1) If $\langle g\rangle>\widehat{M}$, by Abel's inequality and Lemma 7, we have

$$S_M(a/g)=\sum_{\langle x\rangle<\widehat{M}}\langle x\rangle e(x^2a/g)\le \max_{\langle x\rangle<\widehat{M}}\langle x\rangle\max_{J\le M}\Big|\sum_{\langle x\rangle<\widehat{J}} e(x^2a/g)\Big| \ll \widehat{M}\langle g\rangle^{1/2}(\operatorname{ord} g)^{1/2}.$$

Since $\langle g\rangle<\widehat{M}^2\widehat{R}^{-1}$, it follows that

$$S_M(a/g)\ll \widehat{M}^2M^{1/2}\widehat{R}^{-1/2}.$$

(2) Suppose that $\langle g\rangle\le\widehat{M}$. For $x\in\mathbb{F}_q[t]$, we write $x=yg+r$ with $y,r\in\mathbb{F}_q[t]$ and $\langle r\rangle<\langle g\rangle$. Thus,

$$S_M(a/g)=\sum_{\langle r\rangle<\langle g\rangle}\sum_{\langle y\rangle<\widehat{M}\langle g\rangle^{-1}}\langle yg+r\rangle e\big((yg+r)^2a/g\big) = \sum_{\langle r\rangle<\langle g\rangle} e(r^2a/g)\sum_{\langle y\rangle<\widehat{M}\langle g\rangle^{-1}}\langle yg+r\rangle.$$

Since $\sum_{\langle r\rangle<\langle g\rangle} e(r^2a/g)\ll\langle g\rangle^{1/2}$ [5, Lemma 22] and $\langle g\rangle>\widehat{R}$, it follows that

$$S_M(a/g)\ll\langle g\rangle^{1/2}\widehat{M}^2\langle g\rangle^{-1}\ll\widehat{M}^2\widehat{R}^{-1/2}.$$

Combining the above two cases, the lemma follows.

Lemma 9. *For $N\in\mathbb{N}$ and $\alpha\in\mathbb{T}$ with $-N\le\operatorname{ord}\alpha<-2M+2$, we have*

$$\sum_{\langle x\rangle<\widehat{N}}|S_M(x\alpha)|^6\ll\widehat{N}\widehat{M}^{10}.$$

Proof: By [5, Proposition 13], for any $\epsilon > 0$, we have
$$\int_{\mathbb{T}} \Big| \sum_{\langle y \rangle < \widehat{M}} e(y^2\alpha)\Big|^4 d\alpha \ll \widehat{M}^{2+\epsilon}.$$
Then using the argument in [15, Theorem 3], we can derive from the above bound that
$$\int_{\mathbb{T}} \Big| \sum_{\langle y \rangle < \widehat{M}} e(y^2\alpha)\Big|^6 d\alpha \ll \widehat{M}^{4}.$$
By [5, Lemma 1], we have
$$\int_{\mathbb{T}} \Big| \sum_{\langle y \rangle < \widehat{M}} e(y^2\alpha)\Big|^6 d\alpha = \#\big\{(y_1,y_2,y_3,z_1,z_2,z_3) \in {\mathbb{G}_M}^6 \,|\, y_1^2+y_2^2+y_3^2 = z_1^2+z_2^2+z_3^2\big\}.$$
Thus, combining the above estimates with (1), it follows that
$$\begin{aligned}
&\sum_{\langle x \rangle < \widehat{N}} \big|S_M(x\alpha)\big|^6 \\
&= \sum_{\langle x \rangle < \widehat{N}} \sum_{\langle y_1\rangle,\langle y_2\rangle,\langle y_3\rangle,\langle z_1\rangle,\langle z_2\rangle,\langle z_3\rangle < \widehat{M}} \langle y_1\rangle\langle y_2\rangle\langle y_3\rangle\langle z_1\rangle\langle z_2\rangle\langle z_3\rangle e\big((y_1^2+y_2^2+y_3^2-z_1^2-z_2^2-z_3^2)x\alpha\big) \\
&= \widehat{N} \sum_{\substack{\langle y_1\rangle,\langle y_2\rangle,\langle y_3\rangle,\langle z_1\rangle,\langle z_2\rangle,\langle z_3\rangle < \widehat{M} \\ y_1^2+y_2^2+y_3^2 = z_1^2+z_2^2+z_3^2}} \langle y_1\rangle\langle y_2\rangle\langle y_3\rangle\langle z_1\rangle\langle z_2\rangle\langle z_3\rangle \\
&\ll \widehat{N}\widehat{M}^6 \#\big\{(y_1,y_2,y_3,z_1,z_2,z_3) \in {\mathbb{G}_M}^6 \,|\, y_1^2+y_2^2+y_3^2 = z_1^2+z_2^2+z_3^2\big\} \\
&\ll \widehat{N}\widehat{M}^{10}.
\end{aligned}$$
This completes the proof of the lemma.

For $f \in \mathbb{F}_q[t]$, $a \in \mathbb{F}_q$ and $\alpha \in \mathbb{T}$, define
$$R_{f,a}(\alpha) = \big\{x \in \mathbb{F}_q[t] \,|\, \langle x^2\alpha - f - at^{-1}\rangle \le q^{-2}\big\}.$$
The following lemma says that, in a sense, $x^2\alpha$ is uniformly distributed in $\mathbb{T}$.

Lemma 10. *Let $\alpha \in \mathbb{T}$, $a \in \mathbb{F}_q$ and $f \in \mathbb{F}_q[t]$ with $f \neq 0$.*
(1) For $x \in R_{f,a}(\alpha)$ and $b \in \mathbb{F}_q$ with $a \neq b$, there exist unique $c \in \mathbb{F}_q$ and $l \in \mathbb{N} \cup \{0\}$ such that $x + ct^l \in R_{f,b}(\alpha)$.
(2) For any $b \in \mathbb{F}_q$, we have $|R_{f,b}(\alpha)| = |R_{f,a}(\alpha)|$.

Proof: (1) For $x \in R_{f,a}(\alpha)$, we have
$$\begin{aligned}
x + ct^l \in R_{f,b} \quad &\iff \quad \big\langle (x+ct^l)^2\alpha - f - bt^{-1}\big\rangle \le q^{-2} \\
&\iff \quad \big\langle \big((x+ct^l)^2 - x^2\big)\alpha - (b-a)t^{-1}\big\rangle \le q^{-2} \\
&\iff \quad \big\langle ct^l(2x+ct^l)\alpha - (b-a)t^{-1}\big\rangle \le q^{-2}.
\end{aligned}$$
Since $\langle x^2\alpha - f\rangle \le q^{-1}$, $\big\langle (x+ct^l)^2\alpha - f\big\rangle \le q^{-1}$ and $f \neq 0$, we have $\operatorname{ord} x > \operatorname{ord}(ct^l)$. Since $a \neq b$, by comparing the orders, we have
$$l + \operatorname{ord} x + \operatorname{ord} \alpha = -1 \quad \iff \quad l = -\operatorname{ord} \alpha - 1 - \operatorname{ord} x. \tag{7}$$

Thus, l is uniquely determined. Moreover, we see that the leading coefficient of $2cxt^l\alpha$ is equal to $b-a$. Thus, c is uniquely determined.
(2) Consider $\psi_{a,b} : R_{f,a}(\alpha) \longrightarrow R_{f,b}(\alpha)$ defined by $\psi_{a,b}(x) = x + ct^l$, where c, l are defined as in Part (1). Suppose that $x_1, x_1 \in R_{f,a}(\alpha)$ with $x_1 + c_1t^{l_1} = x_2 + c_2t^{l_2}$. Since $\langle x_1^2\alpha\rangle = \langle f\rangle = \langle x_2^2\alpha\rangle$, we have $\langle x_1\rangle = \langle x_2\rangle$. Then by (7), we have

$$l_1 = -\operatorname{ord}\alpha - 1 - \operatorname{ord} x_1 = -\operatorname{ord}\alpha - 1 - \operatorname{ord} x_2 = l_2;$$

from which it follows that $x_1 = x_2$. Thus, $\psi_{a,b}$ is injective. Similarly, we can prove that $\psi_{b,a} : R_{f,b}(\alpha) \longrightarrow R_{f,a}(\alpha)$ is also injective. It follows that $|R_{f,b}(\alpha)| = |R_{f,a}(\alpha)|$.

Lemma 11. *For $\alpha \in \mathbb{T}$, we have*

$$|S_M(\alpha)| \le \langle\alpha\rangle^{-1}.$$

Proof: We first notice that if $\langle\alpha\rangle \le \widehat{M}^{-2}$, then

$$|S_M(\alpha)| \le \widehat{M}^2 \le \langle\alpha\rangle^{-1}.$$

Thus, in the rest of the proof, we can assume that $\langle\alpha\rangle > \widehat{M}^{-2}$. Let $f \in \mathbb{F}_q[t]$, $a \in \mathbb{F}_q$ and $x \in R_{f,a}(\alpha)$. We have

$$e(x^2\alpha) = e(f + at^{-1}) = e_q(a).$$

Notice that $f = 0$ if and only if $\langle x^2\alpha\rangle < 1$. Then it follows that $\langle x\rangle < \langle\alpha\rangle^{-1/2}$. If $f \ne 0$, then $\langle x^2\alpha\rangle = \langle f\rangle$. Thus, $\langle x\rangle$ is independent of a. We have

$$\begin{aligned}
|S_M(\alpha)| &= \Big|\sum_{\langle x\rangle < \widehat{M}} \langle x\rangle e(x^2\alpha)\Big| \\
&\le \Big|\sum_{\langle x^2\alpha\rangle < 1} \langle x\rangle e(x^2\alpha)\Big| + \Big|\sum_{1 \le \langle f\rangle \le \widehat{M}^2 q^{-2}\langle\alpha\rangle^{-1}} \sum_{a \in \mathbb{F}_q} \sum_{x \in R_{f,a}(\alpha)} \langle x\rangle e(x^2\alpha)\Big| \\
&\le \langle\alpha\rangle^{-1/2} \sum_{\langle x^2\alpha\rangle < 1} 1 + \Big|\sum_{1 \le \langle f\rangle \le \widehat{M}^2 q^{-2}\langle\alpha\rangle^{-1}} \big(\langle f\rangle\langle\alpha\rangle^{-1}\big)^{1/2} \sum_{a \in \mathbb{F}_q} e_q(a) \sum_{x \in R_{f,a}(\alpha)} 1\Big| \\
&= \langle\alpha\rangle^{-1} + \Big|\sum_{1 \le \langle f\rangle \le \widehat{M}^2 q^{-2}\langle\alpha\rangle^{-1}} \langle f\rangle^{1/2}\langle\alpha\rangle^{-1/2} \sum_{a \in \mathbb{F}_q} e_q(a)|R_{f,a}(\alpha)|\Big|.
\end{aligned}$$

By Lemma 10 part (2), the above inner sum is 0. This completes the proof of the lemma.

4. Proof of Theorem 3

For $N \in \mathbb{N}$ and $A \subseteq \mathbb{G}_N$, we define

$$W(A, N) = \sum_{f \in \mathbb{F}_q[t]} \langle f\rangle \big|\{(a, a') \in A^2 \mid a - a' = f^2\}\big|,$$

which counts the number of pairs (a, a') in A^2 whose difference is f^2 with weight $\langle f\rangle$. In this section, we will prove the following theorem.

Theorem 12. *There exist constants $C, C' > 0$, depending only on q, such that whenever $A \subseteq \mathbb{G}_N$ with $|A| = \delta \widehat{N}$ and $\delta > C\frac{(\log N)^7}{N}$, we have*

$$W(A,N) \geq \delta^2 \exp\Big(-C'\frac{1}{\delta}(\log N)^7\Big)\widehat{N}^2.$$

We notice that since $W(A,N) > 0$ and $W(A,N) \leq \widehat{N}^{1/2}U(A,N)$, Theorem 3 is a direct consequence of the above theorem.

Let $\gamma \in \mathbb{T}$ with $\operatorname{ord}\gamma = -N$. For $\eta > 0$ and $g \in \mathbb{F}_q[t]$, let

$$\mathcal{M}_{g,\eta} = \bigcup_{\substack{\langle a\rangle < \langle g\rangle \\ (a,g)=1}} \mathcal{M}_{a,g,\eta},$$

where $\mathcal{M}_{a,g,\eta}$ is defined as in Section 3. We also define

$$F(g,\eta) = \frac{1}{|A|\widehat{N}} \sum_{\substack{\langle x\rangle < \widehat{N} \\ x\gamma \in \mathcal{M}_{g,\eta}}} |\widehat{A}(x\gamma)|^2.$$

The following lemma is about the density increment.

Lemma 13. *Let $A \subseteq \mathbb{G}_N$ with $|A| = \delta\widehat{N}$. Let $\eta > 0$ and $g \in \mathbb{F}_q[t]$. Suppose that $N' = -\log_q \eta - 2\operatorname{ord} g > 0$. Then we can find a set $A' \subseteq \mathbb{G}_{N'}$ with $|A'| = \delta'\widehat{N'}$ such that*

1. $\delta' \geq \delta + F(g,\eta)$,
2. $W(A,N) \geq \langle g\rangle^2 W(A',N')$.

Proof: Let $G = g^2\mathbb{G}'_N$. By (3) and (4), we have

$$\sum_{\langle x\rangle < \widehat{N}} |A \cap (G+x)|^2 = \sum_{\langle x\rangle < \widehat{N}} |A * G(x)|^2 = \frac{1}{\widehat{N}} \sum_{\langle x\rangle < \widehat{N}} |\widehat{A * G}(x\gamma)|^2 = \frac{1}{\widehat{N}} \sum_{\langle x\rangle < \widehat{N}} |\widehat{A}(x\gamma)|^2 |\widehat{G}(x\gamma)|^2.$$

For $x\gamma \in \mathcal{M}_{a,g,\eta}$ and $y \in \mathbb{G}_{N'}$, we have

$$\big\langle g^2yx\gamma - gya\big\rangle < \big\langle g^2 y\big\rangle \eta \leq q^{-1}.$$

It follows that

$$\widehat{G}(x\gamma) = \sum_{\langle y\rangle < \widehat{N'}} e(g^2yx\gamma) = \widehat{N'}.$$

Thus, by the definition of $F(g,\eta)$, we have

$$\frac{1}{\widehat{N}} \sum_{\substack{\langle x\rangle < \widehat{N} \\ x\gamma \in \mathcal{M}_{g,\eta}}} |\widehat{A}(x\gamma)|^2 |\widehat{G}(x\gamma)|^2 \geq \delta F(g,\eta)\widehat{N}\widehat{N'}^2.$$

Also, if $x = 0$, we have

$$\frac{1}{\widehat{N}}|\widehat{A}(0)|^2|\widehat{G}(0)|^2 = \delta^2\widehat{N}\widehat{N'}^2.$$

We notice that $0 \notin \mathcal{M}_{g,\eta}$ as $N' > 0$. Combining the above estimates, we have

$$\sum_{\langle x\rangle<\widehat{N}} |A\cap(G+x)|^2 \geq \frac{1}{\widehat{N}} \sum_{\substack{\langle x\rangle<\widehat{N} \\ x\gamma\in\{0\}\cup\mathcal{M}_{g,\eta}}} |\widehat{A}(x\gamma)|^2|\widehat{G}(x\gamma)|^2 \geq \big(\delta^2+\delta F(g,\eta)\big)\widehat{N}\widehat{N'}^2.$$

We also notice that

$$\sum_{\langle x\rangle<\widehat{N}} |A\cap(G+x)| = |A||G| = \delta\widehat{N}\widehat{N'}.$$

Thus, there exists $x' \in \mathbb{G}_N$ such that $|A\cap(G+x')| \geq \big(\delta+F(g,\eta)\big)\widehat{N'}$. Let $A' = \big\{y \in \mathbb{G}_{N'} : g^2y+x' \in A\big\}$, then the set A' satisfies both conditions of the lemma.

Proposition 14. *There exist constants $c_i > 0$ $(0 \leq i \leq 3)$ such that the following hold: let $N \geq c_0$, and let a set $A \subseteq \mathbb{G}_N$ with $|A| = \delta\widehat{N}$ and $\delta \geq N^{-1}$. Suppose that $W(A,N) \leq c_1\delta^2\widehat{N}^2$. Then there exist N' and a set $A' \subseteq \mathbb{G}_N$ with $|A| = \delta'\widehat{N'}$ such that*

(1) $N' \geq N - c_2\log N$,
(2) $\delta' \geq \delta + c_3\delta^2(\log N)^{-6}$,
(3) $W(A',N') \leq W(A,N)$.

Proof: Let $\Phi : \mathbb{F}_q[t] \to \mathbb{C}$ be defined by

$$\Phi(x) = \begin{cases} \langle f\rangle, & \text{if } x = f^2 \in \mathbb{G}_N, \\ 0, & \text{otherwise.} \end{cases}$$

By (6), we have

$$W(A,N) = \sum_{\langle x\rangle<\widehat{N}} A*A(-x)\Phi(x) = \frac{1}{\widehat{N}}\sum_{\langle x\rangle<\widehat{N}} |\widehat{A}(x\gamma)|^2\widehat{\Phi}(x\gamma).$$

Also, we notice that $\widehat{\Phi}(\theta) = S_M(\theta)$, where $M = \lfloor\frac{N+1}{2}\rfloor$. Let $R = \lfloor c_4\log N\rfloor$ and $K = \lfloor c_5\log N\rfloor$, where c_4, c_5 are large constants. Since $W(A,N) \leq c_1\delta^2\widehat{N}^2$ and $|\widehat{A}(0)|^2\widehat{\Phi}(0) \gg \delta^2\widehat{N}^3$, for c_1 sufficiently small, we have

$$\sum_{\substack{\langle x\rangle<\widehat{N} \\ x\neq 0}} |\widehat{A}(x\gamma)|^2|S_M(x\gamma)| \gg \delta^2\widehat{N}^3. \tag{8}$$

Let $\mathcal{M}_{a,g}$, $\mathfrak{M}$ and $\mathfrak{m}$ be defined as in Section 3. We now divide the sum in (8) into various cases. Consider those x with $x\gamma \in \mathfrak{m}$. By Lemma 8 and (5), for N and c_4 sufficiently large, we have

$$\sum_{\substack{\langle x\rangle<\widehat{N} \\ x\gamma\in\mathfrak{m}}} |\widehat{A}(x\gamma)|^2 S_M(x\gamma) \leq \max_{x\gamma\in\mathfrak{m}} |S_M(x\gamma)| \sum_{\langle x\rangle<\widehat{N}} |\widehat{A}(x\gamma)|^2 \ll \widehat{M}^2 M\widehat{R}^{-1/2}\delta\widehat{N}^2 \ll \delta^2\widehat{N}^3. \tag{9}$$

Consider those x with $\widehat{A}(x\gamma) \le |A|\widehat{K}^{-1}$. By Hölder's inequality, (5) and Lemma 9, for N and c_5 sufficiently large, we have

$$\begin{aligned}
&\sum_{\substack{\langle x\rangle<\widehat{N} \\ \widehat{A}(x\gamma)\le|A|\widehat{K}^{-1}}} |\widehat{A}(x\gamma)|^2 S_M(x\gamma) \\
\le\ & \max_{\substack{\langle x\rangle<\widehat{N} \\ \widehat{A}(x\gamma)\le|A|\widehat{K}^{-1}}} |\widehat{A}(x\gamma)|^{1/3} \Big(\sum_{\langle x\rangle<\widehat{N}} |\widehat{A}(x\gamma)|^2 \Big)^{5/6} \Big(\sum_{\langle x\rangle<\widehat{N}} |S_M(x\gamma)|^6 \Big)^{1/6} \\
\le\ & (\delta \widehat{N}\widehat{K}^{-1})^{1/3} (\delta \widehat{N}^2)^{5/6} (\widehat{N}\widehat{M}^{10})^{1/6} \\
\ll\ & \delta^2 \widehat{N}^3. \qquad (10)
\end{aligned}$$

Thus, it remains to consider those x with $x \ne 0$, $x\gamma \in \mathfrak{M}$ and $\widehat{A}(x\gamma) > |A|\widehat{K}^{-1}$. Let

$$\mathcal{M}(a,g) = \big\{ x \in \mathbb{G}_N \,|\, x\gamma \in \mathcal{M}_{a,g} \text{ and } \widehat{A}(x\gamma) > |A|\widehat{K}^{-1} \big\}.$$

By (8), (9) and (10), we have

$$\begin{aligned}
\delta^2 \widehat{N}^3 &\ll \sum_{\substack{1\le\langle g\rangle\le\widehat{R} \\ g \text{ monic} \\ \langle a\rangle<\langle g\rangle \\ (a,g)=1}} \sum_{x\in\mathcal{M}(a,g)} |\widehat{A}(x\gamma)|^2 |S_M(x\gamma)| \\
&\le \sum_{\substack{1\le\langle g\rangle\le\widehat{R} \\ g \text{ monic} \\ \langle a\rangle<\langle g\rangle \\ (a,g)=1}} \max_{x\in\mathcal{M}(a,g)} |\widehat{A}(x\gamma)|^2 \sum_{x\in\mathcal{M}(a,g)} |S_M(x\gamma)|. \qquad (11)
\end{aligned}$$

For $x \in \mathcal{M}(a,g)$, since $\sum_{\langle r\rangle<\langle g\rangle} e\big(r^2 a/g\big) \ll \langle g\rangle^{1/2}$ [5, Lemma 22], by Lemmas 4 and 11, we have

$$S_M(x\gamma) \ \ll\ \langle g\rangle^{-1/2} \big| S_M(x\gamma - a/g) \big| + \langle g\rangle^2 \le \langle g\rangle^{-1/2} \langle x\gamma - a/g\rangle^{-1} + \langle g\rangle^2.$$

Also, by (5), we have

$$|\mathcal{M}(a,g)| \big(|A|\widehat{K}^{-1} \big)^2 \le \sum_{x\in\mathcal{M}(a,g)} |\widehat{A}(x\gamma)|^2 \le \sum_{\langle x\rangle<\widehat{N}} |\widehat{A}(x\gamma)|^2 = \delta \widehat{N}^2.$$

Thus, for c_5 sufficiently large, it follows that

$$|\mathcal{M}(a,g)| \le \delta^{-1}\widehat{K}^2 \le \widehat{K}^3. \qquad (12)$$

Let $T \in \mathbb{N}$ with $\widehat{T-1} \le \widehat{K}^3 < \widehat{T}$. Then for a fixed $\xi \in \mathbb{K}_\infty$ and distinct $f_i \in \mathbb{F}_q[t]$ $(1 \le i \le \widehat{K}^3)$, we have

$$\sum_{i=1}^{\widehat{K}^3} \frac{1}{\langle f_i - \xi\rangle} \le O(1) + \sum_{W=0}^{T} \frac{\widehat{W+1}}{\widehat{W}} \ll T \ll K.$$

Also, since $\operatorname{ord}\gamma = -N$, we have $\langle x\gamma - a/g\rangle = \widehat{N}\langle x - a/(g\gamma)\rangle^{-1}$. Thus, it follows that

$$\sum_{x\in\mathcal{M}(a,g)} |S_M(x\gamma)| \ll \sum_{x\in\mathcal{M}(a,g)} \big(\langle g\rangle^{-1/2} \widehat{N} \langle x - a/(g\gamma)\rangle^{-1} + \langle g\rangle^2 \big) \ll \langle g\rangle^{-1/2}\widehat{N}K + \langle g\rangle^2 \widehat{K}^3 \ll \langle g\rangle^{-1/2}\widehat{N}K.$$

Substituting this into (11), we have

$$\delta^2 \widehat{N}^2 \ll \sum_{\substack{1 \le \langle g \rangle \le \widehat{R} \\ (a,g)=1 \\ g \text{ monic}}} \max_{x \in \mathcal{M}(a,g)} \left| \widehat{A}(x\gamma) \right|^2 \langle g \rangle^{-1/2} K.$$

For $1 \le r \le R$ and $1 \le k \le K$, let $\mathcal{L}_{r,k}$ be the set defined by

$$\mathcal{L}_{r,k} = \left\{ a/g \,|\, \langle g \rangle = \widehat{r}, g \text{ monic}, \langle a \rangle < \langle g \rangle, (a,g) = 1 \text{ and } |A|\widehat{k}^{-1} < \max_{x \in \mathcal{M}(a,g)} |\widehat{A}(x\gamma)| \le |A|\widehat{k-1}^{-1} \right\}.$$

Then it follows from the above inequality that

$$\delta^2 \widehat{N}^2 \ll \sum_{\substack{1 \le r \le R \\ 1 \le k \le K}} |\mathcal{L}_{r,k}||A|^2 \widehat{k}^{-2} \widehat{r}^{-1/2} K,$$

which implies that

$$1 \ll \sum_{\substack{1 \le r \le R \\ 1 \le k \le K}} |\mathcal{L}_{r,k}| \widehat{k}^{-2} \widehat{r}^{-1/2} K.$$

Thus, there exist some r and k such that

$$|\mathcal{L}_{r,k}| \ge \widehat{k}^2 \widehat{r}^{1/2} K^{-2} R. \tag{13}$$

We now aim to obtain an upper bound for $|\mathcal{L}_{r,k}|$. For a fixed $g \in \mathbb{F}_q[t]$, by the definition of $F(g, \eta)$, we have

$$F(g, \widehat{R}\langle g \rangle^{-1} \widehat{M}^{-2}) = \frac{1}{|A|\widehat{N}} \sum_{\substack{\langle x \rangle < \widehat{N} \\ x\gamma \in \mathcal{M}_{g, \widehat{R}\langle g \rangle^{-1} \widehat{M}^{-2}}}} |\widehat{A}(x\gamma)|^2 \ge \frac{1}{|A|\widehat{N}} \sum_{\substack{\langle a \rangle < \langle g \rangle \\ (a,g)=1 \\ a/g \in \mathcal{L}_{r,k}}} |A|^2 \widehat{k}^{-2}.$$

Summing over all $g \in \mathbb{F}_q[t]$ with g monic and $\langle g \rangle = \widehat{r}$, we have

$$\widehat{r} \max_{\langle g \rangle = \widehat{r}} F(g, \widehat{R}\langle g \rangle^{-1} \widehat{M}^{-2}) \ge \frac{1}{|A|\widehat{N}} |\mathcal{L}_{r,k}||A|^2 \widehat{k}^{-2},$$

which implies that

$$|\mathcal{L}_{r,k}| \le \delta^{-1} \widehat{k}^2 \widehat{r} \max_{\langle g \rangle = \widehat{r}} F(g, \widehat{R}\langle g \rangle^{-1} \widehat{M}^{-2}).$$

Also, by using the same argument as in (12), we have

$$|\mathcal{L}_{r,k}| \ll \delta^{-1} \widehat{k}^2.$$

Combining the above two inequalities, we have

$$|\mathcal{L}_{r,k}| \ll \delta^{-1} \widehat{k}^2 \widehat{r}^{1/2} \max_{\langle g \rangle = \widehat{r}} F(g, \widehat{R}\langle g \rangle^{-1} \widehat{M}^{-2})^{1/2}.$$

Combining this with (13), we see that there exists g with $\langle g \rangle \le \widehat{R}$ such that

$$F(g, \widehat{R}\langle g \rangle^{-1} \widehat{M}^{-2}) \gg \delta^2 K^{-4} R^{-2}.$$

Then by Lemma 13, we see that there exist $N' \in \mathbb{N}$ and a set $A' \subseteq \mathbb{G}_{N'}$ with $|A'| = \delta' \widehat{N'}$ such that

(1) $N' = -\log_q(\widehat{R}\langle g\rangle^{-1}\widehat{M}^{-2}) - 2\mathrm{ord}\, g \geq N - 2R \geq N - 2c_4 \log N$,
(2) $\delta' \geq \delta + F(g, \widehat{R}\langle g\rangle^{-1}\widehat{M}^{-2}) \geq \delta + c_4^2 c_5^4 \delta^2 (\log N)^{-6}$,
(3) $W(A', N') \leq \langle g\rangle^2 W(A', N') \leq W(A, N)$.

This completes the proof of the proposition.

Now, we are ready to prove Theorem 12.
Proof of Theorem 12: Suppose that we have a set $A \subseteq \mathbb{G}_N$ with $|A| = \delta\widehat{N}$, $\delta \geq 2N^{-1}$ and $W(A,N) < \delta^2 \exp\big(-c_6 \frac{1}{\delta}(\log N)^7\big)\widehat{N}^2$, where c_6 is a large constant. By applying Proposition 14 repeatedly, we can construct a sequence of triples $(N_i, A_i, \delta_i)_{i\geq 0}$ such that $N_i \in \mathbb{N}$ and $A_i \subseteq \mathbb{G}_{N_i}$ with $|A_i| = \delta_i \widehat{N_i}$ which satisfy

(1) $(N_0, A_0, \delta_0) = (N, A, \delta)$,
(2) $N_{i+1} \geq N_i - c_2 \log N_i$,
(3) $\delta_{i+1} \geq \delta_i + c_3 \delta_i^2 (\log N_i)^{-6}$,
(4) $W(A_{i+1}, N_{i+1}) \leq W(A_i, N_i)$.

Claim 1. For N sufficiently large, we can construct a sequence of triples $(N_i, A_i, \delta_i)_{i=0}^{Z}$ satisfying the above conditions (1)–(4) with $Z = \lfloor c_7 \frac{(\log N)^6}{\delta} \rfloor$ and c_7 a large constant.
Proof: Notice that when we apply Proposition 14 to construct $(N_{i+1}, A_{i+1}, \delta_{i+1})$ from (N_i, A_i, δ_i), we need $N_i \geq c_0$, $\delta_i \geq N_i^{-1}$ and $W(A_i, N_i) \leq c_1 \delta_i^2 \widehat{N_i}^2$. Since the sequence $(N_i)_{i\geq 0}$ is decreasing and the sequence $(\delta_i)_{i\geq 0}$ is increasing, it suffices to show that for N sufficiently large, for any sequence of triples $(N_i, A_i, \delta_i)_{i=0}^{Z}$ satisfying the conditions (1)–(4), we have $N_Z \geq c_0$, $\delta \geq N_Z^{-1}$ and $W(A_i, N_i) \leq c_1 \delta_i^2 \widehat{N_i}^2$ $(0 \leq i \leq Z)$. Notice that

$$N_Z \geq N - c_2 Z \log N \geq N - c_2 c_7 \frac{(\log N)^7}{\delta}.$$

Thus, if $\delta > c_8 \frac{(\log N)^7}{N}$ for some sufficiently large constant c_8 (in terms of c_2 and c_7), we have $N_Z \geq N/2 \geq c_0$. Since $\delta \geq 2N^{-1}$, we have $\delta \geq N_Z^{-1}$. Also, there exists a large constant c_9 (in terms of c_1, c_2, c_7) such that for c_6 sufficiently large (in terms of c_9),

$$W(A,N) < \delta^2 \exp\Big(-c_6 \frac{1}{\delta}(\log N)^7\Big)\widehat{N}^2 \leq \delta^2 q^{-c_9 \frac{(\log N)^7}{\delta}} \widehat{N}^2 \leq \delta^2 c_1 \widehat{N_Z}^2.$$

Since $(N_i)_{i\geq 0}$ is decreasing and $(\delta_i)_{i\geq 0}$ is increasing, it follows that

$$W(A_i, N_i) \leq W(A,N) \leq c_1 \delta^2 \widehat{N_Z}^2 \leq c_1 \delta_i^2 \widehat{N_i}^2 \quad (0 \leq i \leq Z).$$

This completes the proof of the claim.

Claim 2. We have $\delta_Z > 1$.
Proof: Suppose that all $\delta_i \leq 1$ $(0 \leq i \leq Z)$. Let N be sufficiently large such that $c_3 (\log N_i)^{-6} \leq 1$ $(0 \leq i \leq Z)$. Then for $0 \leq i < Z$, we have

$$\frac{1}{\delta_i} - \frac{1}{\delta_{i+1}} \geq \frac{1}{\delta_i} - \frac{1}{\delta_i + c_3 \delta_i^2 (\log N_i)^{-6}} = \frac{c_3 (\log N_i)^{-6}}{1 + c_3 \delta_i (\log N_i)^{-6}} \geq \frac{c_3 (\log N_i)^{-6}}{1 + c_3 (\log N_i)^{-6}} \geq \frac{1}{2} c_3 (\log N)^{-6}.$$

Summing over all i with $0 \leq i < Z$, for c_7 sufficiently large (in terms of c_3), we have

$$\frac{1}{\delta} - \frac{1}{\delta_Z} \geq Z c_3 (\log N)^{-6} > \frac{1}{\delta},$$

which leads to a contradiction. This completes the proof of the claim.
Since it is not possible that $\delta_Z > 1$, we conclude that if $\delta > c_8 \frac{(\log N)^7}{N}$, then we have $W(A, N) \geq \delta^2 \exp\big(-c_6 \frac{1}{\delta}(\log N)^7\big)\widehat{N}^2$. By taking $C = c_8$ and $C' = c_6$, the theorem follows.

Acknowledgment. The authors are grateful to the referee for valuable suggestions about this paper.

References

[1] A. Balog, J. Pelikán, J. Pintz & E. Szemerédi, *Difference sets without κ-th powers*, Acta Math. Hung. 65 (1994), 165–187.

[2] H. Furstenberg, *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. Analyse Math. 31 (1977), 204–256.

[3] B. Green, *On arithmetic structures in dense sets of integers*, Duke Math. Jour. 114 (2002), 215–238.

[4] T. Kamae & M. Mendès France, *Van der Corput's difference theorem*, Israel J. Math. 31 (1978), 335–342.

[5] R. M. Kubota, *Waring's problem for $\mathbb{F}_q[x]$*, Dissertationes Math. (Rozprawy Mat.) 117 (1974), 60pp.

[6] T. H. Lê, *Problems and results on intersective sets*, to appear in the 2011 Proceedings of Combinatorial and Additive Number Theory, Springer.

[7] T. H. Lê & C. V. Spencer, *Difference sets and the irreducibles in function fields*, B. Lond. Math. Soc. 43 (2011), 347–358.

[8] N. Lyall, *A simple proof of Sárközy's theorem*, to appear in Proc. Amer. Math. Soc.

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

[10] I. Z. Ruzsa & T. Sanders, *Difference sets and the primes*, Acta Arith. 131 (2008), 281–301.

[11] A. Sárközy, *On difference sets of sequences of integers, I.*, Acta Math. Acad. Sci. Hungar. 31 (1978), 125–149.

[12] A. Sárközy, *On difference sets of sequences of integers, II.*, Ann. Univ. Sci. Budapest. Etvs Sect. Math. 21 (1978), 45–53.

[13] A. Sárközy, *On difference sets of sequences of integers, III.*, Acta Math. Acad. Sci. Hungar. 31 (1978), 355–386.

[14] T. Tao, *A Fourier-free proof of the Furstenberg-Sárközy theorem*, http://terrytao.wordpress.com/2013/02/28/a-fourier-free-proof-of-the-furstenberg-sarkozy-theorem/

[15] T. D. Wooley, *Some remarks on Vinogradov's mean value theorem and Tarry's problem*, Monatsh. Math. 122 (1996), 265–273.

T. H. Lê, Department of Mathematics, The University of Texas at Austin, 1 University Station, C1200 Austin, Texas 78712

E-mail address: `leth@math.utexas.edu`

Y.-R. Liu, Department of Pure Mathematics, Faculty of Mathematics, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

E-mail address: `yrliu@math.uwaterloo.ca`