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 $\mathcal{S}_N$ denote the subset of $\mathbb{F}_q[t]$ containing all polynomials of degree strictly less than N. For non-zero elements $r_1, \cdots, r_s$ of $\mathbb{F}_q$ satisfying $r_1 + \cdots + r_s = 0$, let $D_{\mathbf{r}}(\mathcal{S}_N)$ denote the maximal cardinality of a set $A \subseteq \mathcal{S}_N$ 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 $D_{\mathbf{r}}(\mathcal{S}_N) \ll |\mathcal{S}_N|/(\log_q |\mathcal{S}_N|)^{s-2}$.

1. Introduction

For $k \in \mathbb{N} = \{1, 2, \cdots\}$, 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 $D_3([1, k]) \ll k(\log\log k)^{1/2}/(\log k)^{1/2}$, 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 $\mathcal{S}_N$ denote the subset of $\mathbb{F}_q[t]$ containing all polynomials of degree strictly less than N. For an integer $s \geq 3$, let $\mathbf{r} = (r_1, \cdots, r_s)$ be a vector of non-zero elements of $\mathbb{F}_q$ satisfying $r_1 + \cdots + r_s = 0$. A solution $\mathbf{x} = (x_1, \cdots, x_s) \in \mathcal{S}_N^s$ 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 $\{j_1, \cdots, j_l\} \subseteq \{1, \cdots, s\}$ with $r_{j_1} + \cdots + r_{j_l} = 0$. Otherwise, we say a solution $\mathbf{x}$ is *non-trivial*. Let $D_{\mathbf{r}}(\mathcal{S}_N)$ denote the maximal cardinality of a set $A \subseteq \mathcal{S}_N$ 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 $|\mathcal{S}_N|$ denote the cardinality of $\mathcal{S}_N$. In this paper, we prove that

Theorem 1. *For $N \in \mathbb{N}$,*
$$D_{\mathbf{r}}(\mathcal{S}_N) \ll \frac{|\mathcal{S}_N|}{(\log_q |\mathcal{S}_N|)^{s-2}}.$$
Here the implicit constant depends only on $\mathbf{r}$.

In the special case that $\mathbf{r} = (1, -2, 1)$, the number $D_{\mathbf{r}}(\mathcal{S}_N)$ denotes the maximal cardinality of a set $A \subseteq \mathcal{S}_N$ which contains no non-trivial 3-term arithmetic progression. As

Date: September 24, 2023.

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.

a direct consequence of Theorem 1, we have $D_{\mathbf{r}}(\mathcal{S}_N) \ll |\mathcal{S}_N|/\log_q|\mathcal{S}_N|$. 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 $\mathbf{r} = (1, -2, 1)$ and $\gcd(2, q) = 1$, by viewing $\mathcal{S}_N$ as a vector space over $\mathbb{F}_p$ of dimension MN, where $q = p^M$, one can also derive the above bound for $D_{\mathbf{r}}(\mathcal{S}_N)$ from the result of Meshulam in [4, Theorem 1.2]. However, for a general $\mathbf{r} = (r_1, \cdots, r_s)$, if $r_i \in \mathbb{F}_q \setminus \mathbb{F}_p$ for some $1 \le i \le s$, then Meshulam's method can not be extended to bound $D_{\mathbf{r}}(\mathcal{S}_N)$. In order to prove Theorem 1, we employ a variant of the Hardy-Littlewood circle method for $\mathbb{F}_q[t]$.

One can also obtain some information about irreducible polynomials from Theorem 1. Let $\mathcal{P}_N$ denote the set of all monic irreducible polynomials in $\mathbb{F}_q[t]$ of degree strictly less than N, and let A_N denote a subset of $\mathcal{P}_N$. By the prime number theorem for $\mathbb{F}_q[t]$ (see [5, Theorem 2.2]), we have $|\mathcal{P}_N| \gg |\mathcal{S}_N|/\log_q|\mathcal{S}_N|$. For $s \ge 4$, Theorem 1 implies that there exists a positive constant $c(\mathbf{r})$ such that whenever $|A_N|/|\mathcal{P}_N| \ge c(\mathbf{r})/(\log_q|\mathcal{S}_N|)^{s-3}$, it follows that A_N contains a non-trivial solution of $r_1x_1 + \cdots + r_sx_s = 0$ with $x_i \in A_N$ $(1 \le i \le s)$. More work is needed to study the case when $s = 3$, and we will return to this matter in a future paper.

We conclude this section by introducing the Fourier analysis of $\mathbb{F}_q[t]$. 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 ∞. We may write each element $\alpha \in \mathbb{K}_\infty$ in the shape $\alpha = \sum_{i \le v} a_i t^i$ for some $v \in \mathbb{Z}$ and $a_i = a_i(\alpha) \in \mathbb{F}_q$ $(i \le v)$. If $a_v \ne 0$, we define $\operatorname{ord}\alpha = v$, and we write $\langle\alpha\rangle$ for $q^{\operatorname{ord}\alpha}$. We adopt the conventions that $\operatorname{ord} 0 = -\infty$ and $\langle 0\rangle = 0$. For a real number R, we let $\widehat{R}$ denote q^R. 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. 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 any Haar measure $d\alpha$ on $\mathbb{K}_\infty$, we normalize it in such a manner that $\int_{\mathbb{T}} 1\, d\alpha = 1$. Thus, if $\mathfrak{M}$ is the subset of $\mathbb{K}_\infty$ defined by $\mathfrak{M} = \{\alpha \in \mathbb{K}_\infty : \operatorname{ord}\alpha < -N\}$, then the measure of $\mathfrak{M}$, $\operatorname{mes}(\mathfrak{M})$, is equal to $\widehat{N}^{-1}$.

We are now equipped 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 $e_q(a_{-1}(\alpha))$. It is often convenient to refer to $a_{-1}(\alpha)$ as being the residue of α, an element of $\mathbb{F}_q$ that we denote by $\operatorname{res}\alpha$. In this guise we have $e(\alpha) = e_q(\operatorname{res}\alpha)$. The orthogonality relation underlying the Fourier analysis of $\mathbb{F}_q[t]$, established in [3, Lemma 1], takes the shape

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

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 $|f(k)| \le cg(k)$, we write $f(k) \ll g(k)$. In this paper, all the implicit constants depend only on $\mathbf{r}$.

2. Proof of Theorem 1

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

For a set $A \subseteq \mathcal{S}_N$, let $T(A) = T_{\mathbf{r}}(A)$ denote the number of solutions of $r_1x_1 + \cdots + r_sx_s = 0$ with $x_i \in A$ $(1 \le i \le s)$. 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

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

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

$$T(A) = \int_{\mathbb{T}} f_1(\alpha) f_2(\alpha) \cdots f_s(\alpha)\, d\alpha. \tag{1}$$

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

Lemma 2. *Suppose that $A \subseteq \mathcal{S}_N$ contains no non-trivial solution of $r_1x_1 + \cdots + r_sx_s = 0$ with $x_i \in A$ $(1 \le i \le s)$. Then we have*

$$\sup_{\alpha \in \mathfrak{m}} \big| f_i(\alpha) \big| \le d(N-1)\widehat{N} - |A|.$$

Proof: For $\alpha \in \mathfrak{m}$, let $W = W(\alpha, r_i) = \big\{ y \in \mathcal{S}_N : e(\alpha r_i y) = 1 \big\}$. Since $\operatorname{ord} r_i = 0$ and $\operatorname{ord} \alpha \ge -N$, we can write $\operatorname{ord}(\alpha r_i) = -l$ and $\alpha r_i = \sum_{j \le -l} b_j t^j$ with $-N \le -l \le -1$, $b_j \in \mathbb{F}_q$ $(j \le -l)$, and $b_{-l} \ne 0$. Then for $y = c_{N-1}t^{N-1} + \cdots + c_0 \in \mathcal{S}_N$, the polynomial $y \in W$ if and only if

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

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

Since $\operatorname{ord}(\alpha r_i) \ge -N$, by [3, Lemma 7], we have

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

Hence,

$$|W|\,|f_i(\alpha)| = \Bigg| \sum_{y \in W} \sum_{\langle x \rangle < \widehat{N}} d(N-1) e(\alpha r_i x) - \sum_{y \in W} \sum_{\langle x \rangle < \widehat{N}} 1_A(x) e(\alpha r_i x) \Bigg|.$$

For $y \in W$, since $e(\alpha r_i y) = 1$ and $y \in \mathcal{S}_N$, we have by a change of variables that

$$\sum_{\langle x\rangle<\widehat{N}} 1_A(x)e(\alpha r_i x) = \sum_{\langle x\rangle<\widehat{N}} 1_A(x)e(\alpha r_i(x+y)) = \sum_{\langle x\rangle<\widehat{N}} 1_A(x-y)e(\alpha r_i x).$$

Hence, it follows that

$$\begin{aligned}
|W|\,|f_i(\alpha)| &= \Bigg|\sum_{\langle x\rangle<\widehat{N}} \Bigg(\sum_{y\in W} d(N-1) - \sum_{y\in W} 1_A(x-y)\Bigg)e(\alpha r_i x)\Bigg| \\
&\leq \sum_{\langle x\rangle<\widehat{N}} \Bigg|\sum_{y\in W} d(N-1) - \sum_{y\in W} 1_A(x-y)\Bigg| \\
&= \sum_{\langle x\rangle<\widehat{N}} \Big|d(N-1)|W| - \big|W\cap(x-A)\big|\Big|.
\end{aligned}$$

Since $r_1 + \cdots + r_s = 0$ and A contains no non-trivial solution of $r_1x_1 + \cdots + r_sx_s = 0$ 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 $W \simeq \mathcal{S}_{N-1}$ 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 $\mathcal{S}_{N-1}$ maps $W\cap(x-A)$ to a subset of $\mathcal{S}_{N-1}$ which contains no non-trivial solution of $r_1x_1 + \cdots + r_sx_s = 0$. This implies that $|W \cap (x-A)| \leq d(N-1)|W|$. It follows that

$$|W|\,|f_i(\alpha)| \leq \sum_{\langle x\rangle<\widehat{N}} \Big(d(N-1)|W| - \big|W\cap(x-A)\big|\Big) = d(N-1)|W|\widehat{N} - |W||A|.$$

Thus, if $\alpha \in \mathfrak{m}$, we have

$$|f_i(\alpha)| \leq d(N-1)\widehat{N} - |A|.$$

This completes the proof of the lemma.

Now, we are ready to prove Theorem 1.

Proof: (of Theorem 1) Suppose that $A \subseteq \mathcal{S}_N$ contains no non-trivial solution of $r_1x_1 + \cdots + r_sx_s = 0$ with $x_i \in A$ $(1 \leq i \leq s)$. We suppose further that $|A|/|\mathcal{S}_N| = d(N)$. By (1), we have

$$\begin{aligned}
T(A) &= \int_{\mathbb{T}} f_1(\alpha)f_2(\alpha)\cdots f_s(\alpha)\,d\alpha \\
&= \int_{\mathfrak{M}} f_1(\alpha)f_2(\alpha)\cdots f_s(\alpha)\,d\alpha + \int_{\mathfrak{m}} f_1(\alpha)f_2(\alpha)\cdots f_s(\alpha)\,d\alpha.
\end{aligned} \tag{2}$$

If $\alpha \in \mathfrak{M}$ and $x \in \mathcal{S}_N$, we have $e(\alpha r_i x) = 1$. It follows that

$$\int_{\mathfrak{M}} f_1(\alpha)f_2(\alpha)\cdots f_s(\alpha)\,d\alpha = |A|^s \cdot \mathrm{mes}(\mathfrak{M}) = d(N)^s\,\widehat{N}^{s-1}. \tag{3}$$

By the orthogonality relation for the exponential function,

$$\int_{\mathbb{T}} |f_1(\alpha)|^2\,d\alpha = |A| = \int_{\mathbb{T}} |f_2(\alpha)|^2\,d\alpha.$$

Hence, by Cauchy's inequality and Lemma 2, we have

$$\begin{aligned}
&\left| \int_{\mathfrak{m}} f_1(\alpha) f_2(\alpha) \cdots f_s(\alpha)\, d\alpha \right| \\
&\le \sup_{\alpha \in \mathfrak{m}} \left| f_3(\alpha) \cdots f_s(\alpha) \right| \left(\int_{\mathbb{T}} |f_1(\alpha)|^2 \, d\alpha \right)^{1/2} \left(\int_{\mathbb{T}} |f_2(\alpha)|^2 \, d\alpha \right)^{1/2} \\
&\le d(N) \big(d(N-1) - d(N) \big)^{s-2} \widehat{N}^{s-1}.
\end{aligned} \tag{4}$$

By combining (2), (3), and (4), we obtain

$$\begin{aligned}
T(A) &\ge \int_{\mathfrak{M}} f_1(\alpha) f_2(\alpha) \cdots f_s(\alpha)\, d\alpha - \left| \int_{\mathfrak{m}} f_1(\alpha) f_2(\alpha) \cdots f_s(\alpha)\, d\alpha \right| \\
&\ge \Big(d(N)^s - d(N) \big(d(N-1) - d(N) \big)^{s-2} \Big) \widehat{N}^{s-1}.
\end{aligned}$$

Since A contains no non-trivial solution of $r_1 x_1 + \cdots + r_s x_s = 0$ with $x_i \in A$ $(1 \le i \le s)$, there exists a constant $B = B(\mathbf{r})$ such that

$$T(A) \le B|A|^{s-2} = B d(N)^{s-2} \widehat{N}^{s-2}.$$

Combining the above two inequalities, we have

$$d(N)^s - B d(N)^{s-2} \widehat{N}^{-1} - d(N) \big(d(N-1) - d(N) \big)^{s-2} \le 0. \tag{5}$$

We now claim that there exists a constant $C = C(\mathbf{r}) \ge 1$ such that for all $N \in \mathbb{N}$,

$$d(N) \le \frac{C^{s-2}}{N^{s-2}}.$$

This statement will follow by induction. Since $d(N) \le 1$, the cases where $N \le C$ follow trivially. Let $N > C$, and suppose that $d(N-1) \le C^{s-2}(N-1)^{2-s}$. We will now verify that $d(N) \le C^{s-2} N^{2-s}$. Since $N^{s-1}(2^N)^{-1/2} \to 0$ as $N \to \infty$, without loss of generality, we may assume that $C^{s-2} \ge B^{1/2} N^{s-1} (2^N)^{-1/2}$ for all $N \in \mathbb{N}$. Hence, if $d(N)^2 \le B N^2 \widehat{N}^{-1}$, since $\widehat{N} \ge 2^N$, we have

$$d(N) \le B^{1/2} N \widehat{N}^{-1/2} \le B^{1/2} N (2^N)^{-1/2} \le C^{s-2} N^{2-s},$$

which gives the desired conclusion. Thus, in what follows, we will assume that $d(N)^2 > B N^2 \widehat{N}^{-1}$. Since $B d(N)^{s-2} \widehat{N}^{-1} < d(N)^s N^{-2}$ and $N \ge 2$, by (5), we have

$$d(N)^s 2^{-1} < d(N)^s (1 - N^{-2}) < d(N) \big(d(N-1) - d(N) \big)^{s-2}.$$

Let $E = E(\mathbf{r})$ be the unique positive number satisfying $E^{s-2} = 2^{-1}$. By the induction hypothesis for $d(N-1)$, the above inequality implies that

$$E d(N)^{\frac{s-1}{s-2}} + d(N) < d(N-1) \le \frac{C^{s-2}}{(N-1)^{s-2}}. \tag{6}$$

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

$$\begin{aligned} N^{s-1} &= (N-1)^{s-1} + \binom{s-1}{1}(N-1)^{s-2} + \binom{s-1}{2}(N-1)^{s-3} + \cdots + \binom{s-1}{s-1} \\ &\leq (N-1)^{s-1} + (N-1)^{s-2}(2^{s-1}-1) \\ &\leq (N-1)^{s-1} + (N-1)^{s-2}(CE+1). \end{aligned}$$

Then it follows that

$$\frac{C^{s-2}}{(N-1)^{s-2}} \leq E\left(\frac{C^{s-2}}{N^{s-2}}\right)^{\frac{s-1}{s-2}} + \frac{C^{s-2}}{N^{s-2}}.$$

We note that $Ex^{\frac{s-1}{s-2}} + x$ 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

[1] J. Bourgain, *On triples in arithmetic progression*, Geom. Funct. Anal. **9** (1999), 968-984.

[2] D. R. Heath-Brown, *Integer sets containing no arithmetic progressions*, J. London Math. Soc. **35** (1987), 385-394.

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

[4] R. Meshulam, *On subsets of finite abelian groups with no 3-term arithmetic progressions*, J. Combin. Theory Ser. A **71** (1995), 168-172.

[5] M. Rosen, *Number theory in function fields*, GTM **210**, Springer (2002).

[6] R. F. Roth, *On certain sets of integers*, J. London Math. Soc. **28** (1953), 104-109.

[7] E. Szemerédi, *Integer sets containing no arithmetic progressions*, Acta Math. Hungar. **56** (1990), 155-158.

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

Email address: yrliu@math.uwaterloo.ca

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

Email address: craigvspencer@gmail.com