1

Problems and results on intersective sets

Thái Hoàng Lê

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

1.1 Intersective sets in the integers

In the late 1970s, Sárközy and Furstenberg independently proved the following result, now commonly known as Sárközy's theorem, which had previously been conjectured by Lovász:

Theorem 1 (Sárközy [45], Furstenberg [14, 15]). *If A is a subset of positive upper density*[1] *of $\mathbf{Z}$, then there are two distinct elements of A whose difference is a perfect square.*

Furstenberg used ergodic theory, while Sárközy's proof is inspired by Roth's proof of Roth's theorem[2] and employs the circle method. Kamae and Mendès France [22] also came up with another approach shortly after that. We will discuss about all these approaches in turn. To date, simplest proofs of Sárközy's theorem are due to Green [17] and Lyall [33]. Very recently, Green, Tao and Ziegler [47] gave yet another very simple and elementary proof of this result.

Sárközy went on and proved in [46] that the same conclusion holds if we replace the set of squares by $\{n^2 - 1 : n > 1\}$ and $\{p - 1 : p \text{ prime}\}$, as well as $\{p + 1 : p \text{ prime}\}$, confirming conjectures of Erdős. What are the reasons that make the set of squares and the set of primes shifted by 1 so special, and are there other sets having this property? Clearly, this property is not enjoyed by the polynomials $2n + 1$ or $n^2 + 1$ due to obvious obstructions modulo 2 and 3, respectively. It is also easy to see that there are no translates of the primes other than $\{p - 1\}$ and $\{p + 1\}$ having this property. Let us first make the following:

[1] If $A \subset \mathbf{Z}$, then the upper density of A is defined by $\overline{d}(A) = \overline{\lim}_{N\to\infty} \frac{\sharp A \cap \{1,\dots,N\}}{N}$.

[2] Roth's theorem says that a set of positive upper density must contain non-trivial 3-term arithmetic progressions.

Definition 1. *A set $H \subset \mathbf{Z}^+$ is called intersective*[3] *if whenever A is a subset of positive upper density of $\mathbf{Z}$, we have $A - A \cap H \neq \emptyset$.*

Thus Sárközy's results say that the sets $\{n^2 : n > 0\}$ and $\{p - 1 : p \text{ prime}\}$ are intersective. We are also interested in the following quantitative aspect of the problem. For a set $H \subset \mathbf{Z}^+$, we denote by $D(H, N)$ the maximal size of a subset A of $\{1, \ldots, N\}$ such that the difference set $A - A$ does not contain any element of H. Then it is not difficult to see that H is intersective if and only if $D(H, N) = o(N)$. If we have an explicit estimate for $D(H, N)$, then we can still conclude that $A - A \cap H \neq \emptyset$ for certain sets A not necessarily having positive density, such as the primes.

Let us call a polynomial $h \in \mathbf{Z}[x]$ an *intersective polynomial (of the first kind)* if the set $\{h(n)\} \cap \mathbf{Z}^+$ is intersective. Let us call h an *intersective polynomial of the second kind* if the set $\{h(p) : p \text{ prime}\} \cap \mathbf{Z}^+$ is intersective [4]. Thus Sárközy's results say that the polynomial $h(n) = n^2$ is intersective, while $h(n) = n^2 + 1$ is not. The polynomial $h(p) = p - 1$ is intersective of the second kind, while $h(p) = p - 2$ is not.

Van der Corput sets. Kamae and Mendès France gave several criteria for intersective sets. Actually, their work was motivated by a different, stronger notion than intersective sets that they called *van der Corput sets.* A set H is called van der Corput if it has the following property. Given a sequence $(u_n)_{n \geq 1}$, if $(u_{n+h} - u_n)_{n \geq 1}$ are uniformly distributed (mod 1) for all $h \in H$, then the sequence (u_n) itself is uniformly distributed (mod 1)[5]. Kamae and Mendès France showed that any van der Corput set is also intersective, and proved the following:

Theorem 2. *A set $H \subset \mathbf{Z}^+$ is van der Corput (hence intersective) if for every $m \neq 0$, the set $H_m = \{h \in H : h \text{ is divisible by } m\}$ is infinite, and the sequence αH_m is uniformly distribute modulo 1 for every irrational α.*

This explains why the sets $\{n^2\}$ and $\{p - 1\}$ are intersective. Also, using Kamae and Mendès France's criterion, it is a simple matter to determine which polynomials are intersective of the first/second kind.

Corollary 1. *A polynomial $h \in \mathbf{Z}[x]$ is intersective if and only if for every $m \neq 0$, there is $n \in \mathbf{Z}$ such that $h(n) \equiv 0 \pmod{m}$. A polynomial $h \in \mathbf{Z}[x]$ is intersective of the second kind if and only if for every $m \neq 0$, there is $n \in \mathbf{Z}$ such that $h(n) \equiv 0 \pmod{m}$, and moreover $(n, m) = 1$.*

[3] The term intersective was coined by Ruzsa.

[4] In [37], Rice addressed these polynomials and called them *$\mathcal{P}$-intersective polynomials.* The author also learned from [37] that Wierdl had previously considered these polynomials in his thesis [49] and called them *intersective polynomials along the primes.*

[5] This definition is motivated by a theorem of van der Corput, which says that the set $\mathbf{Z}^+$ is van der Corput.

Note that the necessary condition is obvious (simply let $A = m\mathbf{Z}^+$). Informally speaking, this means that the only obstructions for a polynomial to be intersective are the local ones.

Ruzsa [42] gave some further characterizations for van der Corput sets. Extensive accounts of van der Corput sets can be found in [34, Chapter 2] and [7].

At first sight, it is not obvious at all that van der Corput sets is a strictly stronger notion than intersective sets. Bourgain [10] constructed an example of a set that is intersective but not van der Corput.

The criterion in Corollary 1 is also not quite satisfactory. Given a polynomial h, how do we check its solvability modulo m for every m? Berend and Bilu [1] gave a procedure to determine whether or not a polynomial is intersective. One can modify their argument slightly to obtain a procedure to determine intersective polynomials of the second kind. It is easy to see that polynomials with an integer root are intersective, and polynomials vanishing at 1 are intersective of the second kind, but the classes of intersective polynomials of the first/second kind are much larger than these. For example, it can be shown that the polynomials $(x^2 - 13)(x^2 - 17)(x^2 - 221)$ and $(x^3 - 19)(x^2 + x + 1)$ are intersective of the second kind (and therefore, intersective of the first kind).

Ergodic methods. Furstenberg's proof of Sárközy's theorem appeared in the same paper [15] in which he proved Szemerédi's theorem[6] and laid the foundations of Ergodic Ramsey Theory. Via what is now known as the Furstenberg Correspondence Principle, Furstenberg found a connection between intersective sets and sets of recurrence. A measure preserving system is a quadruple $(X, \mathcal{B}, \mu, T)$ where $(X, \mathcal{B}, \mu)$ is a probability space, and $T : X \to X$ is a measure preserving map, that is, $\mu(T^{-1}A) = \mu(A)$ for any measurable set $A \in \mathcal{B}$. A set $H \subset \mathbf{Z}^+$ is called a set of (single, or Poincare) recurrence if whenever $A \in \mathcal{B}$ is a set of positive measure, there must be $h \in H$ such that $\mu(A \cap T^{-h}A) > 0$.[7] It was noticed implicitly by Furstenberg, and later pointed out explicitly by Bergelson [2] and Bertrand-Mathis [9], that intersective sets and sets of recurrence are one and the same. Thus the problem can then be translated into a purely ergodic setting in which an arsenal of tools is available, such as ergodic theorems, characteristic factors, and transfinite induction.

Ergodic methods have been extremely successful in establishing far-fetched results regarding not only single recurrence, but also multiple recurrence, most of which are still out of reach by finitary methods. For example, Bergelson and Leibman [6] proved the following impressive joint generalization of Sárközy's

[6] Szemerédi's theorem says that any dense subset of positive density of $\mathbf{Z}$ must contain arbitrarily long progression, a generalization of Roth's theorem.

[7] There is also the more general notion of sets multiple recurrence. A set H is called k-recurrence if whenever $\mu(A) > 0$, there exists $h \in H$ such that $\mu(A \cap T^{-h}A \cap \cdots \cap T^{-kh}A) > 0$.

theorem and Szemerédi's theorem: if $P_1, \dots, P_k \in \mathbf{Z}[x]$ are polynomials with zero constant term, A is a set of positive upper density in $\mathbf{Z}$, then A contains configurations $\{a, a + P_1(d), \dots, a + P_k(d)\}$ for some $a, d \in \mathbf{Z}$ with $d \neq 0$. In this survey, however, we limit our interest to sets of single recurrence and will not touch the subject of multiple recurrence. We refer the reader to [3] for an overview of ideas and problems in this rich area of research.

Ergodic theorists are also able to tackle sets of recurrence of untraditional, exotic forms. Bergelson-Håland Knutson [4] and Bergelson-Håland Knutson-McCutcheon [5] studied sets of single recurrence coming from *generalized polynomials*. Generalized (or bracket) polynomials are functions obtained from regular polynomials using multiplication, addition, and the integer part function $[\cdot]$. For example, $[\alpha x^2][\beta x], [\alpha x[\beta x^2]^3 + \gamma]$ are generalized polynomials. It can be proved, for example, that if $p \in \mathbf{R}[x]$ and $p(0) = 0$, then the set $\{[p(n)] : n \in \mathbf{Z}\} \cap \mathbf{Z}^+$ is a set of recurrence. Bergelson-Håland Knutson-McCutcheon proved that if a generalized polynomial belongs a certain class called *admissible generalized polynomials*, then the set of its positive values form a set of recurrence. While we do not give the definition of admissible generalized polynomials here, it suffices to note that the class of admissible generalized polynomials is fairly large. It contains $p(x) = x$, is closed under addition and multiplication, and if p is in the class, r is a real number and $0 < h < 1$, then $q(x) = [rp(x) + h]$ is also admissible. If p is a generalized polynomial and q is admissible, then pq is also admissible.

In another direction, Frantzikinakis-Wierdl [13] and Frantzikinakis [12] considered another source of sets of recurrence, namely functions coming from a Hardy field. A Hardy field is a collection of real-valued functions[8] $f(x)$ defined for x sufficiently large, that is a field in the usual algebraic sense (with the usual addition and multiplication), and furthermore closed under differentiation. Let $\mathcal{H}$ be the union of all Hardy fields. They proved the following

Theorem 3. *Let $a \in \mathcal{H}$ be a function of polynomial growth (that is, $a(x) \ll x^k$ for some $k > 0$) and suppose that $|a(x) - cp(x)| \to \infty$ for every $p \in \mathbf{Z}[x]$ and $c \in R$. Then $S = \{[a(1)], [a(2)], \dots\}$ is a set of single recurrence*[9].

Consequently, the sequences $[n \log n], [n^c]$ (where $c > 1$), $[n^{\sqrt{5}} + \log n]$ and $[n^2 + \log\log n]$ form sets of recurrence.

Quantitative bounds. As we have seen so far, Kamae-Mendès France's and Furstenberg's methods are able to give very general results on a qualitative level. However, they are not quantitative, i.e., yielding any bound for $D(H, N)$. So far, only the circle method has been able to give explicit bounds for $D(H, N)$. Actually, Sárközy originally obtained the following explicit bounds:

[8] To be precise, equivalence classes of functions.

[9] Actually, it is also a set of multiple recurrence.

$$D(\mathcal{S}_2, N) \ll N \frac{(\log\log N)^{2/3}}{(\log N)^{1/3}} \tag{1.1}$$

if $\mathcal{S}_2$ is the set of squares, and

$$D(\mathcal{P}, N) \ll N \frac{(\log\log\log N)^3 \log\log\log\log N}{(\log\log N)^2} \tag{1.2}$$

if $\mathcal{P}$ is the set $\{p-1 : p \text{ prime}\}$.

To date, the current record is due to Pintz-Steiger-Szemerédi [35] (for the squares) and Balog-Pelikán-Pintz-Szemerédi [11] (for higher powers). They proved that if $\mathcal{S}_k$ is the set of all non-zero k-th powers, then

$$D(\mathcal{S}_k, N) \ll_k N(\log N)^{-(1/4)\log\log\log\log N} \tag{1.3}$$

For the shifted primes, the current record is due to Ruzsa and Sanders, who showed in [44] that:

$$D(\mathcal{P}, N) \ll N \exp(-c\sqrt[4]{\log N}) \qquad \text{for some constant } c > 0. \tag{1.4}$$

For the set of values of general intersective polynomials, Lucier [31] obtained the following bound. If h is and intersective polynomial, $H = \{h(n) : n \in \mathbf{Z}\} \cap \mathbf{Z}^+$, then

$$D(H, N) \ll_h N \frac{(\log\log N)^{\mu/(k-1)}}{(\log N)^{1/(k-1)}} \qquad \text{where } \mu = \begin{cases} 3, \text{ if } k = 2; \\ 2, \text{ if } k \geq 3. \end{cases} \tag{1.5}$$

This density is much weaker than Pintz-Steiger-Szemerédi's bound for the powers. Naturally, this raises the question of whether we can obtain bounds of Pintz-Steiger-Szemerédi quality for general intersective polynomials. Indeed, this was hinted to be the case in [32], but has never been carried out.

Problem 1. Obtain bounds of Pintz-Steiger-Szemerédi quality for general intersective polynomials.

Recently, this has been done by Hamel-Lyall-Rice [21] in the case of quadratic polynomials. They are able to improve the constant $1/4$ in (1.3) to $1/\log 3 - \epsilon$, which is the limit of the Pintz-Steiger-Szemerédi method. Obtaining a bound of the same quality for higher degree polynomials, however, is still an open problem.

As for intersective polynomials h of the second kind, Li and Pan [29] considered the case $h(1) = 0$ and gave a rather weak bound $D(H, N) \ll N(\log\log\log N)^{-1}$. We would like a bound for general intersective polynomials of the second kind, which is clearly larger than the class of polynomials having 1 as a root.

Problem 2. If h is an intersective polynomial of the second kind and $H = \{h(p) : p \text{ prime}\}$, obtain a good bound for $D(H, N)$. By good we mean one of the form $D(H, N) \ll N(\log N)^{-A}$ where A is a large constant, or better yet, a function that tends to ∞ with N.

Again, for quadratic intersective polynomials of the second kind, Rice [38] obtained a bound of Pintz-Steiger-Szemerédi quality.

In another direction, by special constructions, Ruzsa [41, 43] obtained the following lower bounds:

$$D(\mathcal{S}_2, N) \gg N^{0.733..} \tag{1.6}$$

$$D(\mathcal{P}, N) \gg \exp\left(\left(\frac{\log 2}{2} + o(1)\right)\frac{\log N}{\log\log N}\right) \tag{1.7}$$

Clearly, the gaps between the upper bounds and lower bounds are still huge, and it is very desirable to narrow down the gaps. Obtaining the exact order of magnitude of $D(\mathcal{S}_2, N)$ and $D(\mathcal{P}, N)$ seems to be very difficult. Ruzsa [41] believed the answer to the following question is affirmative:

Problem 3. Is it true that $\lim_{N\to\infty} \frac{\log D(S_2,N)}{\log N}$ exist?

In [44], Ruzsa and Sanders posed the following:

Problem 4. Can one obtain a bound of the form $D(P, N) \ll N^{1-c+o(1)}$, for some $c > 0$, even under the Generalized Rieman Hypothesis?

We now address the problem of finding special elements in $A - A$ where $A \subset \mathbf{Z}^+$ is not necessarily of positive upper density. Let us first generalize Definition 1.

Definition 2. *Given a subset $X \subset \mathbf{Z}$. A set $H \subset \mathbf{Z}^+$ is called X-intersective if whenever $A \subset X$ is a subset of positive relative upper density*[10]*, we have $A - A \cap H \neq \emptyset$.*

If X is the set of primes and H is X-intersective then we call H *prime intersective.* It follows from the bounds (1.3) and (1.4) that the sets $\mathcal{S}_k$ and $\mathcal{P}$ are prime intersective. However, if h is an intersective polynomial of degree > 1, it does not follow from the bound (1.5) that the set $\{h(n) : n \in \mathbf{Z}\} \cap \mathbf{Z}^+$ is prime intersective on the ground of density alone.

The idea of a *tranference principle* was first introduced by Green [17], which allowed him to deduce from Roth's theorem the result that any dense subset of the primes contains a non-trivial 3-term arithmetic progression, despite the fact that the primes have zero density. This transference principle was later simplified and extended by Green-Tao [20]. It was also the precursor to another transference principle which enabled Green and Tao to prove that any dense subset of the primes contains an arithmetic progression of arbitrary length, a result now known as the Green-Tao theorem [19]. These transference principles apply not only to primes, but also to other sets exhibiting properties close to randomness. Łaba and Hamel [24] used Green's transference principle to obtain a version of Sárközy's theorem for random sets.

[10] The relative upper density of A with respect to X is defined by $\overline{d}_X(A) = \lim_{N\to\infty} \frac{\sharp A\cap\{1,\ldots,N\}}{\sharp X\cap\{1,\ldots,N\}}$.

Using the same transference principle and Lucier's results in [31], the author proved in [28] that if h is a intersective polynomial, then $\{h(n) : n \in \mathbf{Z}\} \cap \mathbf{Z}^+$ is prime intersective[11].

Li and Pan [29] used Green's transference principle to show that if $h(1) = 0$, then the set $\{h(p) : p \text{ prime}\} \cap \mathbf{Z}^+$ is prime intersective. The general case of intersective polynomials of the second kind was proved by Rice [37], again using the transference principle (although this may be true on the ground of density alone). We close this section with the following question

Problem 5. Does there exist a set that is intersective, but not prime intersective?

1.2 Intersective sets in function fields

Let $\mathbf{F}_q$ be a finite field on q elements with characteristic p, and $\mathbf{F}_q[t]$ be the ring of polynomials over $\mathbf{F}_q$. As is well known, $\mathbf{F}_q[t]$ and $\mathbf{Z}$ possess many similarities from various points of view. Both are countable abelian groups and unique factorization domains. The Prime Number Theorem holds in $\mathbf{F}_q[t]$, furthermore, the Generalized Riemann Hypothesis is known to be true in $\mathbf{F}_q[t]$.

We can also do Fourier analysis on $\mathbf{F}_q[t]$. Let $\mathbf{F}_q(t) = \{\frac{f}{g} : f, g \in \mathbf{F}_q[t], g \neq 0\}$ be the field of fractions of $\mathbf{F}_q[t]$. On $\mathbf{F}_q(t)$ we can define a norm by $|f/g| = q^{\deg f - \deg g}$, with the convention $\deg 0 = -\infty$. The completion of $\mathbf{F}_q(t)$ with respect to this norm is $\mathbf{F}_q((\frac{1}{t})) = \{\sum_{i=-\infty}^{n} a_i t^{-i} : a_i \in \mathbf{F}_q \text{ for every } i\}$, the set of formal Laurent series in $\frac{1}{t}$. Then $\mathbf{F}_q[t] \subset \mathbf{F}_q(t) \subset \mathbf{F}_q((\frac{1}{t}))$, and $\mathbf{F}_q[t], \mathbf{F}_q(t)$ and $\mathbf{F}_q((\frac{1}{t}))$ are the analogs of $\mathbf{Z}, \mathbf{Q}, \mathbf{R}$ respectively.

Let us put $\mathbf{T} = \{\alpha \in \mathbf{F}_q((\frac{1}{t})) : |\alpha| < 1\}$, the analog of the torus $\mathbf{R}/\mathbf{Z}$. On $\mathbf{T}$ there is a unique Haar measure λ, normalized such that $\lambda(\mathbf{T}) = 1$. By a *cylinder set* defined by elements $a_1, \dots, a_k \in \mathbf{F}_q$, we mean a set of the form $\mathcal{C} = \{\sum_{i=-\infty}^{-1} x_i t^i \in \mathbf{T} : x_{-i} = a_i \text{ for all } i = 1, \dots, k\}$. Note that if $\mathcal{C}$ is defined this way, then $\lambda(\mathcal{C}) = q^{-k}$.

Let $\mathrm{Tr} : \mathbf{F}_q \to \mathbf{F}_p$ be the trace map. For $a \in \mathbf{F}_q$, let us denote by $e_q(a) = \exp(\frac{2\pi i \mathrm{Tr}(a)}{p})$. If $\alpha = \sum_{j=-\infty}^{n} a_j t^{-j} \in \mathbf{F}_q((\frac{1}{t}))$, let us define $e(\alpha) = e_q(a_{-1})$, the exponential function on $\mathbf{F}_q((\frac{1}{t}))$.

Let us also denote by $\mathbf{G}_N$ the set of all polynomials of degree strictly less than N.

Additively, $\mathbf{F}_q[t]$ is isomorphic to $\mathbf{F}_p^\omega$, the vector space of countable dimension over $\mathbf{F}_p$. We will write $\mathbf{F}_p^\omega$ if we are merely interested in the additive structure, $\mathbf{F}_q[t]$ if we are interested in arithmetic properties.

[11] If $h(0) = 0$, then this is a special case of a theorem of Tao and Ziegler [48], which states that the primes contain configurations $a, a + P_1(d), \dots, a + P_k(d)$ for some $a, d \in \mathbf{Z}$ with $d \neq 0$, where $P_1, \dots, P_k$ are given polynomials without constant term, another application of transference principles.

In view of these analogies, it is natural to ask for the $\mathbf{F}_q[t]$ analogs of known results regarding intersective sets in $\mathbf{Z}$. Of course, we may well work in the more general setting of groups in which we can define a notion of density[12], but we content ourselves with working in $\mathbf{F}_q[t]$, whose rich structure provides an excellent variety of tools.

We can define the upper density of a set $A \subset \mathbf{F}_q[t]$ by

$$\overline{d}(A) = \overline{\lim}_{N\to\infty} \frac{\# A \cap \mathbf{G}_N}{q^N}$$

The notion of intersective sets carries over:

Definition 3. *A set $H \subset \mathbf{F}_q[t] \setminus \{0\}$ is called intersective if whenever A is a set of positive upper density of $\mathbf{F}_q[t]$, we have $A - A \cap H \neq \emptyset$*

We also introduce the quantity that we would like to estimate

$$D_{\mathbf{F}_q}(H, N) = \max\{|A| : A \subset \mathbf{G}_N, A - A \cap H = \emptyset\}$$

and intersectivity of H is equivalent to saying that $D_{\mathbf{F}_q}(H, N) = o(N)$. Intersective polynomials of the first and second kinds in $\mathbf{F}_q[t]$ are defined similarly to their counterparts in $\mathbf{Z}$.[13]

What are examples of intersective sets in $\mathbf{F}_q[t]$? Kamae-Mendès France's machinery can be adapted straightforwardly in the context of $\mathbf{F}_q[t]$. More details can be found in [28, Chapter 2].

Given a sequence $(u_g)_{g\in\mathbf{F}_q[t]} \subset \mathbf{T}$ indexed by $\mathbf{F}_q[t]$, we say that it is (weakly) equidistributed in $\mathbf{T}$ if for any cylinder set $\mathcal{C} \subset \mathbf{T}$, we have

$$\lim_{N\to\infty} \frac{\#\{g \in \mathbf{G}_N : u_g \in \mathcal{C}\}}{q^N} = \lambda(\mathcal{C})$$

Definition 4. *A set $H \subset \mathbf{F}_p^\omega \setminus \{0\}$ is called van der Corput if the sequence $(a_g)_{g\in\mathbf{F}_q[t]}$ is equidistributed in $\mathbf{T}$ whenever the sequence $(a_{g+h} - a_g)_{h\in\mathbf{F}_p^\omega}$ is equidistributed in $\mathbf{T}$ for every $h \in H$.*

An exact analog of the Kamae-Mendès France criterion (Theorem 2) holds

Theorem 4. *The set $H \subset \mathbf{F}_q[t] \setminus \{0\}$ is van der Corput, hence intersective, if for every $Q \in \mathbf{F}_q[t], Q \neq 0$, the set H_Q of elements of H which are multiples of Q is infinite, and*

$$\lim_{N\to\infty} \frac{1}{|\mathbf{G}_N \cap H_Q|} \sum_{x\in\mathbf{G}_N\cap H_Q} e(x\alpha) = 0$$

for every $\alpha \notin \mathbf{F}_q(t)$.

[12] These are known as amenable groups.

[13] In the definitions, one often has to make a choice either to consider all polynomials or just monic ones, but this doesn't seem to matter.

Surprisingly enough, we are not able to tell all intersective polynomials in $\mathbf{F}_q[t]$. Inspired by the integer case, one comes quickly to the conjecture that a polynomial $\Phi(u) \in \mathbf{F}_q[t][u]$ is intersective if and only if it has roots modulo Q for every $Q \in \mathbf{F}_q[t] \setminus \{0\}$, since these are the only obvious obstructions. However, using Theorem 4, we can only verify this in the case $\deg \Phi < p$. The reason is that we know very little about the distribution of polynomial sequences in $\mathbf{T}$. When working with exponential sums over polynomials of degree k, the standard Weyl differencing method consists of taking successive differences of the polynomial in question, reducing the degree of the polynomial by 1 at each step. Finally, we will end up with a linear polynomial, and an extra factor of $k!$, which is 0 if $k \geq p$. Thus, while we can conclude that for $\alpha \notin \mathbf{F}_q(t)$, the sequence $(x^k\alpha)_{x\in\mathbf{F}_q[t]}$ is equidistributed in $\mathbf{T}$ if $k < p$, we know nothing about the distribution of $(x^{p+1}\alpha)_{x\in\mathbf{F}_q[t]}$. On the other hand, there are values of $\alpha \notin \mathbf{F}_q(t)$ such that $(x^p\alpha)_{x\in\mathbf{F}_q[t]}$ is *not* equidistributed in $\mathbf{T}$. Thus the following problem remains open.

Problem 6. Prove that a polynomial $\Phi(u) \in \mathbf{F}_q[t][u]$ is intersective if and only if it has roots modulo Q for every $Q \in \mathbf{F}_q[t] \setminus \{0\}$.

We note that as a special case of the Szemerédi Theorem for countable integral domains [8], $\Phi(u)$ is intersective if Φ has a root in $\mathbf{F}_q[t]$, but the above conjecture implies that these are not the only ones. Exhibiting a polynomial $\Phi(u) \in \mathbf{F}_q[t][u]$ without roots in $\mathbf{F}_q[t]$ but having roots every modulus is yet another interesting problem. Also, there may be some issues with the Berend-Bilu precedure [1] for determining polynomials having roots every modulus in characteristic p, even for polynomials of low degree, since it involves the discriminant of the polynomial in question.

Thanks to the work of Rhin [39], we can deduce from Theorem 4 that the set $\mathcal{P}_r = \{P + r : f \text{ monic, irreducible}\}$ where r is a fixed, non-zero element of $\mathbf{F}_q$ is intersective. Other than the linear case, the distribution of $\{\alpha\Phi(P) : P \text{ monic, irreducible}\}$ is not studied yet, thus the following problem remains open.

Problem 7. Prove that a polynomial $\Phi(u) \in \mathbf{F}_q[t][u]$ is intersective of the second kind if and only if for every $Q \in \mathbf{F}_q[t] \setminus \{0\}$, there is $f \in \mathbf{F}_q[t]$ such that $\Phi(f) \equiv 0 \pmod{Q}$ and $(Q, f) = 1$.

Regarding van der Corput sets in $\mathbf{F}_q[t]$, in view of the integer case, one believes that they constitute a strictly smaller class than intersective sets. However, Bourgain [10]'s construction of a set in that is intersective but not van der Corput in $\mathbf{Z}$ is very specific to the real numbers. Thus it is interesting to settle the following:

Problem 8. Construct a set in that is intersective but not van der Corput in $\mathbf{F}_q[t]$.

On the quantitative side, Spencer and the author [25] obtained the following estimate

$$D_{\mathbf{F}_q}(\mathcal{P}_r, N) \ll q^{N - c\frac{N}{\log N}} \tag{1.8}$$

where c is a constant depending only on q. This bound is better than the Ruzsa-Sanders bound for the shifted primes, thanks to improved exponential sum estimates in $\mathbf{F}_q[t]$, which in turn are due to the Generalized Riemann Hypothesis in $\mathbf{F}_q[t]$.

In [26], Y-R. Liu and the author studied the set $S_k = \{f^k, f \neq 0\}$ and obtained the following bound

$$D_{\mathbf{F}_q}(S_k, N) \ll q^N \frac{(\log N)^7}{N} \qquad \text{if } k < p.$$

This bound is weaker than Pintz-Szemerédi-Steiger's bound, and works only for $k < p$, due to the same reason that exponential sums over k-th powers are hard to estimate when $k \geq p$. In view of Liu and Wooley's recent works on Waring's problem [30] and Vinogradov's mean value theorem in $\mathbf{F}_q[t]$, we hope to be able to treat k-th powers in $\mathbf{F}_q[t]$ where k is arbitrary, and obtain a bound of comparable strength to Pintz-Steiger-Szemerédi's.

In view of intersective sets in $\mathbf{Z}$ formed by generalized polynomials and functions coming from a Hardy field, it is natural to ask the following questions

Problem 9. What are the objects in $\mathbf{F}_q[t]$ which are analogous to generalized polynomials and which form intersective sets?

The answer may be simpler than the integer case, since the integer part function can be defined naturally in $\mathbf{F}_q[t]$ and has much nicer properties, In fact, it is a linear map (that is, $[x] + [y] = [x + y]$ and $[ax] = a[x]$ for every $x, y \in \mathbf{F}_q((\frac{1}{t}))$ and $a \in \mathbf{F}_q$).

On the other hand the following question may be difficult, since the topology on $\mathbf{R}$ and $\mathbf{F}_q((\frac{1}{t}))$ are entirely different.

Problem 10. What are the objects in $\mathbf{F}_q[t]$ which are analogous to functions in a Hardy field and which form intersective sets?

We now address the following question regarding only the additive structure of $\mathbf{F}_p^\omega$. On $\mathbf{F}_p^\omega$ we can still define the notion of a *polynomial mapping.* Given a map $\Phi : \mathbf{F}_p^\omega \to \mathbf{F}_p^\omega$, we define $D_h\Phi(x) = \Phi(x + h) - \Phi(x)$ for every $x, h \in \mathbf{F}_p^\omega$. We say that Φ is a polynomial mapping of degree at most k if $D_{h_{k+1}} D_{h_k} \cdots D_{h_1}\Phi(x)$ is identically zero for any $h_1, \ldots, h_{k+1} \in \mathbf{F}_p^\omega$. A classic polynomial on $\mathbf{F}_q[t]$ is necessarily a polynomial mapping on $\mathbf{F}_p^\omega$, but not vice versa. Its degree when viewed as a classic polynomial and its degree when viewed as a polynomial mapping are not necessarily the same. For example, the map $x \mapsto x^{p+1}$ in $\mathbf{F}_q[t]$ becomes a quadratic mapping on $\mathbf{F}_p^\omega$. We make the following conjecture

Problem 11. Let $\Phi : \mathbf{F}_p^\omega \to \mathbf{F}_p^\omega$ be a polynomial mapping. Then the set of non-zero values of Φ is intersective in $\mathbf{F}_p^\omega$ if and only if for every vector subspace V of $\mathbf{F}_p^\omega$ of finite codimension, there is $x \in \mathbf{F}_p^\omega$ such that $\Phi(x) \in V$.

The condition is very similar to the characterization of intersective polynomials in the integers (note that $m\mathbf{Z}$ is a subgroup of finite index in $\mathbf{Z}$), and its necessity is obvious. Of course, this problem makes sense in any amenable group (one would need the image of Φ to intersect any subgroup of finite index).

We now turn our attention to another example of intesective set in $\mathbf{F}_p^\omega$ that is of combinatorial, rather than arithmetic nature. Let $J = \{0,1\}^\omega = \{(x_0, x_2, \ldots,) \in \mathbf{F}_p^\omega : x_i = 0 \text{ or } 1 \text{ for every } i\}$. There are many ways to see that J is intersective. It is a consequence of the density Hales-Jewett theorem [16, 36]. One can also prove this using Kamae and Mendès France's machinery (not Theorem 4, but a version relevant to $\mathbf{F}_p^\omega$. See [28].) One can also use Sperner's theorem on set families. Regarding $D_{\mathbf{F}_p}(J,N)$, Alon proved the following bounds, whose proof we include here due to its quickness as well as elegance.

Theorem 5 (Alon). *If $p > 2$, then we have*

$$\frac{(p-1)^N}{p\sqrt{N}} \ll D_{\mathbf{F}_p}(J,N) \le (p-1)^N$$

Proof. Suppose A is a subset of $\mathbf{F}_p^N$ such that for two distinct elements $a = (a_0, \ldots, a_{N-1}), b = (b_0, \ldots, b_{N-1}) \in A$, we have $a_i - b_i \notin \{0,1\}$ for some i. Our goal is to show that $|A| \le (p-1)^N$. For each $a = (a_0, \ldots, a_{N-1}) \in A$ let us consider the polynomial

$$\Phi_a(x_0, \ldots, x_{N-1}) = \prod_{i=0}^{N-1} (x_i - a_i - 2) \cdots (x_i - a_i - (p-1))$$

It follows from the assumption on A that $\Phi_a(b) = 0$ for any two distinct element $a, b \in A$. On the other hand, it is easy to see that $\Phi_a(a) \neq 0$. We now claim that the Φ_i are linearly independent over $\mathbf{F}_p$. Indeed, suppose there are $(c_a)_{a\in A}$ such that $\sum_{a\in A} c_a \Phi_a = 0$. Evaluating the expression at a, we have that $c_a \Phi_a(a) = 0$, so that $c_a = 0$, as desired. On the other hand, each Φ_a belongs to the vector space V over $\mathbf{F}_p$ consisting of all polynomials in N variables with the degree in each variable $\le p-2$. Since $\dim V = (p-1)^N$, we conclude that $|A| \le (p-1)^N$.

For the lower bound, let A be the set of all vectors $(a_0, \ldots, a_{N-1})$ with $0 \le a_i \le p-2, \sum_{i=0}^{N-1} a_i = \left[\frac{N(p-2)}{2}\right]$ (as integers). Then it is clear that no two distinct elements of A have difference in $\{0,1\}^N$, and it is easy to see that the size of A is $\gg \frac{(p-1)^N}{p\sqrt{N}}$.

The proof can be slightly modified to accomodate the case where $\mathbf{F}_p$ is replaced by a cylic group whose order is not necessarily prime. Theorem 5 has an immediate consequence that in any dense subset of the irreducible polynomials in $\mathbf{F}_p[t]$, one can find two distinct elements such that their difference is a polynomial all of whose coefficients are either 0 or 1.

Alon also believes that the lower bound is closer to the truth

Problem 12. Is it true that $D_{\mathbf{F}_p}(J,N) \ll \frac{(p-1)^N}{p\sqrt{N}}$?

The intersectivity of J also have an integer counterpart. Let K be the set

$$K = \left\{ \sum_{i=0}^{\infty} a_i 3^i \in \mathbf{Z}^+, a_i = 0 \text{ or } 1 \text{ for any } i \right\}$$

That is, K is the "Cantor-like" set consisting of all integers all of whose digits in base 3 expansion is either 0 or 1. It also follows from the density Hales-Jewett that K is intersective in $\mathbf{Z}$. Tao asks the following, which is certainly harder than its finite field analog:

Problem 13. Estimate $D(K,N)$.

Acknowledgement. I would like to thank Noga Alon for helpful discussions, and for his kind permission to include Theorem 5 and its proof. During the preparation of this paper, I was a member of the Institute for Advanced Study, and I would like to express my gratitude to the Institute for their generous support and hospitality.

References

1. D. Berend, Y.Bilu, *Polynomials with Roots Modulo Every Integer*, Proceedings of the American Mathematical Society, Vol. 124, No. 6 (Jun., 1996), pp. 1663-1671.
2. V. Bergelson, *Sets of recurrence of* $\mathbf{Z}^m$*-actions and properties of sets of differences in* $\mathbf{Z}^m$, J. London Math. Soc. (2) **31** (1985), 295–304.
3. V. Bergelson, *Combinatorial and Diophantine Applications of Ergodic Theory*, **Handbook of Dynamical Systems**, vol. 1B, B. Hasselblatt and A. Katok, eds., Elsevier, 2006, 745–841
4. V. Bergelson, I. J. Håland, *Sets of recurrence and generalized polynomials*, **Convergence in Ergodic Theory and Probability**, Eds.: Bergelson/March/Rosenblatt, Walter de Gruyter & Co, Berlin, NewYork, 1996, 91–110.
5. V. Bergelson, I. J. Håland Knutson, R. McCutcheon, *IP Systems, generalized polynomials and recurrence*, Ergodic Theory and Dynamical Systems **26** (2006), 999–1019.
6. V. Bergelson, A. Leibman, *Polynomial extensions of van der Waerden's and Szemerédi's theorems*, Journal of AMS **9** (1996), no. 3, 725–753.

7. V. Bergelson, E. Lesigne, *Van der Corput sets in* $\mathbf{Z}^d$, Colloq. Math. **110** (2008), no. 1, 1–49.
8. V. Bergelson, A. Leibman, R. McCutcheon, *Polynomial Szemerédi theorem for countable modules over integral domains and finite fields*, Journal d$'$ Analyse Mathématique **95** (2005), 243–296.
9. A. Bertrand-Mathis, *Ensembles intersectifs et récurrence de Poincaré*, Israel J. Math. **55** (1986), 184–198.
10. J. Bourgain, *Ruzsa's problem on sets of recurrence*, Israel J. Math. **59** (1987), no. 2, 150–166.
11. A. Balog, J. Pelikán, J. Pintz, E. Szemerédi, *Difference sets without* κ*-th powers*, Acta Math Hung **65**, 165–187 (1994).
12. N. Frantzikinakis, *Multiple recurrence and convergence for Hardy field sequences of polynomial growth*, Journal d'Analyse Mathématique, **112**, (2010), 79–135.
13. N. Frantzkinakis, M. Wierdl, *A Hardy field extension of Szemerédi's theorem*, Advances in Mathematics, 222, (2009), 1–43.
14. H. Furstenberg, **Recurrence in Ergodic Theory and Combinatorial Number Theory**, Princeton Univ. Press, 1981.
15. H. Furstenberg, *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. dAnalyse Math, 71 (1977), pp. 204–256.
16. H. Furstenberg, Y. Katznelson, *A density version of the Hales-Jewett theorem*, J. d'Analyse Math. **57** (1991), 64–119.
17. B. Green, *On arithmetic structures in dense sets of integers*, Duke Math. Jour., **114**, (2002) (2), 215–238.
18. B. Green, *Roth's Theorem in the primes*, Annals of Math. **161** (2005), no. 3, 1609–1636.
19. B. Green, T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Annals of Math. **167** (2008), 481–547.
20. B. Green, T. Tao, *Restriction theory of the Selberg sieve, with applications*, Jour. Th. Nombres Bordeaux **18** (2006), 147–182.
21. M. Hamel, N. Lyall. A. Rice, *Improved bounds on Sarkozy's theorem for quadratic polynomials*, to appear in Int. Math. Res. Not.
22. T. Kamae, M. Mendès France, *Van der Corput's difference theorem*, Israel J. Math. **31** (1978), no. 3-4, 335–342.
23. R. M. Kubota, *Waring's problem for* $\mathbf{F}_q[x]$, Dissertationes Math. (Rozprawy Mat.) **117** (1974), 60pp.
24. I. Łaba, M. Hamel, *Arithmetic structures in random sets*, Integers: Electronic Journal of Combinatorial Number Theory 8 (2008), #A4.
25. T. H. Lê, C. V. Spencer, *Difference sets and irreducible polynomials in function fields*, B. Lond. Math. Soc. 43 (2011) 347-358.
26. T. H. Lê, Y-R Liu, *On sets of polynomials whose difference set contains no squares*, to appear in Acta Arith.
27. T. H. Lê, *Intersective polynomials and the primes*, Journal of Number Theory **130** (2010), Issue 8, 1705–1717.
28. T. H. Lê, *Topics in Arithmetic Combinatorics in Function Fields*, PhD Thesis, UCLA (2010).
29. H. Li, H. Pan, *Difference sets and Polynomials of prime variables*, Acta Arith, no.1, **138** (2009), 25-52.
30. Y.-R. Liu, T. D. Wooley, *Waring's problem in function fields*, J. Reine Angew. Math. **638** (2010), 1–67.

31. J. Lucier, *Intersective sets given by a polynomial*, Acta Arith., **123** (2006), 57–95.
32. J. Lucier, *Difference sets and shifted primes*, Acta Math. Hungar., **120**(1-2) (2008), 79–102.
33. N. Lyall, *A simple proof of Sárközy's theorem*, to appear in the Proc. Amer. Math. Soc.
34. H. L. Montgomery, **Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis**, CBMS Reg. Conf. Ser. Math. 84, Amer. Math. Soc., 1994.
35. J. Pintz, W. L. Steiger, E. Szemerédi, *On Sets of Natural Numbers Whose Difference Set Contains No Squares*, J. London Math. Soc. (2) **37** (1988), 219–231.
36. D. H. J. Polymath, *A new proof of the density Hales-Jewett theorem*, Annals of Math. **175** (2012), Issue 3, 1283–1327.
37. A. Rice, *Sárközy's theorem for $\mathcal{P}$-intersective polynomials*, to appear in Acta Arith.
38. A. Rice, *Improvements and extensions of two theorems of Sárközy*, PhD Thesis, University of Georgia (2012).
39. G. Rhin, *Répartition modulo* 1 *dans un corps de séries formelles sur un corps fini*, Dissertationes Math. **95** (1972).
40. I. Ruzsa, *On difference sets*, Studia Sci. Math. Hungar. **13** (1978), no. 3-4, 319–326.
41. I. Ruzsa, *On measures of intersectivity*, Acta Math. Hungar. **43** (1984), no. 3-4, 335–340.
42. I. Ruzsa, *Uniform distribution, positive trigonometric polynomials and difference sets*, Seminar on Number Theory, 1981/1982, Exp.No. 18, 18 pp., Univ. Bordeaux I, Talence, 1982.
43. I. Ruzsa, *Difference sets without squares*, Periodica Math. Hungar., **15** (1984), 205–209.
44. I. Ruzsa, T. Sanders, *Difference sets and the primes*, Acta Arith. **131** (2008), 281–301.
45. A. Sárközy, *On difference sets of sequences of integers, I.*, Acta Math. Acad. Sci. Hungar. **31** (1978), 125–149.
46. A. Sárközy, *On difference sets of sequences of integers, III.*, Acta Math. Acad. Sci. Hungar. **31** (1978), 355–386.
47. T. Tao, *A Fourier-free proof of the Furstenberg-Sarkozy theorem*, http://terrytao.wordpress.com/2013/02/28/a-fourier-free-proof-of-the-furstenberg-sarkozy-theorem/
48. T. Tao, T. Ziegler, *The primes contain arbitrarily long polynomial progressions*, Acta Math. **201** (2008), 213–305.
49. M. Wierdl, *Almost everywhere convergence and recurrence along subsequences in ergodic theory*, PhD Thesis, Ohio State University (1989).