# DIFFERENCE SETS AND THE IRREDUCIBLES IN FUNCTION FIELDS

THÁI HOÀNG LÊ AND CRAIG V. SPENCER

ABSTRACT. Let $A$ be a subset of the polynomials of degree less than $N$ over a finite field $\mathbb{F}_q$. Let $r$ be any non-zero element of $\mathbb{F}_q$. We show that if the difference set $A-A$ does not contain elements of the form $P+r$, where $P$ is a monic, irreducible polynomial, then $|A| \leq Cq^{N-c\frac{N}{\log N}}$, where $C$ and $c$ are constants depending only on $q$.

## 1. INTRODUCTION

In a series of papers, Sárközy [9, 10, 11] investigated the set of differences of a set of positive density in the integers. He proved the following theorem in [11]:

**Theorem 1.** *If $\mathcal{A}$ is a subset of positive density of the integers, then there exist two distinct elements $a, a'$ of $\mathcal{A}$ such that $a - a' = p - 1$ for some prime $p$.*

Actually, he showed that if $A \subset \{1, \dots, N\}$ is such that the difference set $A - A$ does not contain elements of the form $p-1$, where $p$ is prime, then

$$|A| \ll N \frac{(\log_3 N)^3 \log_4 N}{(\log_2 N)^2},$$

where $\log_i N$ denotes $i$ iterations of the log function. To date, the current record upper bound on $|A|$ is due to Ruzsa and Sanders, who showed in [8] that:

$$|A| \ll N \exp(-c\sqrt[4]{\log N})$$

for some constant $c > 0$. In view of the many analogies between the integers and the ring $\mathbb{F}_q[t]$ of polynomials over a finite field $\mathbb{F}_q$, it is natural to ask for the analog of Sárközy's theorem in the setting of $\mathbb{F}_q[t]$. Let us fix a field $\mathbb{F}_q$ of $q$ elements. Let $\mathbf{G}_N$ be the set of all polynomials in $\mathbb{F}_q[t]$ of degree less than $N$. In this paper, we prove the following:

**Theorem 2.** *Let $r$ be a fixed element of $\mathbb{F}_q^\times$. Let $A$ be a subset of size $\delta q^N$ of $\mathbf{G}_N$ such that the difference set $A - A$ does not contain elements of the form $P + r$, where $P$ is a monic, irreducible polynomial. Then we have*

$$\delta \leq Cq^{-c\frac{N}{\log N}}$$

*for some constants $C$ and $c$ depending only on $q$.*

---

*Date*: August 31, 2010.

2000 *Mathematics Subject Classification.* 11P55, 11T55, 11L07.

*Key words and phrases.* Difference sets, irreducible polynomials, function fields, circle method.

The research of the second author is supported in part by NSF Grant DMS-0635607 and NSA Young Investigators Grant H98230-10-1-0155.

Note that in the $\mathbb{F}_q[t]$ setting, $q^N$ plays the role of $N$ in the integer setting. Thus, Ruzsa and Sanders's bound corresponds to a bound on $\delta$ of the form $Cq^{-c\sqrt[4]{N}}$ in the $\mathbb{F}_q[t]$ case, which is weaker than our bound. It is possible to adapt Kamae and Mendès France's [3] or Furstenberg's [1, 2] approaches to Theorem 1 in the $\mathbb{F}_q[t]$ setting, but these methods are not quantitative (i.e., not giving explicit dependence of $\delta$ on $N$). Our arguments run in parallel with Ruzsa and Sanders's approach. We are able to obtain better bounds than in the integer case due to better error terms in the exponential sum estimates, which in turn comes from the validity of the Generalized Riemann Hypothesis for $\mathbb{F}_q[t]$.

In another direction, Ruzsa constructed in [7] an example of a subset of $\{1, \dots, N\}$ whose difference set does not contain elements of the form $p-1$ (where $p$ is prime), and whose size is $\gg \exp\left(\left(\frac{\log 2}{2} + o(1)\right)\frac{\log N}{\log\log N}\right)$. A straightforward adaptation of Ruzsa's construction gives the following lower bound of the same type in the $\mathbb{F}_q[t]$ setting, of which we will omit the proof:

**Proposition 3.** *For all integers $N > 1$, there is a set $A \subset \mathbf{G}_N$ such that $|A| \geq q^{\left(\frac{\log q}{q(q-1)}+o(1)\right)\frac{N}{\log N}}$ and $A - A$ does not contain $P + x$, for all (not necessarily monic) irreducible polynomial $P$ and all $x \in \mathbb{F}_q^\times$.*

If we merely require $P$ to be monic, then we can do much better if $q > 3$. Indeed, if $q > 3$, then let $A$ be the set of all polynomials in $\mathbf{G}_N$ whose coefficients are in $R$, where $R$ is a subset of $\mathbb{F}_q$ whose difference set does not contain 1. Then, all the differences in $A$ are not monic, and $A$ is of size $q^{cN}$. It may be interesting for one to study the maximal size of a subset of $\mathbf{G}_N$ whose difference set avoids the monic polynomials.

It should be mentioned that the conclusions of Theorem 1 remain true if we replace $\{p-1 : p \text{ prime}\}$ by the set of the squares. We plan to treat the $\mathbb{F}_q[t]$ analog for the squares (and more generally, $k$-th powers) in a future paper.

**Acknowledgments.** We would like to thank Tom Sanders and Terence Tao for helpful discussions. This research was started while the second author was a member of the Institute for Advanced Study, and he would like to thank the School of Mathematics for their hospitality.

## 2. Notation and preliminaries

2.1. **Notation.** For $k \in \mathbb{N}$, let $f(k)$ and $g(k)$ be functions of $k$. If $g(k)$ is positive and there exists a constant $c > 0$ such that $|f(k)| \leq cg(k)$ for all $k \in \mathbb{N}$, we write $f(k) \ll g(k)$. In this paper, all the implicit constants depend only on $q$. The value of $r$ is also fixed throughout the paper.

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 $\infty$. Each element $\alpha \in \mathbb{K}_\infty$ may be written in the form $\alpha = \sum_{i \leq w} a_i t^i$ for some $w \in \mathbb{Z}$ and $a_i = a_i(\alpha) \in \mathbb{F}_q$ $(i \leq w)$. If $a_w \neq 0$, we say that $\operatorname{ord}\alpha = w$, and we write $\langle\alpha\rangle$ for $q^{\operatorname{ord}\alpha}$. We adopt the conventions that $\operatorname{ord} 0 = -\infty$ and $\langle 0\rangle = 0$. We write $\|\alpha\|$ for $\sum_{i \leq \min\{w,-1\}} a_i t^i$. Also, it is often convenient to refer to $a_{-1}$ as being the residue of $\alpha$, denoted by $\operatorname{res}\alpha$. For a real number $N$, we let $\widehat{N}$ denote $q^N$. Hence, if $x$ is a polynomial in $\mathbb{F}_q[t]$, then $\langle x\rangle < \widehat{N}$ if and only if the degree of $x$ is strictly less than $N$. Recall that $\mathbf{G}_N = \left\{x \in \mathbb{F}_q[t] \,|\, \langle x\rangle < \widehat{N}\right\}$, and let $\mathcal{P}_N$ denote the set of all monic, irreducible polynomials in $\mathbf{G}_N$.

We define the $\mathbb{F}_q[t]$-analogue of the von-Mangoldt function $\Lambda : \mathbb{F}_q[t] \to \mathbb{Z}$ by

$$\Lambda(x) = \begin{cases} \operatorname{ord} \varpi, & \text{if } \varpi^k = x, \text{ where } \varpi \text{ is a monic, irreducible polynomial,} \\ 0, & \text{otherwise.} \end{cases}$$

Let us also define

$$\lambda_m(y) = \lambda_m(y; N) = \begin{cases} \operatorname{ord}(my + r), & \text{if } my + r \text{ is monic, irreducible, and of degree less than } N, \\ 0, & \text{otherwise.} \end{cases}$$

For a polynomial $g$, let $\phi(g)$ denote the Euler totient function of $g$, i.e. the number of units in the ring $\mathbb{F}_q[t]/(m)$. It is easy to see that for every $\epsilon > 0$, $\phi(g) \gg_\epsilon \langle g \rangle^{1-\epsilon}$.

2.2. **The circle method in $\mathbb{F}_q[t]$.** Consider the compact additive subgroup $\mathbb{T}$ of $\mathbb{K}_\infty$ defined by $\mathbb{T} = \{\alpha \in \mathbb{K}_\infty : \langle \alpha \rangle < 1\}$. Given a Haar measure $d\alpha$ on $\mathbb{K}_\infty$, we normalize it so that $\int_{\mathbb{T}} 1 \, d\alpha = 1$. Thus, if $\mathfrak{N}$ is the subset of $\mathbb{K}_\infty$ defined by $\mathfrak{N} = \{\alpha \in \mathbb{K}_\infty \,|\, \operatorname{ord} \alpha < -N\}$, where $N$ is an integer, then the measure of $\mathfrak{N}$, $\operatorname{mes}(\mathfrak{N}) = \int_{\alpha \in \mathfrak{N}} d\alpha$, is equal to $\widehat{N}^{-1}$.

We are now able to define the exponential function on $\mathbb{F}_q[t]$. 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 $\alpha \in \mathbb{K}_\infty$, the value of $e(\alpha)$ to be $e_q(\operatorname{res} \alpha)$. The orthogonality relation underlying the Fourier analysis of $\mathbb{F}_q[t]$, established in [4, Lemma 1], takes the shape

$$\int_{\mathbb{T}} e(h\alpha) \, d\alpha = \begin{cases} 1, & \text{if } h = 0, \\ 0, & \text{if } h \in \mathbb{F}_q[t] \setminus \{0\}. \end{cases} \tag{1}$$

For a function $f$ defined on $\mathbb{F}_q[t]$, of compact support, let us define its Fourier transform by

$$\widehat{f}(\alpha) = \sum_{x \in \mathbb{F}_q[t]} e(\alpha x) f(x).$$

For a monic polynomial $m \in \mathbb{F}_q[t]$, we define the weighted exponential sum over the irreducible polynomials in arithmetic progression by

$$h_m(\alpha) = h_m(\alpha; N) = \sum_{y \in \mathbb{F}_q[t]} \lambda_m(y; N) e(\alpha y).$$

Thus for any set $A \subset \mathbf{G}_N$, by (1), we have

$$\int_{\mathbb{T}} |\widehat{1_A}(\alpha)|^2 h_m(\alpha) \, d\alpha = \sum_{x_1 \in A} \sum_{x_2 \in A} \sum_{\substack{y \in \mathbb{F}_q[t], \\ x_1 - x_2 = y}} \lambda_m(y) \, .$$

For $a, g \in \mathbb{F}_q[t]$ with $\langle a \rangle < \langle g \rangle$, where $g$ is a monic polynomial, we write

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

We also write

$$\mathfrak{M}_{g,\eta} = \bigcup_{\langle a\rangle<\langle g\rangle} \mathfrak{M}_{a,g,\eta}$$

and

$$\mathfrak{M}^*_{g,\eta} = \bigcup_{\substack{\langle a\rangle<\langle g\rangle\\(a,g)=1}} \mathfrak{M}_{a,g,\eta}.$$

## 3. Major and minor arc estimates for $h_m(\alpha)$

In this section, we obtain the necessary major and minor arc estimates for $h_m(\alpha)$ that are needed in the proof of Theorem 2. Before doing this, we will need to establish additional notation. Let $P_R$ denote the set of monic irreducible polynomials of $\operatorname{ord} R$, and let $S_R$ denote the set of monic polynomials of $\operatorname{ord} R$. For $\beta \in \mathbb{T}$, let $\tau_R(\beta) = \tau(\beta; R) = \sum_{x\in S_R} e(\beta)$.

### 3.1. Minor arc estimates.

We now recall [5, Lemma 23], which will be used to derive our minor arc estimate.

**Lemma 4.** *Let $m \in \mathbb{F}_q[t]$ be a monic polynomial, and let $b \in \mathbb{F}_q[t]$ with $\langle b\rangle < \langle m\rangle$ and $(b, m) = 1$. Let $a, g \in \mathbb{F}_q[t]$ with $g$ monic, $\langle a\rangle < \langle g\rangle$, and $(a, g) = 1$. Suppose that $\langle m\rangle \le q^{-2}\widehat{N}^{2/5}N$, $\langle g\rangle \le q^{-1}\widehat{N}\langle m\rangle$, and $\alpha \in \mathfrak{M}_{a,g,\langle g\rangle^{-2}}$. Then, we have*

$$\sum_{\substack{y\in\mathbf{G}_N\\ y\equiv b\,(\mathrm{mod}\ m)}} \Lambda(y)e(\alpha y) \ll \widehat{N}^{4/5}\langle m\rangle N^4 + \langle g\rangle N^3 + \widehat{N}N^{9/2}\langle m\rangle^{1/2}\langle g\rangle^{-1/2} + \widehat{N}^{1/2}N^{9/2}\langle m\rangle^{1/2}\langle g\rangle^{1/2}.$$

**Lemma 5.** *Let $m \in \mathbb{F}_q[t]$ be a monic polynomial with $\langle m\rangle \le q^{-2}\widehat{N}^{2/5}N$, and let $Q$ be a positive real number. Let $a, g \in \mathbb{F}_q[t]$ with $g$ monic, $\langle a\rangle < \langle g\rangle \le \widehat{Q} \le q^{-1}\widehat{N}\langle m\rangle$, and $(a, g) = 1$. Suppose that $\alpha \in \mathfrak{M}_{a,g,\widehat{Q}^{-1}\langle g\rangle^{-1}}$. Then, we have*

$$h_m(\alpha; N) \ll \widehat{N}^{4/5}\langle m\rangle N^4 + \widehat{Q}\langle m\rangle N^3 + \widehat{N}N^{9/2}\langle m\rangle^{1/2}\langle g\rangle^{-1/2} + \widehat{N}^{1/2}N^{9/2}\langle m\rangle\widehat{Q}^{1/2}.$$

*Proof.* We have

$$\begin{aligned} h_m(\alpha; N) &= \sum_{\substack{y\in\mathbf{G}_{N-\operatorname{ord} m}\\ my+r\in\mathcal{P}_N}} \big(\operatorname{ord}(my + r)\big)e(\alpha y)\\ &= e(-\alpha r/m) \sum_{\substack{z\in\mathbf{G}_N\\ z\equiv r\,(\mathrm{mod}\, m)}} \Lambda(z)e(\alpha z/m)\\ &\qquad + O\Bigg(\sum_{\substack{\varpi \text{ monic irred}\\ \langle\varpi\rangle^2<\widehat{N}}} \operatorname{ord}\varpi + \sum_{\substack{\varpi \text{ monic irred}\\ \langle\varpi\rangle^3<\widehat{N}}} \operatorname{ord}\varpi + \cdots\Bigg)\\ &\ll \Bigg|\sum_{\substack{z\in\mathbf{G}_N\\ z\equiv r\,(\mathrm{mod}\, m)}} \Lambda(z)e(\alpha z/m)\Bigg| + \widehat{N}^{1/2}N. \end{aligned} \tag{2}$$

By the Dirichlet approximation theorem, there exist $a', g' \in \mathbb{F}_q[t]$ with $g'$ monic, $(a', g') = 1$, $\langle g' \rangle \leq \langle m \rangle \widehat{Q}$, and $\langle \alpha/m - a'/g' \rangle < \langle m \rangle^{-1} \widehat{Q}^{-1} \langle g' \rangle^{-1}$. Then,

$$\langle \frac{a'}{g'} - \frac{a}{mg} \rangle \leq \max\Big\{ \langle \frac{a'}{g'} - \frac{\alpha}{m} \rangle, \langle \frac{\alpha}{m} - \frac{a}{mg} \rangle \Big\} < \max\{ \langle m \rangle^{-1} \widehat{Q}^{-1} \langle g' \rangle^{-1}, \langle m \rangle^{-1} \widehat{Q}^{-1} \langle g \rangle^{-1} \}.$$

¿From the above inequality, we may deduce that

$$\langle a'mg - ag' \rangle < \max\{ \widehat{Q}^{-1} \langle g \rangle, \widehat{Q}^{-1} \langle g' \rangle^{-1} \}.$$

Suppose for the moment that $\langle g' \rangle < \langle g \rangle \leq \widehat{Q}$. We then have $\langle a'mg - ag' \rangle < 1$, implying that $a'mg = ag'$. Since $(g, a) = 1$, it follows that $g | g'$, and we may deduce that $\langle g \rangle \leq \langle g' \rangle$, which provides a contradiction. Hence, we have $\langle g \rangle \leq \langle g' \rangle$. Applying Lemma 4 with the approximation $a'/g'$ to $\alpha/m$, we find that

$$\begin{aligned} \sum_{\substack{z \in \mathbf{G}_N \\ z \equiv r \pmod m}} \Lambda(z) e(\alpha z/m) &\ll \widehat{N}^{4/5} \langle m \rangle N^4 + \langle g' \rangle N^3 + \widehat{N} N^{9/2} \langle m \rangle^{1/2} \langle g' \rangle^{-1/2} + \widehat{N}^{1/2} N^{9/2} \langle m \rangle^{1/2} \langle g' \rangle^{1/2} \\ &\ll \widehat{N}^{4/5} \langle m \rangle N^4 + \widehat{Q} \langle m \rangle N^3 + \widehat{N} N^{9/2} \langle m \rangle^{1/2} \langle g \rangle^{-1/2} + \widehat{N}^{1/2} N^{9/2} \langle m \rangle \widehat{Q}^{1/2}. \end{aligned} \tag{3}$$

The lemma now follows by combining (2) and (3). □

### 3.2. **Major arc estimates.**

**Lemma 6.** *Let $m \in \mathbb{F}_q[t]$ be a monic polynomial, and let $r \in \mathbb{F}_q[t]$ with $\langle r \rangle < \langle m \rangle$ and $(r, m) = 1$. Let $Q_1$ and $Q_2$ be positive real numbers. Let $a, g \in \mathbb{F}_q[t]$ with $g$ monic, $\langle a \rangle < \langle g \rangle \leq \widehat{Q}_2$, and $(a, g) = 1$. Let $\alpha \in \mathfrak{M}_{a,g,\langle g \rangle^{-1} \widehat{Q}_1^{-1}}$. Let $M \in \mathbb{N}$ with $M \geq Q_2$. Then, we have*

$$\sum_{\substack{y \in S_M \\ my + r \in P_{M + \operatorname{ord} m}}} e(\alpha y) = \begin{cases} \frac{\mu(g) \langle m \rangle e\left(\frac{-ar\bar{m}}{g}\right)}{\phi(m)\phi(g)(M + \operatorname{ord} m)} \tau_M(\alpha - a/g) + O\Big( \frac{\widehat{M}^{3/2} \langle m \rangle^{1/2} (M + \operatorname{ord} m)^2}{\min\left(\widehat{M}/\widehat{Q_2}, \widehat{Q_1}\right)} \Big), & \text{if } (m, g) = 1, \\ O\Big( \frac{\widehat{M}^{3/2} \langle m \rangle^{1/2} (M + \operatorname{ord} m)^2}{\min\left(\widehat{M}/\widehat{Q_2}, \widehat{Q_1}\right)} \Big), & \text{otherwise.} \end{cases}$$

*Here, $\bar{m}$ denotes the multiplicative inverse of $m$ modulo $g$.*

*Proof.* This lemma follows from the proofs of [5, Lemmas 7-11] upon redefining $L$ to be $\min([M - Q_2], [Q_1])$ and $\mathfrak{M}_{a,g}$ to be $\mathfrak{M}_{a,g,\langle g \rangle^{-1} \widehat{Q}_1^{-1}}$. □

**Lemma 7.** *Let $m \in \mathbb{F}_q[t]$ be a monic polynomial, and $r \in \mathbb{F}_q[t]$ with $\langle r \rangle < \langle m \rangle$ and $(r, m) = 1$. Let $Q_1$ and $Q_2$ be positive real numbers. Let $a, g \in \mathbb{F}_q[t]$ with $g$ monic, $\langle a \rangle < \langle g \rangle \leq \widehat{Q}_2$, and $(a, g) = 1$. Let $\alpha \in \mathfrak{M}_{a,g,\langle g \rangle^{-1} \widehat{Q}_1^{-1}}$. Then, we have*

$$h_m(\alpha; N) = \begin{cases} \frac{\mu(g) \langle m \rangle e\left(\frac{-ar\bar{m}}{g}\right)}{\phi(m)\phi(g)} \sum_{\substack{x \in \mathbf{G}_{N - \operatorname{ord} m} \\ x \text{ monic}}} e\big((\alpha - a/g)x\big) + O\big(f(N, Q_1, Q_2; m)\big), & \text{if } (m, g) = 1, \\ O\big(f(N, Q_1, Q_2; m)\big), & \text{otherwise,} \end{cases}$$

*where*

$$f(N, Q_1, Q_2; m) = \widehat{N}^{1/2} N^3 \widehat{Q}_2 + \widehat{N}^{3/2} N^3 \langle m \rangle^{-1} \widehat{Q}_1^{-1}.$$

*Proof.* Note that

$$\begin{aligned} h_m(\alpha;N) &= \sum_{\substack{y\in \mathbf{G}_{N-\operatorname{ord} m}\\ my+r\in\mathcal{P}_N}} \big(\operatorname{ord}(my+r)\big)e(\alpha y)\\ &= \sum_{X=0}^{N-\operatorname{ord} m-1}\Bigg((X+\operatorname{ord} m)\sum_{\substack{z\in S_X\\ mz+r\in P_{X+\operatorname{ord} m}}} e(\alpha z)\Bigg)+O(1)\\ &= \sum_{X=\lceil Q_2\rceil}^{N-\operatorname{ord} m-1}\Bigg((X+\operatorname{ord} m)\sum_{\substack{z\in S_X\\ mz+r\in P_{X+\operatorname{ord} m}}} e(\alpha z)\Bigg)+O\big(\widehat{Q}_2\langle m\rangle\phi(m)^{-1}\big). \end{aligned}$$

By applying Lemma 6, we deduce that

$$h_m(\alpha;N)=\begin{cases}\frac{\mu(g)\langle m\rangle e\left(\frac{-ar\bar{m}}{g}\right)}{\phi(m)\phi(g)}\displaystyle\sum_{\substack{x\in\mathbf{G}_{N-\operatorname{ord} m}\\ x\text{ monic}}} e\big((\alpha-a/g)x\big)+O\big(f(N,Q_1,Q_2;m)\big), & \text{if } (m,g)=1,\\ O\big(f(N,Q_1,Q_2;m)\big), & \text{otherwise,}\end{cases}$$

where

$$f(N,Q_1,Q_2;m)=\widehat{N}^{1/2}N^2\widehat{Q}_2+\widehat{N}^{3/2}N^2\langle m\rangle^{-1}\widehat{Q}_1^{-1}.$$

This completes the proof of the lemma. □

## 4. Energy Increments

In this section, we will establish lemmas concerning energy increments. These are analogous to those found in [8, Section 7].

**Lemma 8.** *Suppose that $L\in\mathbb{N}$ and $m,r\in\mathbb{F}_q[t]$ with $m\neq 0$. Also, suppose that $A\subseteq\mathbf{G}_N$ with $|A|=\delta\widehat{N}$. Let $B=\{ml+r\,|\,\langle l\rangle<\widehat{L}\}$. Furthermore, suppose that*

$$\sum_{x\in\mathbb{F}_q[t]}\big((1_A-\delta 1_{\mathbf{G}_N})*1_B\big)^2(x)\geq c\delta^2\widehat{N}\widehat{L}^2.$$

*Then, there exists $x'\in\mathbb{F}_q[t]$ such that*

$$1_A*1_B(x')\geq(1+c)\delta\widehat{L}+O(\widehat{N}^{-1}\langle m\rangle\widehat{L}^2).$$

*Proof.* Note that

$$\begin{aligned}\sum_{x\in\mathbb{F}_q[t]}\big((1_A*1_B)(1_{\mathbf{G}_N}*1_B)\big)(x)&=\sum_{x\in\mathbb{F}_q[t]}1_A(x)\big(1_{\mathbf{G}_N}*1_{-B}*1_B\big)(x)\\ &=\delta\widehat{N}\widehat{L}^2+O(\delta\langle m\rangle\widehat{L}^3).\end{aligned}\tag{4}$$

Also, we have

$$\sum_{x\in\mathbb{F}_q[t]}\big(1_{\mathbf{G}_N}*1_B\big)^2(x)=\widehat{N}\widehat{L}^2+O(\langle m\rangle\widehat{L}^3).\tag{5}$$

Since

$$\sum_{x\in\mathbb{F}_q[t]}\big((1_A-\delta 1_{\mathbf{G}_N})*1_B\big)^2(x)\geq c\delta^2\widehat{N}\widehat{L}^2,$$

we may deduce from (4) and (5) that

$$\begin{aligned}\sum_{x\in\mathbb{F}_q[t]}\big(1_A*1_B\big)^2(x)&\geq c\delta^2\widehat{N}\widehat{L}^2+2\delta\sum_{x\in\mathbb{F}_q[t]}\big((1_A*1_B)(1_{\mathbf{G}_N}*1_B)\big)(x)-\delta^2\sum_{x\in\mathbb{F}_q[t]}\big(1_{\mathbf{G}_N}*1_B\big)^2(x)\\&=c\delta^2\widehat{N}\widehat{L}^2+2\delta^2\widehat{N}\widehat{L}^2-\delta^2\widehat{N}\widehat{L}^2+O(\delta\langle m\rangle\widehat{L}^3)\\&=(1+c)\delta^2\widehat{N}\widehat{L}^2+O(\delta\langle m\rangle\widehat{L}^3).\end{aligned}\tag{6}$$

By the triangle inequality, we have

$$\sum_{x\in\mathbb{F}_q[t]}\big(1_A*1_B\big)^2(x)\leq\sup_{x'\in\mathbb{F}_q[t]}\big(1_A*1_B\big)(x')\sum_{x\in\mathbb{F}_q[t]}\big(1_A*1_B\big)(x)=\delta\widehat{N}\widehat{L}\sup_{x'\in\mathbb{F}_q[t]}\big(1_A*1_B\big)(x').\tag{7}$$

The lemma now follows by combining (6) and (7). □

**Lemma 9.** *Suppose that $\eta>0$, $N\in\mathbb{N}$, and $g\in\mathbb{F}_q[t]\setminus\{0\}$. Suppose that $A\subseteq\mathbf{G}_N$ with $|A|=\delta\widehat{N}$. Write*

$$E_{A,g,\eta}=\delta^{-2}\widehat{N}^{-1}\int_{\mathfrak{M}_{g,\eta}}\big|\big(1_A-\delta 1_{\mathbf{G}_N}\big)^\wedge(\alpha)\big|^2\,d\alpha.$$

*Then, there exist $L\in\mathbb{N}$ with $\widehat{L}\gg\langle g\rangle^{-1}\min\{\eta^{-1},E_{A,g,\eta}|A|\}$ and $r\in\mathbb{F}_q[t]$ such that for $B=\{lg+r\,|\,\langle l\rangle<\widehat{L}\}$, we have $|A\cap B|\geq\delta(1+E_{A,g,\eta}/2)\widehat{L}$.*

*Proof.* Let $L\in\mathbb{N}$ be a parameter to be chosen later with $\widehat{L}\leq\eta^{-1}\langle g\rangle^{-1}$, and let $D=\{gl\,|\,\langle l\rangle<\widehat{L}\}$. For $x\in D$ and $\alpha\in\mathfrak{M}_{a,g,\eta}$, we have $\langle(\alpha-a/g)x\rangle<\eta\langle g\rangle q^{-1}\widehat{L}\leq q^{-1}$, which implies that $e(\alpha x)=e(ax/g)$. Hence, for $\alpha\in\mathfrak{M}_{a,g,\eta}$, we have

$$|\widehat{1_D}(\alpha)|=\Big|\sum_{x\in D}e(\alpha x)\Big|=\Big|\sum_{\langle x\rangle\in D}e(ax/g)\Big|=\Big|\sum_{\langle l\rangle<\widehat{L}}e(al)\Big|=\widehat{L}.$$

It follows from the triangle inequality that

$$\begin{aligned}\delta^2\widehat{N}\widehat{L}^2E_{A,g,\eta}&\leq\int_{\mathfrak{M}_{g,\eta}}\big|\big(1_A-\delta 1_{\mathbf{G}_N}\big)^\wedge(\alpha)\big|^2|1_D^\wedge(\alpha)|^2\,d\alpha\\&\leq\int_{\mathbb{T}}\big|\big(1_A-\delta 1_{\mathbf{G}_N}\big)^\wedge(\alpha)\big|^2|1_D^\wedge(\alpha)|^2\,d\alpha\\&=\sum_{x\in\mathbb{F}_q[t]}\big((1_A-\delta 1_{\mathbf{G}_N})*1_D\big)^2(x).\end{aligned}$$

By Lemma 8, there exists $x'\in\mathbb{F}_q[t]$ such that

$$1_A*1_D(x')\geq(1+E_{A,g,\eta})\delta\widehat{L}+O(\widehat{N}^{-1}\langle g\rangle\widehat{L}^2).$$

Thus, there is a choice of $L\in\mathbb{N}$ for which $\widehat{L}\gg\langle g\rangle^{-1}\min\big(\eta^{-1},E_{A,g,\eta}|A|\big)$ and

$$1_A*1_D(x')\geq\delta\Big(1+\frac{E_{A,g,\eta}}{2}\Big)\widehat{L}.$$

The lemma now follows. □

**Lemma 10.** *Suppose that $\eta > 0$, $N \in \mathbb{N}$, and $g \in \mathbb{F}_q[t] \setminus \{0\}$. Suppose that $A \subseteq \mathbf{G}_N$ with $|A| = \delta \widehat{N}$. Write*

$$E^*_{A,g,\eta} = \delta^{-2}\widehat{N}^{-1} \int_{\mathfrak{M}^*_{g,\eta}} \left|\left(1_A - \delta 1_{\mathbf{G}_N}\right)^\wedge(\alpha)\right|^2 d\alpha.$$

*Suppose that for $K \in \mathbb{N}$, we have*

$$\sum_{\substack{1 \leq \langle g \rangle \leq \widehat{K} \\ g \text{ monic}}} \frac{1}{\phi(g)} E^*_{A,g,\eta} \geq c.$$

*Then, there exist $g, r \in \mathbb{F}_q[t]$ with $1 \leq \langle g \rangle \leq \widehat{K}$ and $L \in \mathbb{N}$ with $\widehat{L} \gg \langle g \rangle^{-1} \min\{\eta^{-1}, \delta c \widehat{N}\}$ such that for $B = \{lg + r \,|\, \langle l \rangle < \widehat{L}\}$, we have $|A \cap B| \geq \delta(1 + c_1 c)\widehat{L}$, where $c_1 = c_1(q)$ is a positive constant depending at most on $q$.*

*Proof.* Define $E_{A,g,\eta}$ as in Lemma 9, and write

$$I_{A,a,g,\eta} = \delta^{-2}\widehat{N}^{-1} \int_{\mathfrak{M}_{a,g,\eta}} \left|\left(1_A - \delta 1_{\mathbf{G}_N}\right)^\wedge(\alpha)\right|^2 d\alpha.$$

Note that

$$\begin{aligned}
\sum_{\substack{1 \leq \langle g \rangle \leq \widehat{K} \\ g \text{ monic}}} \frac{\langle g \rangle}{\phi(g)} E_{A,g,\eta} &= \sum_{\substack{1 \leq \langle g \rangle \leq \widehat{K} \\ g \text{ monic}}} \frac{\langle g \rangle}{\phi(g)} \sum_{\langle r \rangle < \langle g \rangle} I_{A,r,g,\eta} \\
&= \sum_{\substack{1 \leq \langle g \rangle \leq \widehat{K} \\ g \text{ monic}}} \frac{\langle g \rangle}{\phi(g)} \sum_{\substack{g'h = g \\ g' \text{ monic}}} \sum_{\substack{\langle r' \rangle < \langle g' \rangle \\ (r', g') = 1}} I_{A,r'h,g'h,\eta} \\
&= \sum_{\substack{1 \leq \langle g \rangle \leq \widehat{K} \\ g \text{ monic}}} \frac{\langle g \rangle}{\phi(g)} \sum_{\substack{g'h = g \\ g' \text{ monic}}} E^*_{A,g',\eta} \\
&= \sum_{\substack{1 \leq \langle g' \rangle \leq \widehat{K} \\ g' \text{ monic}}} E^*_{A,g',\eta} \sum_{\substack{1 \leq \langle h \rangle \leq \widehat{K}/\langle g' \rangle \\ h \text{ monic}}} \frac{\langle g'h \rangle}{\phi(g'h)}.
\end{aligned}$$

Also, we have

$$\sum_{\substack{1 \leq \langle h \rangle \leq \widehat{K}/\langle g' \rangle \\ h \text{ monic}}} \frac{\langle g'h \rangle}{\phi(g'h)} \geq \frac{\langle g' \rangle}{\phi(g')} \sum_{\substack{1 \leq \langle h \rangle \leq \widehat{K}/\langle g' \rangle \\ h \text{ monic}}} 1 \geq \frac{\widehat{K}}{\phi(g')}.$$

Therefore, we have

$$\sum_{\substack{1 \leq \langle g \rangle \leq \widehat{K} \\ g \text{ monic}}} \frac{\langle g \rangle}{\phi(g)} E_{A,g,\eta} \geq \widehat{K} \sum_{\substack{1 \leq \langle g' \rangle \leq \widehat{K} \\ g' \text{ monic}}} \frac{1}{\phi(g')} E^*_{A,g',\eta} \geq \widehat{K} c \tag{8}$$

by the hypothesis. Also, we have

$$\sum_{\substack{1 \leq \langle g \rangle \leq \widehat{K} \\ g \text{ monic}}} \frac{\langle g \rangle}{\phi(g)} = \sum_{\substack{1 \leq \langle g \rangle \leq \widehat{K} \\ g \text{ monic}}} \sum_{\substack{d | g \\ d \text{ monic}}} \frac{\mu(d)^2}{\phi(d)} = \sum_{\substack{1 \leq \langle d \rangle \leq \widehat{K} \\ d \text{ monic}}} \frac{\mu(d)^2}{\phi(d)} \sum_{\substack{1 \leq \langle g \rangle \leq \widehat{K}/\langle d \rangle \\ g \text{ monic}}} 1 \ll \widehat{K} \sum_{\substack{1 \leq \langle d \rangle \leq \widehat{K} \\ d \text{ monic}}} \frac{1}{\langle d \rangle \phi(d)} \ll \widehat{K}. \tag{9}$$

By (8) and (9), there exists a monic polynomial $g$ with $1 \le \langle g\rangle \le \widehat{K}$ and $E_{A,g,\eta} \gg c$. The result now follows from Lemma 9. □

## 5. An iteration and the proof of Theorem 2

In this section, we first prove the following lemma.

**Lemma 11.** *Suppose that $\widehat{N} \ge C_0$, $A \subset \mathbf{G}_N, |A| = \delta\widehat{N}$, $\delta^{-1} \le \widehat{N}^{\kappa}$, and $\langle m\rangle \le \widehat{N}^{\kappa}$, where $\kappa$ is a small, absolute constant. If the difference set $A-A$ does not contain elements of the form $\frac{P+r}{m}$, where $P$ is monic, irreducible, then there exists an integer $N'$, a set $A' \subset \mathbf{G}_{N'}$ of density $\delta'$ in $\mathbf{G}_{N'}$, and a monic polynomial $m'$ such that the following hold:*

(1) $\delta' \ge (1+C_1)\delta$,
(2) $\langle m'\rangle \le C_2\delta^{-2}\langle m\rangle$,
(3) $\widehat{N'} \ge C_3\left(\frac{\delta}{N\langle m\rangle}\right)^9 \widehat{N}$,
(4) $(A'-A') \cap \{\frac{P+r}{m'} : P \text{ monic, irreducible}\} = \emptyset$,

*where $C_0$, $C_1$, $C_2$, and $C_3$ are constants depending at most on $q$.*

*Proof.* Let $f_A = 1_A - \delta 1_{\mathbf{G}_N}$, the balanced function of $A$. Note that $\int_{\mathbb{T}} |\widehat{f_A}(\alpha)|^2 d\alpha = (\delta-\delta^2)\widehat{N}$. Let us consider the expression

$$I = \int_{\mathbb{T}} |\widehat{f_A}(\alpha)|^2 h_m(\alpha; N) d\alpha.$$

Let us first compute $I$ explicitly. We have

$$\begin{aligned} I &= \sum_{x\in A, y\in \mathbf{G}_N} A(x+y)A(x)\lambda_m(y) + \delta^2 \sum_{x\in\mathbf{G}_N, y\in\mathbf{G}_N} \mathbf{G}_N(x+y)\mathbf{G}_N(x)\lambda_m(y) \\ &\quad - \delta \sum_{x\in\mathbf{G}_N, y\in\mathbf{G}_N} \mathbf{G}_N(x+y)A(x)\lambda_m(y) - \delta \sum_{x\in\mathbf{G}_N, y\in\mathbf{G}_N} \mathbf{G}_N(x)A(x+y)\lambda_m(y) \\ &= -\delta^2\widehat{N}\sum_y \lambda_m(y), \end{aligned} \tag{10}$$

since by hypothesis the first term is zero.

Let $\widehat{Q}_1 = c\delta^2\frac{\widehat{N}}{N^9\langle m\rangle^4}$, $\widehat{Q}_2 = c^{-1}\delta^{-2}N^9\langle m\rangle^3$, where $c$ is a sufficiently small constant to be chosen later. By the Dirichlet approximation theorem, the sets $\mathfrak{M}_{a,g,\langle g\rangle^{-1}\widehat{Q}^{-1}}$, where $(a,g)=1$, $g$ is monic, and $\langle a\rangle < \langle g\rangle \le \widehat{Q}_1$, are disjoint and form a partition of $\mathbb{T}$. Let us define the major arcs

$$\mathfrak{M} = \bigcup_{\substack{\langle a\rangle<\langle g\rangle,\,(a,g)=1\\ \langle g\rangle\le\widehat{Q_2},\, g \text{ monic}}} \mathfrak{M}_{a,g,\langle g\rangle^{-1}\widehat{Q_1}^{-1}}$$

and the minor arcs

$$\mathfrak{m} = \bigcup_{\substack{\langle a\rangle<\langle g\rangle,\,(a,g)=1\\ \widehat{Q_2}<\langle g\rangle\le\widehat{Q_1}\\ g \text{ monic}}} \mathfrak{M}_{a,g,\langle g\rangle^{-1}\widehat{Q_1}^{-1}}$$

so that $\mathbb{T} = \mathfrak{M} \bigcup \mathfrak{m}$.

**Claim 1.** The contribution from the minor arcs in $I$ is small. Indeed, by Lemma 5 we have

$$\sup_{\alpha \in \mathfrak{m}} |h_m(\alpha; N)| \ll \widehat{N}^{4/5}\langle m\rangle N^4 + \widehat{Q}_1\langle m\rangle N^3 + \widehat{N}N^{9/2}\langle m\rangle^{1/2}\widehat{Q_2}^{-1/2} + \widehat{N}^{1/2}N^{9/2}\langle m\rangle \widehat{Q}_1^{1/2}.$$

By our choices of $\widehat{Q}_1$ and $\widehat{Q}_2$, all the four terms are dominated by $\delta \frac{\widehat{N}}{\langle m\rangle}$. Thus,

$$\left| \int_{\mathfrak{m}} |f_A(\alpha)|^2 h_m(\alpha; N) d\alpha \right| \ll \delta \frac{\widehat{N}}{\langle m\rangle} \int_{\mathbb{T}} |f_A(\alpha)|^2 d\alpha \ll \delta^2 \frac{\widehat{N}^2}{\langle m\rangle}.$$

By Lemma 7, we see that $\sum_y \lambda_m(y) \geq \frac{1}{2}\frac{\widehat{N}}{\phi(m)} \geq \frac{1}{2}\frac{\widehat{N}}{\langle m\rangle}$ if $\langle m\rangle \leq N^\kappa$ and $N$ is sufficiently large. Thus, for an appropriate choice of $c$, we have that for all sufficiently large $N$,

$$\left| \int_{\mathfrak{m}} |f_A(\alpha)|^2 h_m(\alpha, N) d\alpha \right| \leq \frac{1}{2}\delta^2 \widehat{N} \sum_y \lambda_m(y).$$

Now let $\widehat{Q}_3 = c'\delta^{-2}$, where $c'$ is a sufficiently large positive constant to be chosen later, and let us split the major arcs $\mathfrak{M}$ into two parts, $\mathfrak{M} = \mathfrak{M}_1 \bigcup \mathfrak{M}_2$, where

$$\mathfrak{M}_1 = \bigcup_{\substack{\langle a\rangle < \langle g\rangle,\, (a,g)=1 \\ \langle g\rangle \leq \widehat{Q}_3,\, g \text{ monic}}} \mathfrak{M}_{a,g,\langle g\rangle^{-1}\widehat{Q_1}^{-1}}$$

and

$$\mathfrak{M}_2 = \bigcup_{\substack{\langle a\rangle < \langle g\rangle,\, (a,g)=1 \\ \widehat{Q}_3 < \langle g\rangle \leq \widehat{Q}_2 \\ g \text{ monic}}} \mathfrak{M}_{a,g,\langle g\rangle^{-1}\widehat{Q_1}^{-1}}.$$

**Claim 2.** The contribution from $\mathfrak{M}_2$ in $I$ is small. Indeed, for $\alpha \in \mathfrak{M}_{a,g,\langle g\rangle^{-1}\widehat{Q_1}^{-1}}$, where $\widehat{Q}_3 < \langle g\rangle \leq \widehat{Q}_2$, Lemma 5 implies that

$$h_m(\alpha; N) \ll \frac{\widehat{N}}{\phi(g)\phi(m)} \ll \frac{\widehat{N}}{\langle g\rangle^{1/2}\phi(m)} \leq \frac{\widehat{N}}{\widehat{Q}_3^{1/2}\phi(m)} \ll \delta \sum_y \lambda_m(y).$$

Therefore,

$$\left| \int_{\mathfrak{M}_2} |f_A(\alpha)|^2 h_m(\alpha, N) d\alpha \right| \ll \delta \int_{\mathbb{T}} |f_A(\alpha)|^2 d\alpha \sum_y \lambda_m(y) \leq \delta^2 \widehat{N} \sum_y \lambda_m(y).$$

Thus, for an appropriate choice of $c'$, we have that for all sufficiently large $N$,

$$\left| \int_{\mathfrak{M}_2} |f_A(\alpha)|^2 h_m(\alpha, N) d\alpha \right| \leq \frac{1}{4}\delta^2 \widehat{N} \sum_y \lambda_m(y).$$

Therefore, for sufficiently large values of $N$, we have

$$\left| \int_{\mathfrak{M}_1} |f_A(\alpha)|^2 h_m(\alpha; N) d\alpha \right| \geq \frac{1}{4}\delta^2 \widehat{N} \sum_y \lambda_m(y).$$

For $\alpha \in \mathfrak{M}_{a,g,\langle g\rangle^{-1}\widehat{Q_1}^{-1}}$, where $\langle g\rangle \le \widehat{Q}_3$, we have $h_m(\alpha;N) \ll \frac{1}{\phi(g)}\sum_y \lambda_m(y)$. We conclude that there exists a positive constant $\tilde{c}$ satisfying

$$\sum_{\substack{\langle g\rangle \le \widehat{Q}_3 \\ g \text{ monic}}} \frac{1}{\phi(g)} \sum_{\substack{\langle a\rangle < \langle g\rangle \\ (a,g)=1}} \int_{\mathfrak{M}_{a,g,\langle g\rangle^{-1}\widehat{Q_1}^{-1}}} |f_A(\alpha)|^2 d\alpha \ge \tilde{c}\delta^2 \widehat{N}$$

for all sufficiently large values of $N$.

We can now apply Lemma 10 for $\widehat{K} = \widehat{Q}_3$ and $\eta = \widehat{Q}_1^{-1}$, with the observation that

$$\bigcup_{\substack{\langle a\rangle < \langle g\rangle \\ (a,g)=1}} \mathfrak{M}_{a,g,\langle g\rangle^{-1}\widehat{Q_1}^{-1}} \subset \mathfrak{M}^*_{g,\eta}.$$

We can thus find $g, s \in \mathbb{F}_q[t]$ with $1 \le \langle g\rangle \le \widehat{Q}_3 = c'\delta^{-2}$ and $L$ with

$$\widehat{L} \gg \langle g\rangle^{-1} \min(\widehat{Q}_1, \tilde{c}\delta\widehat{N}) \gg \delta^2 \widehat{Q}_1 = c\delta^4 \frac{\widehat{N}}{N^9\langle m\rangle^4}$$

such that $A \cap \{gl + s : \langle l\rangle < \widehat{L}\} \ge \delta(1 + c_1\tilde{c})\widehat{L}$, where $c_1$ is the constant in Lemma 10.

Let us now set $N_1 = L$, $A' = \{l : \langle l\rangle < \widehat{L}, gl + s \in A\}$, and $m' = gm$. Clearly, if $A - A$ avoids $\{\frac{P+r}{m} : P \text{ monic, irreducible}\}$, then $A' - A'$ avoids $\{\frac{P+r}{m'} : P \text{ monic, irreducible}\}$. □

*Proof of Theorem 2.* Suppose for a contradiction, $A-A$ does not contain elements of the form $P+r$, where $P$ is a monic, irreducible polynomial. We use Lemma 11 to successively construct a sequence of quadruples $(N_i, A_i, \delta_i, m_i)$ such that $A_i \subset \mathbf{G}_{N_i}$, $|A_i| = \delta_i\widehat{N_i}$, and the following hold for every $i$:

(1) $(N_0, A_0, \delta_0, m_0) = (N, A, \delta, 1)$,
(2) $\delta_{i+1} \ge (1 + C_1)\delta_i$,
(3) $\langle m_{i+1}\rangle \le C_2\delta_i^{-2}\langle m_i\rangle$,
(4) $\widehat{N_{i+1}} \ge C_3\left(\frac{\delta_i}{N_i\langle m_i\rangle}\right)^9 \widehat{N}_i$,
(5) $(A_i - A_i) \cap \{\frac{P+r}{m_i} : P \text{ monic, irreducible}\} = \emptyset$.

We claim that if $N$ is sufficiently large depending on $\delta$, we can construct a sequence of $Z = \lfloor C_4\left(\log\frac{1}{\delta} + 1\right)\rfloor$ quadruples, where $C_4$ is a sufficiently large constant to be chosen later, at which point we have a contradiction since $\delta_Z > 1$. Once we have $(N_i, A_i, \delta_i, m_i)$, we can produce $(N_{i+1}, A_{i+1}, \delta_{i+1}, m_{i+1})$ as long as the hypothesis of Lemma 11 is satisfied, i.e. $\widehat{N}_i \ge C_0$, $\delta^{-1} \le \widehat{N}_i^{\kappa}$, and $\langle m_i\rangle \le \widehat{N}_i^{\kappa}$. Since the sequence $(N_i)$ is decreasing and the sequence $(\langle m_i\rangle)$ is increasing, it suffices to show that for $N$ sufficiently large, for any sequence of triples $(N_i, \delta_i, m_i)_{i=0}^{Z}$ satisfying the recursive relations (1),(2),(3) above, we have

- $\widehat{N}_Z \ge C_0$,
- $\langle m_Z\rangle \le \widehat{N}^{\kappa}$,
- $\delta^{-1} \le \widehat{N}^{\kappa}$.

By induction it is easy to see that for every $i \in \{0, \dots, Z\}$,

- $\delta_i \geq (1+C_1)^i \delta$,
- $\langle m_i \rangle \leq C_2^i (1+C_1)^{-i(i-1)} \delta^{-2i}$.

Therefore, for every $i = \{0, \dots, Z\}$,

$$\widehat{N}_{i+1} \geq \frac{C_3}{N^9} \left( \frac{(1+C_1)^i \delta}{C_2^i (1+C_1)^{-i(i-1)} \delta^{-2i}} \right)^9 \widehat{N}_i \geq \frac{C_3}{N^9} (C_2^{-i} (1+C_1)^{i^2} \delta^{2i+1})^9 \widehat{N}_i.$$

Consequently,

$$\widehat{N}_Z \geq \widehat{N} \frac{C_3^Z}{N^{9Z}} \left( C_2^{-Z^2} (1+C_1)^{Z^3/6} \delta^{Z^2} \right)^9.$$

Let us verify that the conditions of Lemma 11 hold for $i = Z$, that is, $\widehat{N}_Z \geq C_0$, $\delta^{-1} \leq \widehat{N}_Z^\kappa$, and $\langle m_Z \rangle \leq \widehat{N}_Z^\kappa$. Notice that since $Z = \lfloor C_4 \left( \log \frac{1}{\delta} + 1 \right) \rfloor$, for an appropriate value of $C_4$, we have

$$\left( C_2^{-Z^2} (1+C_1)^{Z^3/6} \delta^{Z^2} \right)^9 \geq \left( C_2^Z (1+C_1)^{-Z(Z-1)} \delta^{-2Z} \right)^{1/\kappa} \geq \langle m_Z \rangle^{1/\kappa}.$$

Thus, $\widehat{N}_Z \geq \langle m_Z \rangle^{1/\kappa}$ if $\widehat{N} \frac{C_3^Z}{N^{9Z}} \geq 1$, which holds if $\frac{N}{\log N} \geq C_5 \left( \log(1/\delta) + 1 \right)$, where $C_5$ is a large constant. If we choose $C_5$ large enough, then we also have $\widehat{N}_Z \geq C_0$ and $\widehat{N}_Z \geq \delta^{-1/\kappa}$ as well, thus completing the proof of Theorem 2. □

We have a few concluding remarks. An inspection of the proof of Lemma 11 shows that, in order to have a density increment on $\mathbf{G}_{N'}$, it suffices to have few solutions to $a_1 - a_2 = \frac{P+r}{m}$, where $a_1, a_2 \in A$ and $P$ is a monic, irreducible polynomial (as opposed to none at all). Incorporating this observation into the iteration, we have a contradiction even if the number of solutions to $a_1 - a_2 = P + r$ is small enough (as opposed to none at all). Thus, we can actually give a lower bound for the number of such solutions. Precisely, let

$$R_m(A) = \sum_y \sharp\{a_1 - a_2 = y : a_1, a_2 \in A\} \lambda_m(y; N)$$

be the number of weighted solutions. Then, we have

$$R(A) = R_1(A) \geq C(\delta) \frac{\widehat{N}^2}{N^{c(\delta)}},$$

where $C(\delta)$ and $c(\delta)$ are constants depending on $q$ and $\delta$. This bound falls short of the expected order of magnitude $\widehat{N}^2$. It is possible to use alternative methods to show that the number of (weighted) solutions is indeed of order $\widehat{N}^2$ (see e.g. [12, Section 10.2]). Obtaining the optimal dependence of $C(\delta)$ on $\delta$, however, is yet another interesting problem.

## References


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

[2] H. Furstenberg, **Recurrence in Ergodic Theory and Combinatorial Number Theory**, Princeton Univ. Press, 1981.

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

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

[5] Y.-R. Liu & C. V. Spencer, *A prime analogue of Roth's theorem in function fields*, preprint.

[6] M. Rosen, **Number theory in function fields**, Springer-Verlag, 2002.
[7] I. Z. Ruzsa, *On measures on intersectivity*, Acta Math. Hungar. **43** (1984), 335-340.
[8] I. Z. Ruzsa & T. Sanders, *Difference sets and the primes*, Acta Arith. **131** (2008), 281–301.
[9] A. Sárközy, *On difference sets of sequences of integers, I.*, Acta Math. Acad. Sci. Hungar. **31** (1978), 125–149.
[10] A. Sárközy, *On difference sets of sequences of integers, II.*, Ann. Univ. Sci. Budapest. Etvs Sect. Math. **21** (1978), 45–53.
[11] A. Sárközy *On difference sets of sequences of integers, III.*, Acta Math. Acad. Sci. Hungar. **31** (1978), 355–386.
[12] Vaughan, **The Hardy-Littlewood method**, 2nd ed., Cambridge Univ. Press, 1997.

T. H. Lê, School of Mathematics, Institute for Advanced Study, 1 Einstein Drive, Princeton, NJ 08540

*E-mail address*: leth@math.ias.edu

C. V. Spencer, Department of Mathematics, Kansas State University, 138 Cardwell Hall, Manhattan, KS 66506

*E-mail address*: cvs@math.ksu.edu