A GENERALIZATION OF SÁRKÖZY'S THEOREM IN FUNCTION FIELDS

PIERRE-YVES BIENVENU, THÁI HOÀNG LÊ, AND GAUREE WATHODKAR

Abstract. Sárközy's theorem says that if $A \subset \mathbb{Z}$ has positive upper asymptotic density, then there are distinct $a_1, a_2 \in A$ and $n \in \mathbb{Z}$ such that $a_1 - a_2 = n^2$. The same is true if n^2 is replaced by $F(n)$ for any polynomial $F \in \mathbb{Z}[x]$ with constant term zero. Green proved an $\mathbb{F}_q[t]$-analog of Sárközy's theorem with strong quantitative bounds, but required a technical condition on the number of roots of the polynomial $F \in \mathbb{F}_q[x]$. This condition was recently removed by Li and Sauermann. In this paper, we generalize Green's argument to accommodate equations in more variables in $\mathbb{F}_q[t]$, while pointing out that the technical condition can be removed by means of a simple observation.

1. Introduction

The *upper asymptotic density* of a set $A \subset \mathbb{Z}$ is given by

$$\overline{d}(A) = \limsup_{N\to\infty} \frac{|A \cap \{1, \dots, N\}|}{N}.$$

Sárközy [13] proved that if $\overline{d}(A) > 0$, then there are distinct $a_1, a_2 \in A$ and $n \in \mathbb{Z}$ such that $a_1 - a_2 = n^2$. The same conclusion holds when n^2 is replaced by $F(n)$, where $F \in \mathbb{Z}[x]$ is a polynomial with constant term zero. More generally, the conclusion holds if and only if F is an *intersective polynomial*, that is, for any $d \in \mathbb{Z}^+$, there exists $n \in \mathbb{Z}$ such that $d|F(n)$. This condition is easily seen to be necessary, by taking $A = d\mathbb{Z}$. We refer the reader to the survey [5] for a discussion on sets enjoying the same property as $\{n^2\}$.

The finitary version of (the generalization of) Sárközy's theorem is as follows:

Theorem 1 (Generalized Sárközy)**.** *Let $F \in \mathbb{Z}[x]$ be intersective. For $N \in \mathbb{N}$, let $\alpha_F(N)$ be the maximum size of a subset $A \subset \{1, \dots, N\}$ that do not contain distinct elements a_1, a_2 such that $a_1 - a_2 = F(n)$ for some $n \in \mathbb{Z}$. Then $\alpha_F(N) = o(N)$ as $N \to \infty$.*

To date, the best bound is $\alpha_F(N) \leq C\frac{N}{(\log N)^{c \log\log\log N}}$ for some constants $C, c > 0$, where C depends on F and c depends on $\deg F$. It is due to Arala [1], building on previous works of Bloom-Maynard [2] and Rice [9].

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a power of a prime p. Let $\mathbb{F}_q[t]$ be the ring of polynomials with coefficients in $\mathbb{F}_q$ in an indeterminate t. Also, let $G_n \subset \mathbb{F}_q[t]$ be the set of all polynomials in $\mathbb{F}_q[t]$ with degree less than n. In [6], Liu and the second author of the present paper studied the analogue of Sárközy's theorem in $\mathbb{F}_q[t]$ and proved the following, using the circle method.

Theorem 2 (Lê-Liu)**.** *Let $A \subset G_n$ with $|A| \gg q^n(\log n)^7/n$. Then, there are distinct polynomials $a_1(t), a_2(t) \in A$ such that $a_1(t) - a_2(t) = (b(t))^2$ for some $b(t) \in \mathbb{F}_q[t]$.*

Using the polynomial method developed by Croot-Lev-Pach [12], Green [4] gave a much stronger bound than Theorem 2.

Theorem 3 (Green). *Let $F(x) = \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_\ell\, x^\ell \in \mathbb{F}_q[x]$ be a polynomial of degree ℓ with constant term zero such that the number of roots of F in $\mathbb{F}_q[t]$ is coprime to q. Then there is a constant $c = c(q,\ell) \in (0,1)$ such that if $A \subset G_n$ has cardinality greater than $2q^{cn}$, then there are distinct polynomials $a_1(t), a_2(t) \in A$ such that $a_1(t) - a_2(t) = F(b(t))$ for some $b(t) \in \mathbb{F}_q[t]$.*

In particular, Theorem 3 applies when $F(x) = x^\ell$, but does not apply when $F(x) = x^{\ell-p+1}(x-1)\cdots(x-p+1)$. The condition on the number of roots of F is not quite satisfactory, and is conceivably an artifact of the proof. This condition is not needed qualitatively (see [7, Section 6]). Recently, Li and Sauermann [8] showed that the root condition on F can indeed be removed.

Theorem 4 (Li-Sauermann). *Theorem 3 remains valid without the condition on the number of roots of F, at the cost of adjusting $2q^{cn}$ to $c'q^{cn}$, for some constant $c' = c'(q,\ell) > 0$.*

Li and Sauermann proved Theorem 4 by generalizing a key lemma of Green (Lemma 10 below). Alternatively, Theorem 4 follows from the following observation. Green only considered $F \in \mathbb{F}_q[x]$, but an inspection shows that the same proof works for $F \in \mathbb{F}_q[t][x]$, at the cost of adjusting $2q^{cn}$ to $c'q^{cn}$. (Note that when $F \in \mathbb{F}_q[x]$, any root in $\mathbb{F}_q[t]$ of F must necessarily be in $\mathbb{F}_q$.) Now, suppose

$$F(x) = \alpha_1(t)x + \alpha_2(t)x^2 + \cdots + \alpha_\ell(t)x^\ell \in \mathbb{F}_q[t][x]$$

is an arbitrary polynomial with constant term zero (and no assumption on the number of roots). Then

$$F(t^m x) = \alpha_1(t)t^m x + \alpha_2(t)t^{2m}x^2 + \cdots + \alpha_\ell(t)t^{\ell m}x^\ell.$$

If $m > \max_{1\le i\le \ell} \deg_t \alpha_i(t)$, then the degrees of t in the non-zero terms $\alpha_i(t)t^{im}x^i$ are all distinct. Therefore, the only root in $\mathbb{F}_q[t]$ of $F(t^m x)$ is $x = 0$. Applying Theorem 3 with $F(t^m x)$ in place of F, we see that any set $A \subset G_n$ with cardinality greater than $c'q^{cn}$, must contain distinct elements $a_1(t), a_2(t)$ such that $a_1(t) - a_2(t) = F(t^m b(t))$ for some $b(t) \in \mathbb{F}_q[t]$. Hence, Theorem 4 follows.

For example, if $F(x) = x^{\ell-p+1}(x-1)\cdots(x-p+1)$, then $F(tx) = t^{\ell-p+1}x^{\ell-p+1}(tx-1)\cdots(tx-p+1)$ has only one root $x = 0$ in $\mathbb{F}_q[t]$.

In this paper, we generalize Theorems 3 and 4 to equations in more variables.

Theorem 5. *Let r, k, d and ℓ be integers satisfying $k > 2r^2(1-1/\ell^2)$. Suppose $c_1, \ldots, c_k \in \mathbb{F}_q[t]$ have degree at most d and satisfy $\sum_{i=1}^k c_i = 0$. Let $F(x) \in \mathbb{F}_q[t][x]$ be a polynomial of degree ℓ with constant term zero. Then there exist constants $c = c(q,r,k,\ell) \in (0,1)$ and $c' = c'(q,r,k,d,F) > 0$ such that the following holds: Any $A \subset G_n$ satisfying $|A| > c' \cdot q^{cn}$ must contain a nontrivial solution to*

$$c_1 a_1^r + \cdots + c_k a_k^r = F(b) \tag{1}$$

for some $b \in \mathbb{F}_q[t]$.

By a trivial solution we mean $(a_1, \dots, a_k) = (a, \dots, a)$ for some $a \in A$ and $b = 0$. Theorems 3 and 4 are a special case of Theorem 5 when $r = 1$ and $k = 2$.

Theorem 5 was inspired by the following result [3] of the first author of the present paper.

Theorem 6 (Bienvenu). *Let, r, k and d be integers satisfying $k \geq 2r^2 + 1$. Suppose $c_1, \dots, c_k \in \mathbb{F}_q[t]$ have degree at most d and $\sum_{i=1}^{k} c_i = 0$. Then there exist constants $c(r, q) \in (0, 1)$ and $c' = c'(q, r, k, d) > 0$ such that the following holds: Any $A \subset G_n$ with $|A| \geq c' \cdot q^{cn}$ must contain a non-trivial solution to*

$$c_1 a_1^r + \cdots + c_k a_k^r = 0. \tag{2}$$

Again, by a trivial solution we mean $(a_1, \dots, a_k) = (a, \dots, a)$ for some $a \in A$.

Note that Theorem 6 provides a stronger conclusion than Theorem 5, but the number of variables required in Theorem 6 is greater than the number of variables required in Theorem 5. Therefore, Theorems 5 and 6 do not subsume each other.

The organization of the paper is as follows. In Section 2, we deduce Theorem 5 from a general statement (Proposition 7). In Section 3, we prove Proposition 7 using the Croot-Lev-Pach polynomial method.

2. Proof of Theorem 5

Theorem 5 is a consequence of the following proposition, which is a hybrid of [3, Proposition 2] and [4, Theorem 1.3].

Proposition 7. *Let m, n, n', d' and d'' be integers with $0 < m \leq n'$. Let $\Psi : (\mathbb{F}_q^n)^k \to \mathbb{F}_q^{n'}$ be a polynomial map with degree at most d'*[1] *and $\Phi : \mathbb{F}_q^m \to \mathbb{F}_q^{n'}$ be a polynomial map with degree at most d''. Let $A \subset \mathbb{F}_q^n$. Assume that*

(1) For any $(a_1, \dots, a_k) \in A^k$, $\Psi(a_1, \dots, a_k) = 0$ if and only if $a_1 = \cdots = a_k = a$ for some $a \in A$,
(2) $|\Phi^{-1}(0)|$ is coprime to q, and
(3) $\Psi(A^k) \cap \mathrm{Im}(\Phi) = \{0\}$.

Then,

$$|A| \leq k \cdot \inf_{0<x<1} \frac{(1 + x + \cdots + x^{q-1})^n}{x^{\left(\frac{q-1}{k}\right)\left(n' - \frac{m}{d''}\right)d}}. \tag{3}$$

Proof of Theorem 5 assuming Proposition 7. By the observation made in the introduction, we can assume that $F(x)$ has only one root $x = 0$ in $\mathbb{F}_q[t]$.

We identify G_n with $\mathbb{F}_q^n$, by identifying each polynomial $g = g_0 + g_1 t + \cdots + g_{n-1} t^{n-1} \in G_n$ with the vector $(g_0, g_1, \dots, g_{n-1}) \in \mathbb{F}_q^n$. Then $g^r \in G_{(n-1)r+1}$ corresponds to the vector $(g_0^r, r g_0^{r-1} g_1, \dots, g_{n-1}^r) \in \mathbb{F}_q^{r(n-1)+1}$. Note that each component of g^r is a polynomial of degree at most r in $g_0, g_1, \dots, g_{n-1}$.

[1] That is, $\Psi(x_1, x_2, \dots, x_{nk}) = (\psi_1(x_1, x_2, \dots, x_{nk}), \dots, \psi_{n'}(x_1, x_2, \dots, x_{nk}))$, where each ψ_i is a polynomial of degree at most d'.

Under this identification, the map $(a_1, \dots, a_k) \mapsto \sum_{i=1}^k c_i a_i^r$ induces a polynomial map

$$\Psi : (\mathbb{F}_q^n)^k \to \mathbb{F}_q^{n'}$$
$$(a_1, \dots, a_k) \mapsto (\psi_1(a_1, \dots, a_k), \dots, \psi_{n'}(a_1, \dots, a_k))$$

where $n' := (n-1)r + d + 1$ and $\psi_i(a_1, \dots, a_k)$ is the coefficient of t^{i+1} in $\sum_{i=1}^k c_i a_i^r$. Moreover, the degree of each ψ_i is at most $d' := r$.

Suppose

$$F(x) = \alpha_1(t)x + \alpha_2(t)x^2 + \cdots + \alpha_\ell(t)x^\ell \in \mathbb{F}_q[t][x].$$

Let $u = \max\{\deg_t \alpha_i : i = 1, \dots, \ell\}$ and $m = \lfloor \frac{n'-u}{\ell} \rfloor + 1$. If $h = h_0 + h_1 t + \cdots + h_{m-1}t^{m-1} \in G_m$, then

$$F(h_0 + h_1 t + \cdots + h_{m-1}t^{m-1})$$
$$= f_0(h_0, \dots, h_{m-1}) + f_1(h_0, \dots, h_{m-1})t + \cdots + f_{n'-1}(h_0, \dots, h_{m-1})t^{n'-1} \in G_{n'}$$

where $f_i \in \mathbb{F}_q[x_1, \dots, x_m]$ are polynomials with degrees at most ℓ and $f_i(0) = 0$, for $0 \le i \le n' - 1$.

Consider the polynomial map

$$\Phi : \mathbb{F}_q^m \to \mathbb{F}_q^{n'},$$
$$(h_0, \dots, h_{m-1}) \mapsto (f_0(h_0, \dots, h_{m-1}), \dots, f_{n'-1}(h_0, \dots, h_{m-1})).$$

Then Φ has degree at most $d'' := l$. Suppose now $A \subset G_n$ is a subset that does not contain a nontrivial solution to $c_1 a_1^r + \cdots + c_k a_k^r = F(b)$. We apply Proposition 7 to Ψ, Φ and the set A. The first and third condition are satisfied by the assumption on A. The second condition is satisfied by the assumption on the number of roots in $\mathbb{F}_q[t]$ of F.

Substituting $n' = (n-1)r + d + 1, d' = r, d'' = \ell$ and $m = \lfloor \frac{n'-u}{\ell} \rfloor + 1$, (3) implies that

$$|A| \le k \inf_{0<x<1} \frac{(1 + x + \cdots + x^{q-1})^n}{x^{\frac{q-1}{k}\left(1-\frac{1}{\ell^2}\right)nr^2 + O_{q,r,k,d,F}(1)}}.$$

Writing $E := (q-1)r^2(1 - 1/\ell^2)k^{-1}$, then we have $E < (q-1)/2$ since $k > 2r^2(1 - 1/\ell^2)$.

Let $f(x) = (1 + x + \cdots + x^{q-1})x^{-E}$. Then $f'(1) = \sum_{i=0}^{q-1}(i - E) > 0$, so f is increasing on some interval $(1 - \epsilon, 1)$. Therefore, $\inf_{0<x<1} f(x) < f(1) = q$. Let $x \in (0, 1)$ be such that $f(x) < q$, then

$$|A| \le k \cdot x^{O_{q,r,k,d,F}(1)} \cdot (f(x))^n \le c' \cdot q^{cn}$$

for some constants $c = c(q, r, k, \ell) \in (0, 1)$ and $c'(q, r, k, d, F) > 0$, as desired. □

3. Proof of Proposition 7

The remainder of the paper is devoted to the proof of Proposition 7. First we recall some preliminaries. The first one is the notion of slice rank introduced by Tao [10] (see also [11, Definition 6.5.2]).

Definition 8 (Slice rank of a function)**.** Let A be a finite set and $\mathbb{F}$ be a field. A function $f : A^k \to \mathbb{F}$ is said to have *slice rank* 1 if it can be written as

$$f(x_1, x_2, \dots, x_k) = g(x_j)h(x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_k),$$

for some $j \in \{1, \dots, k\}$ and some nonzero functions $g : A \to \mathbb{F}$ and $h : A^{k-1} \to \mathbb{F}$.

The *slice rank* of a function $F : A^k \to \mathbb{F}$ is the minimum integer r such that F can be written as a sum of r slice rank 1 functions.

Tao [10, Lemma 1] (see also [11, Lemma 6.5.5]) also proved the following fact regarding the slice rank of a diagonal function.

Lemma 9 (Tao). *Let A be a finite set. Suppose a function $f : A^k \mapsto \mathbb{F}$ satisfies $f(a_1, \dots, a_k) \neq 0$ if and only if $a_1 = a_2 = \cdots = a_k$. Then f has slice rank $|A|$.*

Our next tool is the following key lemma by Green [4, Lemma 3.1], which says that the image of a polynomial map can be realized as the support of a low degree polynomial.

Lemma 10 (Green). *Let $\Phi : \mathbb{F}_q^m \to \mathbb{F}_q^n$ be a polynomial map with degree at most d and $|\Phi^{-1}(0)|$ is coprime to q. Then there exists a polynomial $P \in \mathbb{F}_q[x_1, x_2, \dots, x_n]$ whose degree in every single variable is at most $(q-1)$ such that*

(1) $\deg(P) \leq (q-1)\left(n - \frac{m}{d}\right)$,
(2) P is supported on $\mathrm{Im}(\Phi)$ (i.e., $P(x) = 0$ if $x \notin \mathrm{Im}(\Phi)$), and
(3) $P(0) \neq 0$.

We are now ready to prove Proposition 7.

Proof of Proposition 7. Applying Lemma 10 to the polynomial map $\Phi : \mathbb{F}_q^m \to \mathbb{F}_q^{n'}$, we find that there exists a polynomial $P \in \mathbb{F}_q[x_1, x_2, \dots, x_{n'}]$ whose degree in every single variable is at most $(q-1)$ such that

(1) $\deg(P) \leq (q-1)\left(n' - \frac{m}{d''}\right)$,
(2) P is supported on $\mathrm{Im}(\Phi)$, and
(3) $P(0) \neq 0$.

We now consider the function $f(a_1, \dots, a_k) := P(\Psi(a_1, \dots, a_k))$ from A^k to $\mathbb{F}_q$.
Claim: $f(a_1, \dots, a_k) \neq 0$ if and only if $a_1 = \cdots = a_k = a$ for some $a \in A$.

Indeed, for any $a \in A$, $f(a, \dots, a) = P(\Psi(a, \dots, a)) = P(0) \neq 0$. Conversely, suppose the a_i's are not all equal. By the assumption on Ψ, we have $\Psi(a_1, \dots, a_k) \neq 0$. Since $\Psi(A^k)$ and $\mathrm{Im}(\Phi)$ only intersect at 0, we have that $\Psi(a_1, \dots, a_k) \notin \mathrm{Im}(\Phi)$. Therefore, $P(\Psi(a_1, \dots, a_k)) = 0$ since P is supported on $\mathrm{Im}(\Phi)$, and the claim is proved.

By Lemma 9, the slice rank of f is $|A|$. We will now estimate the slice rank of f in a different way. Note that f is a polynomial of degree at most $\deg P \cdot \deg \Psi \leq (q-1)\left(n' - \frac{m}{d''}\right) d' := D$. For each $i = 1, \dots, k$, let $a_i = (a_{i,1}, \dots, a_{i,n})$. Then $f(a_1, \dots, a_k)$ can be written as a sum of monomials of the form

$$a_{1,1}^{\alpha_{1,1}} a_{1,2}^{\alpha_{1,2}} \cdots a_{1,n}^{\alpha_{1,n}} a_{2,1}^{\alpha_{2,1}} \cdots x_{2,n}^{\alpha_{2,n}} \cdots x_{k,1}^{\alpha_{k,1}} \cdots x_{k,n}^{\alpha_{k,n}}$$

where $\alpha_{i,j} \leq q-1$ and $\sum_{i=1}^{k} \sum_{j=1}^{n} \alpha_{i,j} \leq D$.

By the pigeonhole principle, there exists $i \in \{1, \dots, k\}$ such that $\sum_{j=1}^{n} \alpha_{i,j} \leq D/k$. Hence, the slice rank of f is at most kN, where N is the number of tuples $(\alpha_1, \alpha_2, \dots, \alpha_n)$ such that $\alpha_j \leq q-1$ for all $j \in \{1, \dots, n\}$ and $\sum_{j=1}^{n} \alpha_j \leq D/k$. It remains to estimate N.

We have

$$N = \sum_{\substack{u_0,u_1,\ldots,u_{q-1}\geq 0 \\ u_0+u_1+\cdots+u_{q-1}=n \\ u_1+2u_2+\cdots+(q-1)u_{q-1}\leq D/k}} \frac{n!}{u_0!u_1!\ldots u_{q-1}!}.$$

Note that N equals the sum of all the coefficients of x^v with $v \leq D/k$ in the expansion of $(1+x+\cdots+x^{q-1})^n$. Let $x \in (0,1)$ be arbitrary. When $v \leq D/k$, we have $x^v \geq x^{D/k}$, so

$$N \cdot x^{D/k} \leq (1+x+\cdots+x^{q-1})^n.$$

Therefore, the slice rank of f is

$$|A| \leq kN \leq k \cdot \inf_{0<x<1} \frac{(1+x+\cdots+x^{q-1})^n}{x^{\left(\frac{q-1}{k}\right)\left(n'-\frac{m}{d''}\right)d}},$$

as desired. □

Acknowledgments. The second and third authors are supported by National Science Foundation Grant DMS-2246921. The second author is also supported by a travel gift from the Simons Foundation.

References

[1] N. Arala, *A maximal extension of the Bloom-Maynard bound for sets with no square differences*, Funct. Approx. Comment. Math. 71 (2024), no. 2, 271–296.

[2] T. Bloom and J. Maynard, *A new upper bound for sets with no square differences*, Compositio Math. 158 (2022), 1777–1798.

[3] P.-Y. Bienvenu, *Polynomial equations in $\mathbb{F}_q[t]$*, Q. J. Math. 68 (2017), no. 4, 1395–1398.

[4] B. Green, *Sárközy's Theorem in Function Fields*, The Quarterly Journal of Mathematics 68 (2017), no. 1, 237–242.

[5] T. H. Lê, *Problems and results on intersective sets*, Combinatorial and additive number theory – CANT 2011 and 2012, 115–128. Springer Proc. Math. Stat., 101

[6] T. H. Lê and Y.-R. Liu, *On sets of polynomials whose difference set contains no squares*, Acta Arithmetica 161 (2013), 127–143.

[7] T. H. Lê, Y.-R. Liu, and T. D. Wooley, *Equidistribution of polynomial sequences in function fields, with applications*, preprint, https://arxiv.org/abs/1311.0892v2

[8] A. Li and L. Sauermann, *Sárközy's Theorem in Various Finite Field Settings*, SIAM Journal on Discrete Mathematics 38 (2024), no. 2, 1409–1416.

[9] A. Rice, *A maximal extension of the best-known bounds for the Furstenberg-Sárközy Theorem*, Acta Arith. 187 (2019), 1–41.

[10] T. Tao, *A symmetric formulation of the Croot-Lev-Pach-Ellenberg-Gijswijt capset bound*, Blog post (2016). Available at https://terrytao.wordpress.com/2016/05.

[11] Y. Zhao, *Graph Theory and Additive Combinatorics*, Cambridge University Press, 2023.

[12] E. Croot, V. F. Lev, and P. P. Pach, *Progression-free sets in $\mathbb{Z}_4^n$ are exponentially small*, Annals of Mathematics (2) 185 (2017), no. 1, 331–337.

[13] A. Sárközy, *On difference sets of sequences of integers. I*, Acta. Math. Hungar. 31(1-2) (1978), 125–149.

Institute for Discrete Mathematics and Geometry (E104), TU Vienna, 08-10 Wiedner Hauptstrasse, 1040 Vienna, Austria
Email address: pierre.bienvenu@tuwien.ac.at

Department of Mathematics, University of Mississippi, University, MS 38677, USA
Email address: leth@olemiss.edu
Email address: gaukiwa@gmail.com