A GENERALIZATION OF ROTH’S THEOREM IN FUNCTION FIELDS

YU-RU LIU AND CRAIG V. SPENCER

Abstract. Let \( \mathbb{F}_q[t] \) denote the polynomial ring over the finite field \( \mathbb{F}_q \), and let \( S_N \) denote the subset of \( \mathbb{F}_q[t] \) containing all polynomials of degree strictly less than \( N \). For non-zero elements \( r_1, \ldots, r_s \) of \( \mathbb{F}_q \) satisfying \( r_1 + \cdots + r_s = 0 \), let \( D_r(S_N) \) denote the maximal cardinality of a set \( A \subseteq S_N \) which contains no non-trivial solution of \( r_1x_1 + \cdots + r_sx_s = 0 \) with \( x_i \in A \) \((1 \leq i \leq s)\). We prove that \( D_r(S_N) \ll |S_N|/(\log_q |S_N|)^{s-2} \).

1. Introduction

For \( k \in \mathbb{N} = \{1, 2, \ldots\} \), let \( D_3([1, k]) \) denote the maximal cardinality of an integer set \( A \subseteq [1, k] \) containing no non-trivial 3-term arithmetic progression. In a fundamental paper \[6\], Roth proved that \( D_3([1, k]) \ll k/\log \log k \). His result was later improved by Heath-Brown \[2\] and Szemerédi \[7\] to \( D_3([1, k]) \ll k/(\log k)^{\alpha} \) for some small positive constant \( \alpha > 0 \). Recently, Bourgain \[1\] proved that \( D_3([1, k]) \ll k(\log \log k)^2/(\log k)^{2/3} \), which provides the best bound currently known. In this paper, we consider a generalization of Roth’s theorem in function fields.

Let \( \mathbb{F}_q[t] \) denote the ring of polynomials over the finite field \( \mathbb{F}_q \). For \( N \in \mathbb{N} \), let \( S_N \) denote the subset of \( \mathbb{F}_q[t] \) containing all polynomials of degree strictly less than \( N \). For an integer \( s \geq 3 \), let \( r = (r_1, \ldots, r_s) \) be a vector of non-zero elements of \( \mathbb{F}_q \) satisfying \( r_1 + \cdots + r_s = 0 \). A solution \( x = (x_1, \ldots, x_s) \in S_N \) of \( r_1x_1 + \cdots + r_sx_s = 0 \) is said to be trivial if \( x_{j_1} = \cdots = x_{j_l} \) for some subset \( \{j_1, \ldots, j_l\} \subseteq \{1, \ldots, s\} \) with \( r_{j_1} + \cdots + r_{j_l} = 0 \). Otherwise, we say a solution \( x \) is non-trivial. Let \( D_r(S_N) \) denote the maximal cardinality of a set \( A \subseteq S_N \) which contains no non-trivial solution of \( r_1x_1 + \cdots + r_sx_s = 0 \) with \( x_i \in A \) \((1 \leq i \leq s)\), and let \( |S_N| \) denote the cardinality of \( S_N \). In this paper, we prove that

**Theorem 1.** For \( N \in \mathbb{N} \),

\[
D_r(S_N) \ll \frac{|S_N|}{(\log_q |S_N|)^{s-2}}.
\]

Here the implicit constant depends only on \( r \).

---

Date: December 11, 2009.

2000 Mathematics Subject Classification. 11B25, 11T55, 11P55.

Key words and phrases. Roth’s theorem, function fields, circle method.

The research of the first author is supported in part by an NSERC discovery grant.

The research of the second author is supported in part by NSF grant DMS-0601367.

In the special case that $r = (1, -2, 1)$, the number $D_r(S_N)$ denotes the maximal cardinality of a set $A \subseteq S_N$ which contains no non-trivial 3-term arithmetic progression. As a direct consequence of Theorem 1, we have $D_r(S_N) \ll |S_N|/\log_p |S_N|$. We note that this result is sharper than its integer analogue proved by Bourgain. Our improvement comes from a better estimate of an exponential sum in $\mathbb{F}_q[t]$ than in $\mathbb{Z}$ (see Lemma 2). In addition, when $r = (1, -2, 1)$ and $\gcd(2, q) = 1$, by viewing $S_N$ as a vector space over $\mathbb{F}_p$ of dimension $MN$, where $q = p^{3l}$, one can also derive the above bound for $D_r(S_N)$ from the result of Meshulam in [4, Theorem 1.2]. However, for a general $r = (r_1, \ldots, r_s)$, if $r_i \in \mathbb{F}_q \setminus \mathbb{F}_p$ for some $1 \leq i \leq s$, then Meshulam’s method cannot be extended to bound $D_r(S_N)$. In order to prove Theorem 1, we employ a variant of the Hardy-Littlewood circle method for $\mathbb{F}_q[t]$. 

Acknowledgement The authors are grateful to Prof. Trevor Wooley for many valuable discussions during the completion of this work.
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 $|f(k)| \leq cg(k)$, we write $f(k) \ll g(k)$. In this paper, all the implicit constants depend only on $r$.

2. Proof of Theorem 1

For $N \in \mathbb{N}$ and $s \geq 3$, let $r = (r_1, \cdots, r_s)$ and $D_r(S_N)$ be defined as in Section 1. Write $d_r(N) = D_r(S_N)/|S_N|$. For convenience, in what follows, we will write $D(S_N)$ in place of $D_r(S_N)$ and $d(N)$ in place of $d_r(N)$. Hence, to prove Theorem 1, it is equivalent to show that $d(N) \ll 1/N^{s-2}$.

For a set $A \subseteq S_N$, let $T(A) = T_r(A)$ denote the number of solutions of $r_1x_1 + \cdots + r_sx_s = 0$ with $x_i \in A$ $(1 \leq i \leq s)$. Let $1_A$ be the characteristic function of $A$, i.e., $1_A(x) = 1$ if $x \in A$ and $1_A(x) = 0$ otherwise. Define

$$f_i(\alpha) = \sum_{\langle x \rangle < \mathcal{N}} 1_A(x)e(\alpha r_i x) = \sum_{x \in A} e(\alpha r_i x).$$

Then by the orthogonality relation for the exponential function, we have

$$T(A) = \int_{\mathcal{M}} f_1(\alpha)f_2(\alpha) \cdots f_s(\alpha) \, d\alpha. \quad (1)$$

We will estimate $T(A)$ by dividing $\mathcal{M}$ into two parts: the major arc $\mathcal{M}$ defined by $\mathcal{M} = \{\alpha : \text{ord} \alpha < -N\}$ and the minor arc $\mathcal{m} = \mathcal{M} \setminus \mathcal{M}$.

Lemma 2. Suppose that $A \subseteq S_N$ contains no non-trivial solution of $r_1x_1 + \cdots + r_sx_s = 0$ with $x_i \in A$ $(1 \leq i \leq s)$. Then we have

$$\sup_{\alpha \in \mathcal{m}} |f_i(\alpha)| \leq d(N-1)\mathcal{N} - |A|.$$

Proof: For $\alpha \in \mathcal{m}$, let $W = W(\alpha, r_i) = \{y \in S_N : \text{res}(\alpha r_i y) = 0\}$. Since ord $r_i = 0$ and ord $\alpha \geq -N$, we can write ord $(\alpha r_i) = -l$ and $\alpha r_i = \sum_{j \leq -l} b_j t^j$ with $-N \leq -l \leq -1$, $b_j \in \mathbb{F}_q$ $(j \leq -l)$, and $b_{-l} \neq 0$. Then for $y = c_{N-1}t^{N-1} + \cdots + c_0 \in S_N$, the polynomial $y \in W$ if and only if

$$\text{res}(\alpha r_i y) = b_{-l-1}c_{l-1} + b_{-l-1}c_l + \cdots + b_{-N}c_{N-1} = 0.$$

Hence, we have that $W \simeq \mathbb{F}_q^{N-1}$ as a vector space over $\mathbb{F}_q$.

Since ord $(\alpha r_i) \geq -N$, by [3, Lemma 7], we have

$$\sum_{\langle x \rangle < \mathcal{N}} e(\alpha r_i x) = 0.$$

Hence,

$$|W| |f_i(\alpha)| = \left| \sum_{y \in W} \sum_{\langle x \rangle < \mathcal{N}} d(N-1)e(\alpha r_i x) - \sum_{y \in W} \sum_{\langle x \rangle < \mathcal{N}} 1_A(x)e(\alpha r_i x) \right|.$$
For $y \in W$, since $e(\alpha r_i y) = 1$ and $y \in S_N$, we have by a change of variables that
\[
\sum_{(x) < \tilde{N}} 1_A(x)e(\alpha r_i x) = \sum_{(x) < \tilde{N}} 1_A(x)e(\alpha r_i (x + y)) = \sum_{(x) < \tilde{N}} 1_A(x - y)e(\alpha r_i x).
\]
Hence, it follows that
\[
|W| |f_i(\alpha)| = \sum_{(x) < \tilde{N}} \left( \sum_{y \in W} d(N - 1) - \sum_{y \in W} 1_A(x - y) \right)e(\alpha r_i x) \leq \sum_{(x) < \tilde{N}} \left( \sum_{y \in W} d(N - 1) - \sum_{y \in W} 1_A(x - y) \right) = \sum_{(x) < \tilde{N}} \left( d(N - 1)|W| - |W \cap (x - A)| \right).
\]
Since $r_1 + \cdots + r_s = 0$ and $A$ contains no non-trivial solution of $r_1 x_1 + \cdots + r_s x_s = 0$ with $x_i \in A$ ($1 \leq i \leq s$), the set $W \cap (x - A)$ also contains no non-trivial solution of the same equation. Since $W \simeq S_{N-1}$ as a vector space over $\mathbb{F}_q$ and $r_i \in \mathbb{F}_q$ ($1 \leq i \leq s$), any invertible $\mathbb{F}_q$-linear transformation from $W$ to $S_{N-1}$ maps $W \cap (x - A)$ to a subset of $S_{N-1}$ which contains no non-trivial solution of $r_1 x_1 + \cdots + r_s x_s = 0$. This implies that $|W \cap (x - A)| \leq d(N - 1)|W|$. It follows that
\[
|W| |f_i(\alpha)| \leq \sum_{(x) < \tilde{N}} \left( d(N - 1)|W| - |W \cap (x - A)| \right) = d(N - 1)|W|\tilde{N} - |W||A|.
\]
Thus, if $\alpha \in \mathfrak{m}$, we have
\[
|f_i(\alpha)| \leq d(N - 1)\tilde{N} - |A|.
\]
This completes the proof of the lemma.

Now, we are ready to prove Theorem 1.

Proof: (of Theorem 1) Suppose that $A \subseteq S_N$ contains no non-trivial solution of $r_1 x_1 + \cdots + r_s x_s = 0$ with $x_i \in A$ ($1 \leq i \leq s$). We suppose further that $|A|/|S_N| = d(N)$. By (1), we have
\[
T(A) = \int_{\mathfrak{m}} f_1(\alpha)f_2(\alpha) \cdots f_s(\alpha) \, d\alpha = \int_{\mathfrak{m}} f_1(\alpha)f_2(\alpha) \cdots f_s(\alpha) \, d\alpha + \int_{\mathfrak{m}} f_1(\alpha)f_2(\alpha) \cdots f_s(\alpha) \, d\alpha.
\]
If $\alpha \in \mathfrak{m}$ and $x \in S_N$, we have $e(\alpha r_i x) = 1$. It follows that
\[
\int_{\mathfrak{m}} f_1(\alpha)f_2(\alpha) \cdots f_s(\alpha) \, d\alpha = |A|^s \cdot \text{mes} (\mathfrak{m}) = d(N)^s \tilde{N}^{s-1}.
\]
By the orthogonality relation for the exponential function,
\[
\int_{\mathfrak{m}} |f_1(\alpha)|^2 \, d\alpha = |A| = \int_{\mathfrak{T}} |f_2(\alpha)|^2 \, d\alpha.
\]
Hence, by Cauchy’s inequality and Lemma 2, we have
\[
\left| \int_{\mathbb{R}} f_1(\alpha) f_2(\alpha) \cdots f_s(\alpha) \, d\alpha \right| \\
\leq \sup_{\alpha \in \mathbb{R}} |f_3(\alpha) \cdots f_s(\alpha)| \left( \int_{\mathbb{T}} |f_1(\alpha)|^2 \, d\alpha \right)^{1/2} \left( \int_{\mathbb{T}} |f_2(\alpha)|^2 \, d\alpha \right)^{1/2} \tag{4}
\]
\[
\leq d(N) \left( d(N-1) - d(N) \right)^{s-2} \tilde{N}^{s-1}.
\]

By combining (2), (3), and (4), we obtain
\[
T(A) \geq \int_{\mathbb{R}} f_1(\alpha) f_2(\alpha) \cdots f_s(\alpha) \, d\alpha - \left| \int_{\mathbb{R}} f_1(\alpha) f_2(\alpha) \cdots f_s(\alpha) \, d\alpha \right| \\
\geq \left( d(N)^s - d(N)(d(N-1) - d(N))^{s-2} \right) \tilde{N}^{s-1}.
\]

Since \( A \) contains no non-trivial solution of \( r_1 x_1 + \cdots + r_s x_s = 0 \) with \( x_i \in A \) (\( 1 \leq i \leq s \)), there exists a constant \( B = B(r) \) such that
\[
T(A) \leq B|A|^{s-2} = Bd(N)^{s-2} \tilde{N}^{s-2}.
\]

Combining the above two inequalities, we have
\[
d(N)^s - Bd(N)^{s-2} \tilde{N}^{-1} - d(N)(d(N-1) - d(N))^{s-2} \leq 0. \tag{5}
\]

We now claim that there exists a constant \( C = C(r) \geq 1 \) such that for all \( N \in \mathbb{N} \),
\[
d(N) \leq \frac{C^{s-2}}{N^{s-2}}.
\]

This statement will follow by induction. Since \( d(N) \leq 1 \), the cases where \( N \leq C \) follow trivially. Let \( N > C \), and suppose that \( d(N-1) \leq C^{s-2}(N-1)^{2-s} \). We will now verify that \( d(N) \leq C^{s-2}N^{2-s} \). Since \( N^{s-1}(2^N)^{-1/2} \to 0 \) as \( N \to \infty \), without loss of generality, we may assume that \( C^{s-2} \geq B^{1/2}N^{s-1}(2^N)^{-1/2} \) for all \( N \in \mathbb{N} \). Hence, if \( d(N)^2 \leq BN^2 \tilde{N}^{-1} \), since \( \tilde{N} \geq 2^N \), we have
\[
d(N) \leq B^{1/2}N\tilde{N}^{-1/2} \leq B^{1/2}N(2^N)^{-1/2} \leq C^{s-2}N^{2-s},
\]
which gives the desired conclusion. Thus, in what follows, we will assume that \( d(N)^2 > BN^2 \tilde{N}^{-1} \). Since \( Bd(N)^{s-2} \tilde{N}^{-1} < d(N)^s \tilde{N}^{-2} \) and \( N \geq 2 \), by (5), we have
\[
d(N)^{s-2} < d(N)^s(1 - N^{-2}) < d(N)(d(N-1) - d(N))^{s-2}.
\]

Let \( E = E(r) \) be the unique positive number satisfying \( E^{s-2} = 2^{-1} \). By the induction hypothesis for \( d(N - 1) \), the above inequality implies that
\[
Ed(N)^{s-1} + d(N) < d(N - 1) \leq \frac{C^{s-2}}{(N-1)^{s-2}}. \tag{6}
\]
We note that without loss of generality, we can assume that $C \geq E^{-1}(2^{s-1} - 2)$. Then by
the binomial theorem, we have
\[
N^{s-1} = (N - 1)^{s-1} + \binom{s-1}{1}(N - 1)^{s-2} + \binom{s-1}{2}(N - 1)^{s-3} + \ldots + \binom{s-1}{s-1}
\leq (N - 1)^{s-1} + (N - 1)^{s-2}(2^{s-1} - 1)
\leq (N - 1)^{s-1} + (N - 1)^{s-2}(CE + 1).
\]
Then it follows that
\[
\frac{C^{s-2}}{(N - 1)^{s-2}} \leq E\left(\frac{C^{s-2}}{N^{s-2}}\right)^\frac{s-2}{s-1} + \frac{C^{s-2}}{N^{s-2}}.
\]
We note that $Ex^{\frac{s-2}{s-1}} + x$ is an increasing function of $x$. Thus by combining the above
inequality with (6), we conclude that $d(N) \leq C^{s-2}N^{2-s}$. This completes the proof of
Theorem 1.

References

155-158.

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

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

C. V. Spencer, School of Mathematics, Institute for Advanced Study, 1 Einstein Drive,
Princeton, NJ 08540

E-mail address: craigvspencer@gmail.com