# LONELY RUNNERS IN FUNCTION FIELDS

SAM CHOW AND LUKA RIMANIĆ

Abstract. The lonely runner conjecture, now over fifty years old, concerns the following problem. On a unit length circular track, consider $m$ runners starting at the same time and place, each runner having a different constant speed. The conjecture asserts that each runner is *lonely* at some point in time, meaning distance at least $1/m$ from the others. We formulate a function field analogue, and give a positive answer in some cases in the new setting.

## 1. Introduction

Introduced by Wills [Wi67] in 1967, and then independently by Cusick [Cu73], the *lonely runner conjecture* (LRC) concerns the following problem. On a unit length circular track one considers $m$ runners who all start at the same place and at the same time, each runner having a constant speed, with speeds being pairwise distinct. We say that a runner is *lonely* if all the other runners are of distance at least $1/m$ from her. A well-known reformulation of the problem [BHK01], provided below, states the problem in terms of integer speeds, with one of the runners having zero speed. Throughout, let $\|x\|$ denote the distance from a real number $x$ to the nearest integer.

**Conjecture 1.1** (LRC)**.** *Let $D$ be a set of $k$ positive integers. Then there exists $t \in \mathbb{R}$ such that*

$$\|t \cdot d\| \geqslant \frac{1}{k+1}, \quad \forall d \in D.$$

At present, the problem is open for $k \geqslant 7$, that is, for eight or more runners. For $k = 1$ the conjecture is trivial, and the $k = 2$ case is resolved during the first lap of the slower non-stationary runner. The case $k = 3$ was solved by Betke and Wills [BW72], and Cusick [Cu73, Cu74, Cu82] as a problem in diophantine approximation. Cusick and Pomerance [CP84] established the conjecture for $k = 4$ by extending Cusick's previous work with additional estimates on certain exponential sums, though their proof needed a computer check for certain cases. Later Biennia et al. [BGGST] presented a much simpler proof of the $k = 3, 4$ cases, and additionally connected the lonely runner conjecture with a conjecture on flows in matroids. The case $k = 5$ was first solved by Bohman, Holzman and Kleitman [BHK01], and then Renault [Re04] provided a shorter proof. Finally, Barajas and Serra [BS08] settled the case $k = 6$.

There has been recent progress for large values of $k$. For instance, Dubickas [Du11] employed the Lovász local lemma [AS08] to establish the conjecture for

2010 *Mathematics Subject Classification.* 11J71, 11K41, 05D05, 05B20.

*Key words and phrases.* lonely runner conjecture, function fields, extremal combinatorics, sunflowers, circulant matrices.

certain lacunary sequences of speeds. For any set $D$ of $k$ non-zero integers, define

$$\delta_k(D) := \sup_{t \in \mathbb{R}/\mathbb{Z}} \min_{d \in D} \|dt\|,$$

and let $\delta_k$ be the infimum over all such sets $D$. We note that Dirichlet's approximation theorem in the form [Va97, Lemma 2.1] yields $\delta_k \leqslant \frac{1}{k+1}$, and the lonely runner conjecture states that $\delta_k \geqslant \frac{1}{k+1}$. The union bound

$$\mathbb{P}_{t \in \mathbb{R}/\mathbb{Z}}\Big( \|dt\| \geqslant \frac{1}{2k+\varepsilon}, \quad \forall d \in D \Big) \geqslant 1 - k\frac{2}{2k+\varepsilon} > 0$$

implies that $\delta_k \geqslant \frac{1}{2k}$. Until recently, previous work [Ch94, CC99, PS16] had only improved the denominator by an additive constant. Tao [Ta17] showed that there exists an absolute constant $c > 0$ such that

$$\delta_k \geqslant \frac{1}{2k} + \frac{c \log k}{k^2 (\log \log k)^2} \tag{1.1}$$

for all sufficiently large $k$. In addition, he showed that it is enough to verify the conjecture for speeds at most $k^{O(k^2)}$, and also that the conjecture holds when the speeds are all small.

**Theorem 1.2** ([Ta17])**.** *Let $k \geqslant 1$ and suppose that $\max_{d \in D} |d| \leqslant 1.2k$. Then $\delta_k(D) \geqslant \frac{1}{k+1}$.*

Czerwiński and Grytczuk [CG08] proved that the conjecture holds provided one is allowed to make a runner invisible to the other runners.

**Theorem 1.3** ([CG08])**.** *Let $k$ and $s$ be integers such that $0 \leqslant s < k$. Then for every set $D$ of $k$ positive integers there exists a subset $S \subseteq D$ of size $k - s$ such that*

$$\delta_{k-s}(S) \geqslant \frac{s+1}{2k}.$$

Recently Perarnau and Serra [PS16] extended this result by showing that there exists a time when either a runner is lonely or four runners are "almost lonely". Finally, Czerwiński [Cz12] confirmed the conjecture for a random set of positive integer speeds (see also [Al13]), establishing the inequality

$$\delta_k(D) \geqslant \frac{1}{2} - \varepsilon$$

with high probability, for any $\varepsilon > 0$.

In this article, we formulate an analogue of the lonely runner problem in function fields, and prove results of a similar flavour to (1.1), Theorem 1.2 and Theorem 1.3. We shall see, however, that our methods are very different.

1.1. **Function fields.** The analogy between number fields and function fields [vdGMS05] has a long and distinguished history, dating back at least to a famous 1882 paper by Weber and Dedekind [WD1882]. A significant milestone was reached by Weil [We41], who established the Riemann hypothesis for algebraic curves defined over finite fields, otherwise known as the "Riemann hypothesis for function fields". Since then, this connection has been deeply investigated in many contexts, and function field models have provided a valuable testing ground for building intuition, making predictions and developing

proof techniques [EVW16, En16, GG17, KS1, KS2, LW10].

Let $q$ be a prime power, and let $\mathbb{F}_q$ denote the field of $q$ elements. We have the following analogy—see for instance [LW10, §2].

| $\mathbb{Z}$ | $\mathbb{F}_q[T]$ |
|---|---|
| $\mathbb{R}$ | $\mathbb{K}_\infty := \mathbb{F}_q((T^{-1}))$ |
| $x \in \mathbb{R}/\mathbb{Z}$ | $x = \sum_{i=1}^{\infty} x_{-i} T^{-i}$ |

In order to measure loneliness, we require a notion of distance. For

$$\alpha = \sum_{i=-\infty}^{n} x_i T^i \in \mathbb{F}_q((T^{-1})),$$

let $\mathrm{ord}(\alpha)$ be the greatest integer $i$ for which $x_i \neq 0$, and write $\langle \alpha \rangle = q^{\mathrm{ord}(\alpha)}$. We adopt the convention that $\mathrm{ord}(0) = -\infty$ and $\langle 0 \rangle = 0$. Our analogue of the unit track shall be the compact additive subgroup

$$\mathbb{T} = \{\alpha \in \mathbb{K}_\infty : \langle \alpha \rangle < 1\}$$

of $\mathbb{K}_\infty$, and the "norms" in $\mathbb{T}$ take values in $\{0\} \cup \{q^{-1}, q^{-2}, \ldots\}$. Observe that any element $\alpha \in \mathbb{K}_\infty$ can be uniquely decomposed as

$$\alpha = [\alpha] + \|\alpha\|,$$

where $[\alpha] \in \mathbb{F}_q[t]$ and $\|\alpha\| \in \mathbb{T}$; this corresponds to decomposing an integer into its integer and fractional parts. For convenience, write

$$|\alpha| := \langle \|\alpha\| \rangle;$$

this corresponds to the distance from a real number to the nearest integer.

In analogy with the notation from the real setting, we define the *loneliness* of a set $\mathcal{F} \subseteq \mathbb{F}_q[T] \setminus \{0\}$ by

$$\delta(\mathcal{F}) := \sup_{\alpha \in \mathbb{T}} \min_{f \in \mathcal{F}} |\alpha f|.$$

We formulate the lonely runner conjecture in the function field setting as follows.

**Conjecture 1.4** (LRC in function fields)**.** *Let $\mathcal{F} \subseteq \mathbb{F}_q[T] \setminus \{0\}$ be such that*

$$1 \leqslant |\mathcal{F}| < \frac{q^{k+1} - 1}{q - 1}.$$

*Then*

$$\delta(\mathcal{F}) \geqslant q^{-k}.$$

We shall assume throughout that all polynomials in $\mathcal{F}$ are monic. We lose nothing in doing so, for if $c \in \mathbb{F}_q \setminus \{0\}$ and $f \in \mathbb{F}_q[T]$ then $|\alpha f| = |\alpha(cf)|$.

1.2. **Principal findings.** The upper bound on $|\mathcal{F}|$ is necessary, as illustrated by the following example. Let

$$\mathcal{F}_k := \bigcup_{j=0}^{k} \left\{ T^j + i_{j-1} T^{j-1} + \cdots + i_1 T + i_0 \colon i_0, \ldots, i_{j-1} \in \mathbb{F}_q \right\}. \tag{1.2}$$

Note that $|\mathcal{F}_k| = \sum_{j=0}^{k} q^j = \frac{q^{k+1}-1}{q-1}$, and we claim that $\delta(\mathcal{F}_k) \leqslant q^{-(k+1)}$. Indeed, for $\alpha \in \mathbb{T}$, the system of $k$ linear equations in $k+1$ variables

$$\langle \alpha f \rangle [T^{-1}] = \langle \alpha f \rangle [T^{-2}] = \cdots = \langle \alpha f \rangle [T^{-k}] = 0$$

always has solutions in $\mathbb{F}_q^{k+1}$, where $\langle g \rangle [T^m]$ denotes the coefficient of $T^m$ in $g$. Therefore, for each $\alpha \in \mathbb{T}$ we can find $f \in \mathcal{F}_k$ such that $|\alpha f| \leqslant q^{-(k+1)}$, verifying our claim.

The lower bounds on the size threshold turn to be much more demanding, and we provide only partial answers in this article. Our first result is that $q^k$ is the correct order of magnitude. The theorem below confirms Conjecture 1.4 for $k = 1$.

**Theorem 1.5.** *Let $\mathcal{F} \subseteq \mathbb{F}_q[T] \setminus \{0\}$ be of size at most $q^k$. Then $\delta(\mathcal{F}) \geqslant q^{-k}$.*

By essentially the same proof, one finds that maximal loneliness is always attained when the coefficient field is infinite. Precisely, if $K$ is an infinite field and $\mathcal{F}$ is a finite subset of $K[T] \setminus \{0\}$ then there exists

$$\alpha = \sum_{i=1}^{\infty} x_{-i} T^{-i} \qquad (x_{-i} \in K)$$

such that $(\alpha f)[T^{-1}] \neq 0$, for all $f \in \mathcal{F}$.

Our second result is that for $k > 1$, Conjecture 1.4 holds provided that $D := \max_{f \in \mathcal{F}} \deg(f) \leqslant q - O(1)$, which can be thought of as an analogue of Theorem 1.2. In order to state the result we denote by $N(m, q)$ the number of irreducible monic polynomials of degree $m$ over $\mathbb{F}_q$. Gauss established the well-known formula

$$N(m, q) = \frac{1}{m} \sum_{d \mid m} \mu(d) q^{m/d},$$

where $\mu$ is the *Möbius function*. In particular

$$N(m, q) \geqslant \frac{q^m - q^{m-1} - \cdots - q}{m}.$$

**Theorem 1.6** (Small degrees)**.** *Let $k > 1$, let $q$ and $D$ be such that*

$$\frac{N(k+1, q)}{q^k + \cdots + q} > \Big\lfloor \frac{D}{k+1} \Big\rfloor.$$

*Then for any set of non-zero polynomials $\mathcal{F}$ of size at most $\frac{q^{k+1}-1}{q-1} - 1$ whose degrees are at most $D$, one has $\delta(\mathcal{F}) \geqslant q^{-k}$.*

Our final result is a non-trivial lower bound on the number of polynomials, irrespective of $D$. We are able to get close to a halfway between Theorem 1.5 and Conjecture 1.4 in the case $k = 2$.

**Theorem 1.7** (Almost halfway there)**.** *There exists a universal constant $C$ such that the following holds. Let $\mathcal{F}$ be a set of non-zero polynomials such that*

$$|\mathcal{F}| \leqslant q^2 + 0.4877q - C.$$

*Then $\mathcal{F}$ is of loneliness at least $q^{-2}$.*

Carefully following the proof of Theorem 1.7, one could obtain $C$ to be 6.

1.3. **Methods.** The first step is to recast the question at hand as a covering problem. In the process we associate to each runner a *partial circulant matrix*; these are well-studied [Da94] and, for instance, have important applications to compressed sensing [RRT12, YMYZ10]. Once viewed as a covering problem, Theorem 1.5 follows straightforwardly from the union bound. We prove Theorem 1.6 by exploiting the structure that irreducible polynomials bring to the covering problem. We argue that if the set of speeds lacks multiples of an irreducible polynomial of degree $k+1$, then one requires many runners to cover the missing structure.

Our proof of Theorem 1.7 is considerably more involved. It uses a very particular structure known as a *sunflower*—see for instance [Ju11]. Formally, a sunflower is a family of subsets for which there exists a *core* $K$ such that for every pair of distinct subsets in the family, their intersection is precisely $K$. Large sunflowers whose core has generic dimension are very efficient at covering many vectors, and these play an indispensable role in our proof. Several authors have investigated upper bounds on the size of a sunflower-free family of sets, and this topic has received some attention recently [NS16, He17]. On the other hand, sunflowers have a fascinating structure, and there appear to be few instances in which this structure has been brought to bear on a separate problem. In the proof of Theorem 1.7 we are able to exploit the structure inherent in vector subspaces forming a sunflower. Sunflowers in this linear setting have been useful in coding theory, see [ER15] and the references within. We consider our use of sunflowers to be an interesting feature in its own right. We ultimately consider two cases, according to whether or not the set of speeds contains a large sunflower.

1.4. **Organisation.** In §2 we present our covering interpretation, and use it to establish Theorem 1.5. Theorems 1.6 and 1.7 are proved in Sections 3 and 4 respectively.

1.5. **Acknowledgements.** The first named author was supported by EPSRC Programme Grant EP/J018260/1 at the University of York, and by the National Science Foundation under Grant No. DMS-1440140 while in residence at the Mathematical Sciences Research Institute in Berkeley, California, during the Spring 2017 semester. The second named author was supported by the School of Mathematics at the University of Bristol. This work began when the authors were graduate students together at the University of Bristol, and forms part of the second named author's dissertation. We thank Julia Wolf and Trevor Wooley for their enthusiastic guidance and unwavering support. In particular, we are grateful to the latter for suggesting the project. Thanks to Tom Bloom and the rest of the HARICOT members for useful discussions. Finally, we are grateful to the anonymous referees for their feedback.

## 2. A covering problem

In this section we connect Conjecture 1.4 with a covering problem in which we cover a vector space by certain subspaces. We will be studying the lonely runner conjecture in this formulation for the remainder of the paper. We finish the section by proving Theorem 1.5.

We will use the following setup for the rest of the paper, unless stated otherwise. For $k, D \in \mathbb{N}$ let $\mathcal{F}$ be a set of non-zero polynomials in $\mathbb{F}_q[T]$ of maximal degree at most $D$, and suppose we want to check whether $\delta(\mathcal{F}) \geqslant q^{-k}$. We can write any $f \in \mathcal{F}$ as

$$f = a_0^{(f)} + a_1^{(f)} T + \cdots + a_D^{(f)} T^D,$$

for some non-zero vector $(a_0^{(f)}, \dots, a_D^{(f)}) \in \mathbb{F}_q^{D+1}$. Note that there is a one-to-one correspondence between vectors in $\mathbb{F}_q^{D+k}$ and polynomials of degree at most $D + k - 1$. To each $f \in \mathcal{F}$ we associate a partial circulant matrix

$$A_f = \begin{bmatrix} a_0^{(f)} & a_1^{(f)} & \dots & a_{k-1}^{(f)} & \dots & a_D^{(f)} & & & \\ & a_0^{(f)} & \dots & a_{k-2}^{(f)} & \dots & a_{D-1}^{(f)} & a_D^{(f)} & & \\ & & \ddots & \dots & \dots & \dots & \dots & \ddots & \\ & & & a_0^{(f)} & \dots & a_{D-k+1}^{(f)} & a_{D-k+2}^{(f)} & \dots & a_D^{(f)} \end{bmatrix} = \begin{bmatrix} f \\ Tf \\ \vdots \\ T^{k-1} f \end{bmatrix},$$

whose size is $k \times (D + k)$. We may assume that a time $\alpha$ takes the form

$$\alpha = x_{-1} T^{-1} + x_{-2} T^{-2} + \cdots + x_{-(D+k)} T^{-(D+k)}.$$

since further terms do not affect whether or not $|\alpha f| \geqslant q^{-k}$. We also associate to $\alpha$ the column vector

$$x = [x_{-1} \ x_{-2} \ \dots \ x_{-(D+k)}]^T.$$

Now $|\alpha f| \geqslant q^{-k}$ for all $f \in \mathcal{F}$ is equivalent to

$$A_f x \neq 0, \quad \forall f \in \mathcal{F}.$$

It is easy to see that the vector subspace

$$\ker(A_f) = \langle f, Tf, \dots, T^{k-1} f \rangle^{\perp} \leqslant \mathbb{F}_q^{D+k}$$

has codimension $k$. Defining $\ker(f) = \ker(A_f)$, we obtain the following.

**Lemma 2.1** (Covering version)**.** *A set $\mathcal{F}$, comprising non-zero polynomials of degree at most $D$, is of loneliness at least $q^{-k}$ if and only if*

$$\bigcup_{f \in \mathcal{F}} \ker(f) \neq \mathbb{F}_q^{D+k}.$$

This simple reformulation of the problem already provides us with the means to prove Theorem 1.5. One only needs to observe that each subspace contains the origin, and apply the union bound.

Proof of Theorem 1.5: As mentioned, for each $f \in \mathcal{F}$, the subspace $\ker(f)$ has codimension $k$ in $\mathbb{F}_q^{D+k}$, meaning that each $\ker(f)$ covers at most $q^D - 1$ non-zero vectors of $\mathbb{F}_q^{D+k}$. Therefore, by the union bound, assuming $|\mathcal{F}| \leqslant q^k$, the number of non-zero vectors covered by $\bigcup_{f \in \mathcal{F}} \ker(f)$ is at most

$$\left| \bigcup_{f \in \mathcal{F}} \ker(f) \setminus \{0\} \right| \leqslant \sum_{f \in \mathcal{F}} |\ker(f) \setminus \{0\}| \leqslant |\mathcal{F}|(q^D - 1) \leqslant q^{D+k} - q^k < q^{D+k} - 1,$$

which gives $\bigcup_{f \in \mathcal{F}} \ker(f) \neq \mathbb{F}_q^{D+k}$, from which Lemma 2.1 yields $\delta(\mathcal{F}) \geqslant q^{-k}$. □

## 3. Low degree polynomials

In this section we prove Theorem 1.6. To do so, we exploit the fact that irreducible polynomials have a particular kernel structure. In particular, we use this to prove that every irreducible polynomial of degree $k+1$ has to be observed in our set of speeds, at least as a factor. We formalise this in the following way.

**Lemma 3.1** (Irreducible polynomials are factors)**.** *Let $\mathcal{F}$ be a set of non-zero polynomials such that $|\mathcal{F}| \leqslant \frac{q^{k+1}-1}{q-1} - 1$ and $\cup_{f\in\mathcal{F}} \ker(f) = \mathbb{F}_q^{D+k}$. Then for each irreducible monic polynomial $G_{k+1}$ of degree $k+1$, there exists $f \in \mathcal{F}$ such that $G_{k+1} \mid f$.*

Proof of Theorem 1.6, assuming Lemma 3.1: For the sake of contradiction suppose that $\delta(\mathcal{F}) < q^{-k}$, or equivalently, by Lemma 2.1, that $\cup_{f\in\mathcal{F}} \ker(f) = \mathbb{F}_q^{D+k}$. In view of the assumption $|\mathcal{F}| \leqslant \frac{q^{k+1}-1}{q-1} - 1$, Lemma 3.1 tells us that for each irreducible polynomial $G_{k+1}$ of degree $k+1$ we can find $f \in \mathcal{F}$ such that $G_{k+1} \mid f$. Since the degree of each $f \in \mathcal{F}$ is bounded by $D$, a single $f$ can contain at most $\lfloor D/(k+1)\rfloor$ such $G_{k+1}$ as factors. Consequently, we need at least

$$\frac{N(k+1,q)}{\left\lfloor \frac{D}{k+1} \right\rfloor}$$

polynomials in $\mathcal{F}$. This yields

$$\frac{N(k+1,q)}{\left\lfloor \frac{D}{k+1} \right\rfloor} \leqslant |\mathcal{F}| \leqslant \frac{q^{k+1}-1}{q-1} - 1 = q^k + \cdots + q,$$

contradicting our hypotheses. This completes the proof of Theorem 1.6, given Lemma 3.1. □

It remains to prove Lemma 3.1. The pivotal idea is that if an irreducible polynomial is not a divisor of some $f \in \mathcal{F}$, we can lower bound the number of lines one needs to cover the missing $k+1$ dimensional space.

**Lemma 3.2** (Covering with lines)**.** *Let $V$ be a vector space over $\mathbb{F}_q$ such that $\dim(V) = k+1$, and let $V_1, \ldots, V_R \leqslant V$ be subspaces such that $\dim(V_i) = 1$, $1 \leqslant i \leqslant R$. If $R \leqslant \frac{q^{k+1}-1}{q-1} - 1$ then*

$$V \neq \bigcup_{i=1}^{R} V_i.$$

Proof: We need to cover $q^{k+1}-1$ non-zero vectors with $R$ lines through the origin. Note that each such line has at most $q-1$ non-zero points, so the union bound gives

$$\left| \bigcup_{i=1}^{R} V_i \setminus \{0\} \right| \leqslant \sum_{i=1}^{R} |V_i \setminus \{0\}| \leqslant \left( \frac{q^{k+1}-1}{q-1} - 1 \right)(q-1) = q^{k+1} - q < q^{k+1} - 1,$$

concluding the proof of Lemma 3.2. □

Let $\mathcal{P}_{=m}$ denote the set of all monic polynomials of degree $m$, and write $\mathcal{P}_{\leqslant m} = \cup_{i=0}^{m} \mathcal{P}_i$. Define

$$\mathcal{P}_{\leqslant m}\mathcal{F} = \{Pf \colon P \in \mathcal{P}_{\leqslant m}, f \in \mathcal{F}\}.$$

Recall that in our covering problem we seek to prove that $\cup_{f\in\mathcal{F}} \ker(f) \neq \mathbb{F}_q^{D+k}$. The following lemma provides a sufficient condition for this to hold.

**Lemma 3.3.** *Let $V \leqslant \mathbb{F}_q^{D+k}$ be such that $\dim(V^\perp) = k+1$, and let $\mathcal{F}$ be such that $|\mathcal{F}| \leqslant \frac{q^{k+1}-1}{q-1} - 1$. If $\mathcal{P}_{\leqslant k-1}\mathcal{F} \cap V = \emptyset$ then*

$$\bigcup_{f\in\mathcal{F}} \ker(f) \neq \mathbb{F}_q^{D+k}.$$

Proof: Let $V = \langle v_1, \dots, v_{D-1}\rangle$. The assumption $\mathcal{P}_{\leqslant k-1}\mathcal{F} \cap V = \emptyset$ implies that for each $f \in \mathcal{F}$ the set $B_f = \{v_1, \dots, v_{D-1}, f, Tf, \dots, T^{k-1}f\}$ is a linearly independent set of vectors in $\mathbb{F}_q^{D+k}$, and so

$$\dim(\mathrm{span}(B_f)^\perp) = 1, \quad \forall f \in \mathcal{F}.$$

Lemma 3.2 finishes the proof, since $|\mathcal{F}| \leqslant \frac{q^{k+1}-1}{q-1} - 1$. Indeed, our kernels fail to cover $V^\perp$ so they cannot cover the entire space. □

We conclude this section by proving Lemma 3.1.

Proof of Lemma 3.1: Define $V_{G_{k+1}} = \langle G_{k+1}, TG_{k+1}, \dots, T^{D-2}G_{k+1}\rangle$. The assumption that $\cup_{f\in\mathcal{F}} \ker(f) = \mathbb{F}_q^{D+k}$, combined with Lemma 3.3, gives that there exist $P \in \mathcal{P}_{\leqslant k-1}$ and $f \in \mathcal{F}$ such that $Pf \in V_{G_{k+1}}$. Thus, there exists a polynomial $p$ such that $Pf = G_{k+1}p$. Now the fact that $G_{k+1}$ is an irreducible monic polynomial of degree $k+1$, coupled with the fact that $P$ is of degree at most $k-1$, yields $G_{k+1} \mid f$. □

## 4. Getting close to halfway when $k = 2$

In this section we prove Theorem 1.7, making use of the combinatorial notion of a *sunflower*. Although we do not use any of the existing results on sunflowers, we are confident that this language helps the reader to understand the main ideas, and that the questions arising are of independent interest.

**Definition 4.1.** A collection of sets $\mathcal{S}$ forms a *sunflower* if there exists a set $K$ such that for each $S_1, S_2 \in \mathcal{S}$ with $S_1 \neq S_2$, one has

$$S_1 \cap S_2 = K.$$

We say that $K$ is the *core* and we call an element $S \in \mathcal{S}$ a *petal*. If $\mathcal{S}$ is a collection of vector subspaces then we say that $\mathcal{S}$ is a *sunflower of codimension* $d$ if $K$ is of codimension $d$.

When considering loneliness $\delta(\mathcal{F}) \geqslant q^{-2}$, the ambient space is $\mathbb{F}_q^{D+2}$, and we will be interested in collections that are formed by the kernels of polynomials in $\mathcal{F}$. A petal thus takes the form $\ker(f)$, for some polynomial $f \in \mathcal{F}$. The fact that we work with subspaces provides us with an additional tool: we have a notion of dimension, which forces the cardinality of a subspace to be a power of $q$. Observe that a "generic" intersection of two kernels has codimension 4, being the null space of a rank four matrix. In light of this, one might attempt to efficiently cover the space by starting with a large sunflower of codimension 4. This motivates us to consider a largest such sunflower, that is, one with the most petals.

We consider two cases: the first is when there exists a large codimension 4 sunflower in the set of speeds, and the second is when all codimension 4 sunflowers are small. We remark that in the former scenario it is possible to sharpen the bound provided here to get the full statement of Conjecture 1.4, see Proposition 4.6 and Remark 4.7 below. In this section, we prove a slightly weaker statement in order to make the paper easier to follow, as the real improvement needs to be made in the second case. We discuss the latter further in the appendix.

We divide the section into several parts, emphasising the connection between sunflowers and the covering statement in Lemma 2.1. We think of $\ker(f)$, $f \in \mathcal{F}$, as being introduced in some order. In order to improve on the union bound, we shall consider the contribution of each polynomial with respect to previous ones, meaning the number of points that $\ker(f)$ covers that were not already covered by the previously introduced polynomials.

The objective of our first lemma is to explain how the existence of a sunflower in the set of speeds reduces the contribution of the remaining polynomials. Moreover, it highlights the role played by the size of a largest sunflower.

**Lemma 4.2** (After the sunflower)**.** *Let $\mathcal{S} = \{f_1, \dots, f_n\}$ be a sunflower of codimension 4 of maximal size in $\mathcal{F}$, and let $f \in \mathcal{F} \setminus \mathcal{S}$. Then the contribution of $f$ is bounded from above by*

$$\left| \ker(f) \setminus \bigcup_{i=1}^{n} \ker(f_i) \right| \leqslant \max\{q^D - q^{D-1},\ q^D - nq^{D-2} + (n-1)q^{D-3}\}. \quad (4.1)$$

Proof: To ease notation define $K_i = \ker(f_i)$, for $1 \leqslant i \leqslant n$, and write $K_f = \ker(f)$. Let $K$ be the core of $\mathcal{S}$, meaning that for all $1 \leqslant i < j \leqslant n$ we have $K = K_i \cap K_j$. The contribution from $f$ is bounded above by

$$\left| K_f \setminus \bigcup_{i=1}^{n} K_i \right| = q^D - |V_1 \cup \cdots \cup V_n|,$$

where $V_i = K_i \cap K_f$ $(1 \leqslant i \leqslant n)$. Note that

$$\begin{aligned} |V_1 \cup \cdots \cup V_n| &= |V_1| + \sum_{j=2}^{n} |V_j \setminus (V_1 \cup \cdots \cup V_{j-1})| \\ &= |V_1| + \sum_{j=2}^{n} \left( |V_j| - |(V_j \cap V_1) \cup \cdots \cup (V_j \cap V_{j-1})| \right). \end{aligned}$$

For $1 \leqslant i < j \leqslant n$ one has $V_j \cap V_i = K \cap K_f$, giving

$$\left| K_f \setminus \bigcup_{i=1}^{n} K_i \right| = q^D - \left( \sum_{j=1}^{n} |V_j| \right) + (n-1)\,|K \cap K_f|. \quad (4.2)$$

Suppose first that $|K \cap K_f| = q^{D-2}$. In this case $K \cap K_f = K$, since $K \cap K_f$ is a subspace of $K$ and is of the same dimension. If each $V_j$ is of size $q^{D-2}$ then $V_j = K$ for each $j$, so $K_f$ is a petal, contradicting the maximality of $n$. Therefore there exists $V_j$ properly containing $K$, so $|V_j| = q^{D-1}$ for some $j$.

Now (4.2) gives

$$\left| K_f \setminus \bigcup_{i=1}^{n} K_i \right| \leqslant q^D - q^{D-1},$$

since $|V_j| \geqslant q^{D-2}$ for $1 \leqslant j \leqslant n$.

If instead $|K \cap K_f| \leqslant q^{D-3}$, then (4.2) becomes

$$\left| K_f \setminus \bigcup_{i=1}^{n} K_i \right| \leqslant q^D - nq^{D-2} + (n-1)q^{D-3},$$

completing the proof. □

Examining the proof of Lemma 4.2, we see that there are two important subsets of polynomials in $\mathcal{F}$:

- a codimension 4 sunflower $\mathcal{S} = \{f_1, \dots, f_n\} \subseteq \mathcal{F}$ of maximal size, with core $K$,
- a set $\mathcal{S}' \subseteq \mathcal{F} \setminus \mathcal{S}$ defined by

$$\mathcal{S}' := \{f \in \mathcal{F} \setminus \mathcal{S} \colon \ker(f) \cap K = K\}, \tag{4.3}$$

  noting from the proof of Lemma 4.2 that if $f \in \mathcal{S}'$ then there exists $i \in \{1, 2, \dots, n\}$ such that $K$ is a proper subspace of $\ker(f) \cap \ker(f_i)$.

We will use this notation for the remainder of the section.

## The structure of a sunflower

As discussed, Lemma 4.2 suggests that the size of a maximal codimension 4 sunflower plays an important role. In this subsection we establish an upper bound on the size of a sunflower.

**Lemma 4.3** (Maximal size of a sunflower)**.** *Let $\mathcal{S} \subseteq \mathcal{F}$ be a sunflower of codimension 4. Then*

$$|\mathcal{S}| \leqslant 1 + \frac{q^2 + q}{2}.$$

We prove the above lemma by exploiting the fact that the sunflowers in $\mathcal{F}$ come in two types, both easy to bound in size. Before stating that result, we prove that the core has a particular structure, a fact that will be used often in the remainder of this section.

**Lemma 4.4** (The core)**.** *Suppose that $\mathcal{S}$ is a sunflower. Define*

$$K_{f,f'} = \langle f, Tf, f', Tf' \rangle^{\perp}.$$

*Then the core $K$ satisfies $K = K_{f,f'}$ for all $f, f' \in \mathcal{S}$, $f \neq f'$.*

Proof: By the definition of a sunflower, for all distinct $f, f' \in \mathcal{S}$ we have

$$K = \ker(f) \cap \ker(f').$$

Note that $\ker(f) \cap \ker(f')$ corresponds to the kernel of the matrix with rows $f, Tf, f', Tf'$, from which the claim follows. □

We are ready to prove that there are only two types of sunflowers.

**Proposition 4.5** (Structure of a sunflower)**.** *For every sunflower $\mathcal{S} \subseteq \mathcal{F}$ one of the following holds.*

(i) *(TYPE I) There exists a polynomial $P$ such that for all $f \in \mathcal{S}$, one can find a polynomial $Q_f$ such that $f = Q_f P$, with $Q_f$ being at most quadratic.*
(ii) *(TYPE II) For all $f, f', f'' \in \mathcal{S}$ we have $f = \lambda f' + \mu f''$, for some scalars $\lambda, \mu \in \mathbb{F}_q$.*

PROOF: Let $f_1 \neq f_2$ be arbitrary elements of $\mathcal{S}$, and let $P = (f_1, f_2)$. Since each $f \in \mathcal{S}$ forms a sunflower with $f_1, f_2$, we have $\langle f_1, f_2, Tf_1, Tf_2\rangle^\perp \subseteq K_f$, and thus $f \in \langle f_1, f_2, Tf_1, Tf_2\rangle$. Therefore we can find polynomials $L_1, L_2$ of degree at most 1 such that

$$f = L_1 f_1 + L_2 f_2 \equiv 0 \pmod{P},$$

which yields $P \mid f$ for all $f \in \mathcal{F}$. Thus, defining $g_f = f/P$, note that the set

$$\mathcal{S}_P := \{g_f \colon f \in \mathcal{S}\}$$

is a well-defined set of polynomials. Moreover, it constitutes a sunflower, for if $g_{f_1}, g_{f_2} \in \mathcal{S}_P$ are distinct then

$$\begin{aligned}(K_{g_{f_1}} \cap K_{g_{f_2}})^\perp &= \langle f_1/P, f_2/P, Tf_1/P, Tf_2/P\rangle = \{h/P : h \in \langle f_1, f_2, Tf_1, Tf_2\rangle\} \\ &= \{h/P : h \in K^\perp\}.\end{aligned}$$

Finally, note that for all distinct $g, g' \in \mathcal{S}_P$ we have $(g, g') = 1$.

Now, let $g, g', g'' \in \mathcal{S}_P$ be pairwise distinct. Since $\mathcal{S}_P$ is a sunflower, we can find polynomials $L_0, L_1, L_2, L_2'$ of degree at most 1 such that

$$\begin{aligned} g &= L_1 g' + L_2 g'', \\ g' &= L_0 g + L_2' g'', \end{aligned} \tag{4.4}$$

giving

$$(1 - L_0 L_1) g = (L_1 L_2' + L_2) g''.$$

Suppose first that $L_0 L_1 \neq 1$. Since $g, g'' \in \mathcal{S}_P$ are coprime, we see that they are at most quadratic, and by a similar argument $\deg(g') \leqslant 2$, so we are in the TYPE I case.

Next, suppose instead that $1 - L_0 L_1 = L_1 L_2' + L_2 = 0$, giving $L_0, L_1 \in \mathbb{F}_q^\times$. Since $\mathcal{S}_P$ is a sunflower, we can also find polynomials $L_0', L_1'$ of degree at most 1 such that

$$g'' = L_0' g + L_1' g',$$

which combined with (4.4) yields

$$(1 - L_0' L_2) g = (L_1' L_2 + L_1) g'.$$

If $L_0' L_2 \neq 1$ we are again in the TYPE I case. Otherwise $L_0', L_2 \in \mathbb{F}_q^\times$, and by symmetry we are in the TYPE II case. □

We are ready to bound the size of a sunflower.

PROOF OF LEMMA 4.3: Recall that we assumed without loss that all $f \in \mathcal{F}$ are monic. If $\mathcal{S}$ is of TYPE II, then counting the polynomials projectively yields

$$|\mathcal{S}| \leqslant \left|\mathbb{P}^1_{\mathbb{F}_q}\right| = \frac{q^2 - 1}{q - 1} = q + 1.$$

Now suppose $\mathcal{S}$ is of TYPE I, with $P$ defined accordingly. We may assume that $P$ is monic. Let $K$ be the core of $\mathcal{S}$. Then $K$ contains the codimension 4 subspace $\{PC : \deg C \leqslant 3\}^\perp$, and so

$$K = \{PC : \deg C \leqslant 3\}^\perp.$$

For each pair $f \neq f' \in \mathcal{S}$, we now have

$$\langle f, Tf, f', Tf' \rangle = \{PC : \deg C \leqslant 3\}. \tag{4.5}$$

Note that $\{f/P : f \in \mathcal{S}\}$ is a set of monic polynomials of degree at most 2. Fix an ordering $\lambda_1, \dots, \lambda_q$ of $\mathbb{F}_q$ and consider the following colouring of the set of monic polynomials of degree at most 2.

- The polynomial 1 has its own colour $c$;
- each irreducible quadratic $Q$ has its own colour $c_Q$;
- for $1 \leqslant i \leqslant q$, multiples of $T - \lambda_i$, but not of $T - \lambda_j$ for $j < i$, have colour $c_i$.

This induces a colouring of $\mathcal{S}$ in the obvious way. Observe from (4.5) that distinct $f$ and $f'$ satisfy $\gcd(f, f') = P$. Therefore the sunflower cannot contain two polynomials of the same colour, so the total number satisfies

$$|\mathcal{S}| \leqslant 1 + \frac{q^2 - q}{2} + q,$$

since the number of monic irreducible quadratics is $\frac{1}{2}(q^2 - q)$. □

### The case when there exists a large sunflower

Here we consider the case in which there is a large codimension 4 sunflower in the set of speeds, that is, a sunflower of size $n \geqslant q + 1$. In this case, we see from Lemma 4.2 that all but $n$ polynomials cover at most $q^D - q^{D-1}$ new points. This gives a non-trivial bound on the number of polynomials needed.

**Proposition 4.6** (Large sunflower implies halfway)**.** *Let $\mathcal{F}$ be of loneliness at most $q^{-3}$. If there exists a sunflower of codimension 4 and size at least $q + 1$, then*

$$|\mathcal{F}| \geqslant q^2 + \frac{q+1}{2}.$$

*Remark* 4.7. In the large-sunflower case, one can work harder to establish the sharp inequality $|\mathcal{F}| \geqslant q^2 + q + 1$. To ease the exposition, we presently only prove a weaker result that corresponds to the bound we obtain in the case when all sunflowers are small. We provide, in the appendix, a proof of the inequality $|\mathcal{F}| \geqslant q^2 + q + 1$, assuming the existence of a sunflower of codimension 4 and size at least $q + 2$, and that $q \geqslant 8$.

Proof: By Lemma 2.1 we see that $\bigcup_{f \in \mathcal{F}} \ker(f) = \mathbb{F}_q^{D+2}$. Let $\mathcal{S}$ be a codimension 4 sunflower of maximal size, and let $n = |\mathcal{S}|$. Since $n \geqslant q + 1$, one has

$$\max\{q^D - q^{D-1}, \quad q^D - nq^{D-2} + (n-1)q^{D-3}\} = q^D - q^{D-1}.$$

Defining $R = |\mathcal{F}|$ and using Lemma 4.2, we get

$$q^{D+2} = \left|\mathbb{F}_q^{D+2}\right| = \left|\bigcup_{f\in\mathcal{F}} \ker(f)\right| \leqslant \left|\bigcup_{f'\in\mathcal{S}} \ker(f')\right| + \sum_{f\in\mathcal{F}\setminus\mathcal{S}} \left|\ker(f) \setminus \bigcup_{f'\in\mathcal{S}} \ker(f')\right|$$
$$\leqslant \left(q^D + (n-1)(q^D - q^{D-2})\right) + (R-n)(q^D - q^{D-1}).$$

Expanding the right-hand side gives

$$R \geqslant q^2 + q + \frac{q+1-n}{q},$$

which together with Lemma 4.3 yields

$$R \geqslant q^2 + \frac{q+1}{2}.$$

□

## The case when all sunflowers are small

Here we discuss the remaining case, where all codimension 4 sunflowers have at most $q$ petals. This turns out to be much more demanding, as the bound (4.1) becomes less powerful. In what follows we are able to improve on (4.1) in this case, by showing that there are many distinct pairwise intersections. In doing so we have to increase the influence of three-fold intersections, and thus are not able to establish Conjecture 1.4 in full. However, the aforementioned improvement of (4.1) yields a significant gain over Theorem 1.5 in the case $k = 2$.

**Proposition 4.8** (Small sunflowers imply almost halfway)**.** *Let $\mathcal{F}$ be such that all sunflowers in $\mathcal{F}$ of codimension 4 are of size at most $q$. If $\mathcal{F}$ is of loneliness at most $q^{-3}$, then there exists a universal constant $C \in \mathbb{R}$ such that $|\mathcal{F}| \geqslant q^2 + 0.4877q - C$.*

The rest of the paper will be devoted to the proof of this proposition. By Lemma 2.1, we have that loneliness at most $q^{-3}$ implies $\bigcup_{f\in\mathcal{F}} \ker(f) = \mathbb{F}_q^{D+2}$. Define $R = |\mathcal{F}|$, and let $n \leqslant q$ be the size of a maximal codimension 4 sunflower $\mathcal{S}$ in $\mathcal{F}$. We order the runners $f_1, f_2, \ldots, f_R$ in such a way that the two-fold intersections all have codimension 4, until the *change point*, after which all the contributions are at most $q^D - q^{D-1}$.

As in the proof of Proposition 4.6, we bound the contribution from the first $n$ runners (those that are in $\mathcal{S}$) by a total of $q^D + (n-1)(q^D - q^{D-2})$, and the next $(n-1)^2$ runners by $q^D - nq^{D-2} + (n-1)q^{D-3}$ each, using Lemma 4.2. We call this the *initial phase*.

Next we consider runner $m > n(n-1)+1$. Using the same notation as in the proof of Lemma 4.2, namely that $K_i = \ker(f_i)$ and $V_i = K_i \cap K_m$, the covering contribution of $f_m$ is

$$q^D - |V_1 \cup \cdots \cup V_{m-1}|.$$

As mentioned in the paragraph at the beginning of this case, the main idea is that there exist sufficiently many distinct two-fold intersections.

*Claim* 1. Let $t \geqslant 2$ be an integer, and assume that at $m$ we have not yet reached the change point. Then there are at least $t$ distinct sets among $V_1, \dots, V_{m-1}$, provided that

$$m - 1 > (t-1)(n-1). \tag{4.6}$$

Moreover, the sets $V_1, \dots, V_n$ are distinct, and the core $K$ of $\mathcal{S}$ satisfies

$$|K \cap K_m| \leqslant q^{D-3}.$$

Proof: Since we have not passed the change point, all of the $V_i$ have codimension 4. If $V_i = V_j$, then $K_i, K_j, K_m$ form a sunflower of codimension 4, as $K_i \cap K_j \subseteq V_i = V_j$. Since $n$ is the maximum size of a sunflower, we see that for each $V_i$ there can be at most $n-1$ indices $j \in \{1, 2, \dots, m-1\}$ such that $V_i = V_j$. In view of the inequality (4.6), the pigeonhole principle ensures that there are at least $t$ distinct sets among $V_1, \dots, V_{m-1}$.

For the second part, assume for a contradiction that for some $1 \leqslant i < j \leqslant n$ we have $V_i = V_j$. Then the core $K$ of $\mathcal{S}$ satisfies

$$K \cap K_m = V_i \cap V_j = V_i = V_j,$$

implying that $K \cap K_m$ has codimension 4. Now $K \cap K_m = K$, so by the definition of $\mathcal{S}'$ following Lemma 4.2, we have that $f_m \in \mathcal{S}'$. However, as discussed following that definition, this implies that there exists $i \in \{1, 2, \dots, n\}$ such that $K$ is a proper subspace of $V_i$, contradicting the assumption that we have not passed the change point. Therefore the sets $V_1, \dots, V_n$ are pairwise distinct, and so $|K \cap K_m| \leqslant q^{D-3}$. □

*Claim* 2. The next $(n-1)(q-n)$ runners after the initial phase contribute a total of at most

$$(n-1) \sum_{t=n+1}^{q} \left( q^D - tq^{D-2} + \left[ \binom{t}{2} - \binom{n-1}{2} \right] q^{D-3} \right).$$

Proof: Consider runner $m > n(n-1)+1$, and suppose for the time being that this process precedes the change point. If $m$ is among the first $n-1$ runners after the initial phase we may assume, by Claim 1, that $V_1, \dots, V_t$ are distinct with $t = n+1$. In this case the contribution of runner $m$ is at most

$$q^D - \sum_{j=1}^{t} |V_j| + (n-1)|K \cap K_m| + \sum_{j=n+1}^{t} |V_j \cap (V_1 \cup \cdots \cup V_{j-1})|, \tag{4.7}$$

since $V_i \cap V_j = K \cap K_m$ for all $1 \leqslant i < j \leqslant n$. Note that for distinct $V_i$ and $V_j$ the codimension of $V_i \cap V_j$ is at least 5, so the quantity in (4.7) is bounded from above by

$$\begin{aligned} &q^D - tq^{D-2} + (n-1)q^{D-3} + q^{D-3} \sum_{j=n+1}^{t} (j-1) \\ &\quad = q^D - tq^{D-2} + \left[ \binom{t}{2} - \binom{n-1}{2} \right] q^{D-3}. \end{aligned}$$

The contribution from the next $n-1$ runners is the same, but with $t = n+2$, and so on. To conclude, observe that the result remains valid even if we cross the change point, as the above bounds on the individual contributions exceed $q^D - q^{D-1}$. □

Now suppose we are in the *final stage*, meaning that

$$m > q(n-1)+1.$$

Then we may apply Claim 1 with $t = q$. The displayed expression in Claim 2 has a minimum at $t = q + \frac{1}{2}$, so there is nothing to be gained from choosing a larger value of $t$. Therefore the contribution of each runner in the final stage is bounded by

$$q^D - \frac{q^{D-1}+q^{D-2}}{2} - \binom{n-1}{2} q^{D-3}, \tag{4.8}$$

which holds irrespective of whether or not we have crossed the change point.

Combining everything, we find that

$$q^{D+2} = \left|\mathbb{F}_q^{D+2}\right| = \left|\bigcup_{i=1}^{R} K_i\right| \leqslant S_1 + S_2 + S_3, \tag{4.9}$$

where

$$S_1 = q^D + (n-1)(q^D - q^{D-2}) + (n-1)^2(q^D - nq^{D-2} + (n-1)q^{D-3})$$

comes from the initial phase,

$$S_2 = (n-1)\sum_{t=n+1}^{q}\left(q^D - tq^{D-2} + \left[\binom{t}{2} - \binom{n-1}{2}\right] q^{D-3}\right)$$

comes from Claim 2, and

$$S_3 = (R-1-q(n-1))\left(q^D - \frac{q^{D-1}+q^{D-2}}{2} - \binom{n-1}{2} q^{D-3}\right)$$

comes from the final stage, using (4.8) for these final polynomials.

We may assume without loss that $R = O(q^2)$. Simplifying the right-hand side of (4.9), dividing by $q^{D-3}$, and then grouping together all the summands that are $O(q^3)$, gives

$$\begin{aligned} &R\left(q^3 - \frac{q^2+n^2}{2}\right) \\ &\qquad \geqslant q^5 + n^3 q - \frac{1}{2}nq^3 - \frac{1}{2}n^4 + n\sum_{t=n+1}^{q}\left(tq - \binom{t}{2}\right) - C_1 q^3, \end{aligned}$$

since $n \leqslant q$. Note that

$$\left(q+\frac{1}{2}\right)\sum_{t=n+1}^{q} t - \frac{1}{2}\sum_{t=n+1}^{q} t^2 = q\frac{q^2-n^2}{2} + \frac{n^3-q^3}{6} + O(q^2),$$

which yields

$$\begin{aligned} &R\left(q^3 - \frac{q^2+n^2}{2}\right) \\ &\qquad \geqslant q^2\left(q^3 - \frac{q^2+n^2}{2}\right) - \frac{2n^4 - 3n^3q - 3n^2q^2 + nq^3 - 3q^4}{6} - C_2 q^3. \end{aligned}$$

Determining $\lambda = n/q \in [0,1]$ numerically to maximise

$$\frac{2n^4 - 3n^3q - 3n^2q^2 + nq^3}{q^4} = 2\lambda^4 - 3\lambda^3 - 3\lambda^2 + \lambda,$$

we see that

$$R\left(q^3 - \frac{q^2+n^2}{2}\right) \geqslant q^2\left(q^3 - \frac{q^2+n^2}{2}\right) + 0.4877q^4 - C_2q^3,$$

giving

$$R \geqslant q^2 + 0.4877q - C.$$

This completes the proof of Proposition 4.8.

Finally, Propositions 4.6 and 4.8 imply Theorem 1.7.

## References


[Al13] N. Alon, *The chromatic number of random Cayley graphs*, European J. Combin. **34** (2013), 1232–1243.

[AS08] N. Alon and J. Spencer, *The Probabilistic Method*, third edition, John Wiley & Sons, Inc., Hoboken, NJ, 2008.

[BS08] J. Barajas and O. Serra, *The lonely runner with seven runners*, Electron. J. Comb. **15** (2008), Research paper 48, 18 pp.

[BW72] U. Betke and J. M. Wills, *Untere Schranken für zwei diophantische Approximations-Funktionen*, Monatsh. Math. **76** (1972), 214–217.

[BGGST] W. Biennia, L. Goddyn, P. Gvozdjak and A. Sebő, M. Tarsi, *Flows, view obstructions and the lonely runner*, J. Combin. Theory Ser. B **72** (1998), 1–9.

[BHK01] T. Bohman, R. Holzman and D. Kleitman, *Six lonely runners*, Electron. J. Comb. **8** (2001), 49 pp.

[Ch94] Y. G. Chen, *View-obstruction problems in n-dimensional Euclidean space and a generalization of them*, Acta Math. Sinica **37** (1994), 551–562.

[CC99] Y. G. Chen and T. W. Cusick, *The view-obstruction problems for n-dimensional cubes*, J. Number Theory **74** (1999), 126–133.

[Cu73] T. W. Cusick, *View-obstruction problems*, Aequationes Math. **9** (1973), 165–170.

[Cu74] T. W. Cusick, *View-obstruction problems in n-dimensional geometry*, J. Combin. Theory Ser. A **16** (1974), 1–11.

[Cu82] T. W. Cusick, *View-obstruction problems II*, Proc. Amer. Math. Soc. **84** (1982), 25–28.

[CP84] T. W. Cusick and C. Pomerance, *View-obstruction problems III*, J. Number Theory **19** (1984), 131–139.

[Cz12] S. Czerwiński, *Random runners are very lonely*, J. Combin. Theory Ser. A **119** (2012), 1194–1199.

[CG08] S. Czerwiński and J. Grytczuk, *Invisible runners in finite fields*, Inform. Process. Lett. **108** (2008), 64–67.

[Da94] P. J. Davis, *Circulant Matrices*, second edition, AMS Chelsea Publishing, 1994.

[Du11] A. Dubickas, *The lonely runner problem for many runners*, Glas. Mat. Ser. III **46**(66) (2011), 25–30.

[EVW16] J. S. Ellenberg, A. Venkatesh and C. Westerland, *Homological stability for Hurwitz spaces and the Cohen–Lenstra conjecture over function fields*, Ann. of Math. **183** (2016), 729–786.

[En16] A. Entin, *On the Bateman–Horn conjecture for polynomials over large finite fields*, Compos. Math. **152** (2016), 2525–2544.

[ER15] T. Etzion and N. Raviv, *Equidistant codes in the Grassmannian*, Disc. Appl. Math. **186** (2015), 87–97.

[GG17] A. Ganguly and A. Ghosh, *Dirichlet's theorem in function fields*, Canad. J. Math. **69** (2017), 532–547.

[vdGMS05] *Number fields and function fields—two parallel worlds.* Edited by Gerard van der Geer, Ben Moonen and René Schoof. Progress in Mathematics **239,** Birkhäuser Boston, Inc., Boston, MA, 2005.

[He17] G. Hegedüs, *An improved upper bound for the size of a sunflower-free family*, Acta Math. Hungar. (2018), doi:10.1007/s10474-018-0798-7.

[Ju11] S. Jukna, *Extremal combinatorics. With applications in computer science*, second edition, Texts in Theoretical Computer Science, an EATCS series, Springer, Heidelberg, 2011.

[KS1] N. Katz and P. Sarnak, *Random Matrices, Frobenius Eigenvalues and Monodromy*, AMS Colloquium Publications **45,** AMS, Providence, 1999.

[KS2] N. Katz and P. Sarnak, *Zeros of zeta functions and symmetries*, Bull. AMS **36** (1999), 1–26.

[LW10] Y.-R. Liu and T. D. Wooley, *Waring's problem in function fields*, J. Reine Angew. Math. **638** (2010), 1–67.

[NS16] E. Naslund and W. F. Sawin, *Upper bounds for sunflower-free sets*, Forum Math. Sigma **5** (2017), e15, 10 pp.

[PS16] G. Perarnau and O. Serra, *Correlation among runners and some results on the lonely runner conjecture*, Elec. J. Comb. **23** (2016), Paper 1.50, 22 pp.

[RRT12] H. Rauhut, J. Romberg and J. A. Tropp, *Restricted isometries for partial random circulant matrices*, Appl. Comput. Harmon. Anal. **32** (2012), 242–254.

[Re04] J. Renault, *View-obstruction: a shorter proof for 6 lonely runners*, Discrete Math. **287** (2004), 93–101.

[Ta17] T. Tao, *Some remarks on the lonely runner conjecture*, Contrib. Disc. Math., to appear.

[Va97] R. C. Vaughan, *The Hardy–Littlewood method*, second edition, Cambridge Tracts in Mathematics, vol. **1**25, Cambridge University Press, Cambridge, 1997.

[WD1882] H. Weber and R. Dedekind, *Theorie der algebraischen Functionen einer Veränderlichen*, J. Reine Angew. Math. **92** (1882), 181–290.

[We41] A. Weil, *On the Riemann hypothesis in function-fields*, Proc. Nat. Acad. Sci. U. S. A. **27** (1941), 345–347.

[Wi67] J. M. Wills, *Zwei Sätze über inhomogene diophantische Approximation von Irrationalzahlen*, Monatsh. Math. **71** (1967), 263–269.

[YMYZ10] W. Yin, S. Morgan, J. Yang and Y. Zhang, *Practical compressive sensing with Toeplitz and circulant matrices*, Proc. SPIE 7744, Visual Communications and Image Processing 2010.

## Appendix A. Large sunflowers

Here we establish the following strong form of Proposition 4.6, as promised in Remark 4.7.

**Proposition A.1.** *Let $\mathcal{F}$ be of loneliness at most $q^{-3}$. If $q \geqslant 8$ and there exists a sunflower of codimension 4 and size at least $q+2$, then*

$$|\mathcal{F}| \geqslant q^2 + q + 1.$$

We start by recalling the proof of Lemma 4.2 and, in particular, the definitions of $\mathcal{S}$ and $\mathcal{S}'$, which we will use for the rest of this appendix. Let $\mathcal{S}$ be a sunflower of codimension 4 that is of maximal size in $\mathcal{F}$, denote its core by $K$, and define $\mathcal{S}'$ by (4.3). Put

$$n := |\mathcal{S}|, \quad k := |\mathcal{S}'|,$$

observing that $n \geqslant q+2$. We order the polynomials in $\mathcal{F}$ so that

$$\mathcal{S} = \{f_1, \dots, f_n\}, \qquad \mathcal{S}' = \{f_{n+1}, \dots, f_{n+k}\},$$

and define $\mathcal{S}'' := \mathcal{F} \setminus (\mathcal{S} \cup \mathcal{S}')$. Lemma 4.2 and its proof imply that for each $f \in \mathcal{S}'$ we have

$$\left| \ker(f) \setminus \bigcup_{i=1}^{n} \ker(f_i) \right| \leqslant q^D - q^{D-1},$$

and for each $f \in \mathcal{S}''$ we have

$$\left| \ker(f) \setminus \bigcup_{i=1}^{n} \ker(f_i) \right| \leqslant q^D - nq^{D-2} + (n-1)q^{D-3} < q^D - q^{D-1}. \tag{A.1}$$

Our strategy is as follows. As before, we consider the covering problem arising from Lemma 2.1. We first show that in order for $\bigcup_{f \in \mathcal{F}} \ker(f) = \mathbb{F}_q^{D+2}$ to hold when there exists a large sunflower in the set of speeds, one needs both $n$ and $k$ to be close to maximal. Moreover, we prove that $\mathcal{S}$ and $\mathcal{S}'$ are "closely connected": loosely speaking, the sunflower $\mathcal{S}$ should be thought of as comprising almost all irreducible polynomials of degree at most 2, and $\mathcal{S}'$ comprising almost all reducible quadratic polynomials. Then $\mathcal{S}''$ has to include any remaining quadratics; thus, $\mathcal{F}$ has to look like the example in (1.2), up to multiplication by a polynomial.

**Lemma A.2** ($\mathcal{S} \cup \mathcal{S}'$ is large)**.** *Let $\mathcal{F}$ be of loneliness at most $q^{-3}$ and let $\mathcal{S}$ be a sunflower of codimension 4 that is of maximal size. If $|\mathcal{F}| \leqslant q^2 + q$ and $|\mathcal{S}| \geqslant q + 2$, then for $\mathcal{S}'$ defined as above one has $|\mathcal{S}| + |\mathcal{S}'| \geqslant q^2$.*

Proof: Recall the definitions of $n$ and $k$, and let $r_n, r_k \in \mathbb{R}$ be such that

$$n = |\mathcal{S}| = \frac{1}{2}q^2 + r_n, \quad k = |\mathcal{S}'| = \frac{1}{2}q^2 + r_k.$$

Then the assumption that $\mathcal{F}$ is of loneliness at most $q^{-3}$, combined with Lemma 2.1 and the above discussion, yields

$$\begin{aligned} q^{D+2} \leqslant \underbrace{\left(q^D + \left(\frac{q^2}{2} + r_n - 1\right)(q^D - q^{D-2})\right)}_{=S_1} + \underbrace{\left(\frac{q^2}{2} + r_k\right)(q^D - q^{D-1})}_{=S_2} \\ + \underbrace{(q - r_n - r_k)\left(\frac{1}{2}q^D - r_n q^{D-2} + \frac{1}{2}q^{D-1} + (r_n - 1)q^{D-3}\right)}_{=S_3}. \end{aligned} \tag{A.2}$$

Here $S_1, S_2$ and $S_3$ are upper bounds for the covering contributions of $\mathcal{S}$, $\mathcal{S}'$ and $\mathcal{S}''$, respectively. We compute that

$$\begin{aligned} S_1 + S_2 + S_3 &= q^{D+2} + (r_n + r_k)q^{D-3}\left(\frac{1}{2}q^3 - \frac{3}{2}q^2 + r_n q - (r_n - 1)\right) \\ &= q^{D+2} + (r_n + r_k)q^{D-3}(q-1)(n - (q+1)). \end{aligned} \tag{A.3}$$

Since $n > q + 1$, we deduce from (A.2) and (A.3) that $r_n + r_k \geqslant 0$, completing the proof. □

In the course of the proof of Lemma 4.3, we showed that any TYPE II sunflower (in the sense of Proposition 4.5) has size at most $q+1$. As $n > q+1$, the sunflower $\mathcal{S}$ must therefore be of TYPE I. In other words, there exists a polynomial $P$ and at most quadratic polynomials $Q_1, \dots, Q_n$ such that $f_i = Q_i P$, for all $i \in \{1, 2, \dots, n\}$. We now show that $\mathcal{S}'$ has the same structure, with the additional information that most of the polynomials involved are reducible quadratics.

**Proposition A.3** ($\mathcal{S}'$ is an extension of $\mathcal{S}$)**.** *For each $f \in \mathcal{S}'$, there exists a polynomial $Q_f$, at most quadratic, such that $f = PQ_f$. Moreover, if $Q_f$ is of degree 2, then $Q_f$ is reducible.*

Proof: First we prove that $f = PQ_f$ for some polynomial $Q_f$ of degree at most 2. The way that $\mathcal{S}'$ is constructed implies that $K \cap \ker(f) = K$. Hence we can find $L_1, L_1', L_2, L_2'$, at most linear, such that

$$f = L_1 f_1 + L_2 f_2 = P(L_1 Q_1 + L_2 Q_2),$$
$$Tf = L_1' f_1 + L_2' f_2 = P(L_1' Q_1 + L_2' Q_2).$$

The first equation gives $P \mid f$, and the second implies that $\deg(f) \leqslant \deg(P)+2$, which combine to give the existence of an at most quadratic $Q_f$ such that $f = PQ_f$.

Now suppose that $Q_f$ is of degree 2. Since $f \in \mathcal{S}'$, we can find $i \in \{1, 2, \dots, n\}$ such that $|\ker(f) \cap \ker(f_i)| = q^{D-1}$. Therefore, there exist polynomials $L$ and $L_i$, at most linear, such that

$$LPQ_f = Lf = L_i f_i = L_i P Q_i.$$

Observe that $Q_f$ being an irreducible quadratic would imply $f = f_i$. Therefore $Q_f$ must instead be reducible. □

As an immediate consequence we obtain $|\mathcal{S}'| \leqslant \frac{1}{2}(q^2 + 3q + 2)$. The aforementioned upper bounds on $|\mathcal{S}|$ and $|\mathcal{S}'|$, together with Lemma A.2, imply that both $|\mathcal{S}|$ and $|\mathcal{S}'|$ are close to maximal. Moreover, Propositions 4.5, A.3, and Lemma A.2 imply that at least $q^2$ polynomials in $\mathcal{F}$ are of the form $f = PQ_f$, with $Q_f$ at most quadratic. This brings us very close to showing that $\mathcal{F}$ indeed looks like the example in (1.2).

The fact that $\mathcal{S}$ and $\mathcal{S}'$ make up most of the set $\mathcal{F}$ allows us to improve on the bound in Lemma 4.2. Informally, the following lemma asserts that it is sufficient to be able to add a small set as a "bridge" between $\mathcal{S}$ and $\mathcal{S}'$, in order that for the remaining polynomials the contribution bound in Lemma 4.2 may be improved to $q^D - 2q^{D-1} + q^{D-2}$.

**Lemma A.4** (Sufficient connections between $\mathcal{S}$ and $\mathcal{S}'$)**.** *Let $\mathcal{F}$ be of loneliness at most $q^{-3}$ such that a sunflower $\mathcal{S} \subseteq \mathcal{F}$ of maximal size satisfies $|\mathcal{S}| \geqslant 2q+1$. Suppose that there exists $\mathcal{C} \subseteq \mathcal{F} \setminus \mathcal{S}$ such that*

$$2|\mathcal{S}| + |\mathcal{C}| < (q+1)^2, \tag{A.4}$$

*and such that for all $f \in \mathcal{S}' \setminus \mathcal{C}$ there exist distinct $f_i, f_j \in \mathcal{S} \cup \mathcal{C}$ satisfying*

$$|\ker(f) \cap \ker(f_i)| = |\ker(f) \cap \ker(f_j)| = q^{D-1}, \quad |\ker(f_i) \cap \ker(f_j)| = q^{D-2}. \tag{A.5}$$

*Then*

$$|\mathcal{F}| \geqslant q^2 + q + 1.$$

*Remark* A.5. The assumption on $|\mathcal{S}|$ in Lemma A.4 is stronger than in previous instances of the large-sunflower case. As $q \geqslant 8$, this will cost us nothing, since Lemma A.4 will only be applied when $|\mathcal{S}| \approx q^2/2$.

Proof: Let $R := |\mathcal{F}|$ and $r := |\mathcal{C}|$. Lemma 4.2 implies that the covering contribution of each $f \in \mathcal{C}$ is at most $q^D - q^{D-1}$, since $\mathcal{C} \subseteq \mathcal{S}' \cup \mathcal{S}''$ and $n = |\mathcal{S}| \geqslant 2q + 1$.

Let $f \in \mathcal{S}' \setminus \mathcal{C}$, and let $f_i, f_j \in \mathcal{S} \cup \mathcal{C}$ be such that (A.5) holds. Then the contribution of $f$ is bounded from above by

$$|\ker(f) \setminus (\ker(f_i) \cup \ker(f_j))| \leqslant q^D - 2q^{D-1} + q^{D-2}.$$

Moreover, we know from (A.1) that the contribution of any $f \in \mathcal{S}''$ is at most

$$q^D - nq^{D-2} + (n-1)q^{D-3} \leqslant q^{D-2}(q-1)^2,$$

since $n \geqslant 2q+1$. Thus, for all $f \in \mathcal{S}' \cup \mathcal{S}'' \setminus \mathcal{C}$ the contribution of $f$ is at most $q^{D-2}(q-1)^2$. Summing all the contributions and using the assumption that $\delta(\mathcal{F}) \leqslant q^{-3}$ via Lemma 2.1, one has

$$q^{D+2} \leqslant q^D + (n-1)(q^D - q^{D-2}) + r(q^D - q^{D-1}) + (R-n-r)q^{D-2}(q-1)^2.$$

This in turn implies that

$$R \geqslant q^2 + q + \frac{(q+1)^2 - (2n+r)}{q-1} > q^2 + q,$$

using the assumption $2n + r < (q+1)^2$. □

We are ready to establish the main result of this section. The key step is to construct the set $\mathcal{C}$ appearing in Lemma A.4.

Proof of Proposition A.1: Let $R = |\mathcal{F}|$, $n = |\mathcal{S}|$ and $k = |\mathcal{S}'|$, as before. For the sake of obtaining a contradiction, suppose $R \leqslant q^2 + q$. By increasing the size of $\mathcal{F}$ if needed, we may in fact assume that

$$R = q^2 + q. \tag{A.6}$$

Recall from Lemma A.2 that

$$n + k \geqslant q^2. \tag{A.7}$$

As $q \geqslant 8$ we have

$$k \leqslant \frac{q^2 + 3q + 2}{2} \leqslant q^2 - 2q - 1,$$

so (A.7) ensures that $n \geqslant 2q+1$. This formalises Remark A.5, and confirms one of the hypotheses of Lemma A.4.

**Claim.** For each $\lambda \in \mathbb{F}_q$ we can find an at most linear polynomial $L$ such that

$$P(T-\lambda)L \in \mathcal{F}.$$

Proof: Suppose to the contrary that there exists $\lambda \in \mathbb{F}_q$ such that

$$P(T-\lambda)L \notin \mathcal{F}$$

for all $L$ that are at most linear. Then (A.7), together with Propositions 4.5 and A.3, implies that

$$\mathcal{S} \cup \mathcal{S}' = \{PQ \colon (T-\lambda) \nmid Q\},$$

since $|\{PQ \colon (T-\lambda) \nmid Q\}| = q^2$. Hence the largest sunflower has $\frac{1}{2}(q^2+q)$ petals, and is formed by multiplying a polynomial $P$ by all (monic) irreducible quadratic polynomials, and all $L^2$, for $L \neq T - \lambda$ at most linear. We wish to prove that in this case $\mathcal{S}$ satisfies the assumptions of Lemma A.4, with $\mathcal{C} = \emptyset$. Indeed, let $f = PL_iL_j \in \mathcal{S}'$ be arbitrary. Since $L_i, L_j \neq T - \lambda$, it is easy to see that (A.5) holds with $f_i := PL_i^2$ and $f_j := PL_j^2 \in \mathcal{S}$. Now Lemma A.4 delivers a contradiction, as we assumed $R \leqslant q^2 + q$. □

Let

$$\mathcal{S}_{\max} := \{\mathcal{S} \subset \mathcal{F} \colon \mathcal{S} \text{ is a maximal sunflower}\}.$$

To each $\mathcal{S} \in \mathcal{S}_{\max}$ we associate the set

$$\lambda_{\mathcal{S}} := \{\lambda \in \mathbb{F}_q \colon \exists Q_\lambda \text{ such that } (T-\lambda) | Q_\lambda \text{ and } PQ_\lambda \in \mathcal{S}\}.$$

The colouring argument in the proof of Lemma 4.3 ensures that for $\lambda \in \lambda_{\mathcal{S}}$ the polynomial $Q_\lambda$ is unique. Define $\lambda_{\mathcal{S}}^c := \mathbb{F}_q \setminus \lambda_{\mathcal{S}}$, and let $\mathcal{S} \in \mathcal{S}_{\max}$ be such that $|\lambda_{\mathcal{S}}^c|$ is maximal, and such that if $PL^2 \in \mathcal{F}$ then $PL \notin \mathcal{S}$.

Observe that if $\lambda, \lambda' \in \lambda_{\mathcal{S}}^c$ then $P(T-\lambda)(T-\lambda') \notin \mathcal{F}$, for otherwise we could add $P(T-\lambda)(T-\lambda')$ to $\mathcal{S}$, contradicting its maximality. In particular $P(T-\lambda)^2 \notin \mathcal{F}$ for $\lambda \in \lambda_{\mathcal{S}}^c$. With $\ell := |\lambda_{\mathcal{S}}^c|$ we have

$$n \leqslant 1 + \frac{q^2+q}{2} - \ell;$$

this bound follows from variant of the colouring argument in the proof of Lemma 4.3.

Roughly speaking, we want $\mathcal{S}$ to attain the fewest distinct elements of $\mathbb{F}_q$ as roots, so that we may construct $\mathcal{C}$ efficiently. Choosing $\mathcal{S}$ as above ensures that if $L$ is at most linear then $PL^2 \notin \mathcal{F} \setminus \mathcal{S}$. Indeed, first consider when $L = 1$, supposing for a contradiction that $P \in \mathcal{F} \setminus \mathcal{S}$. If $\mathcal{S}$ contains no linear multiples of $P$, then we can contradict its maximality by including $P$. If, on the other hand, $\mathcal{S}$ contains a linear multiple of $P$, then we can put $P$ in $\mathcal{S}$ instead of it, to contradict the maximality of $|\lambda_S^c|$. We conclude that $P \notin \mathcal{F} \setminus \mathcal{S}$.

Otherwise $L = T - \lambda$. Suppose for a contradiction that $PL^2 \in \mathcal{F} \setminus \mathcal{S}$. Then we must have $\lambda \in \lambda_S$, so $PLL' \in \mathcal{S}$ for some $L'$ at most linear. Moreover, we must have $L' = 1$, for otherwise we could replace $PLL'$ by $PL^2$ in $\mathcal{S}$ to increase $|\lambda_{\mathcal{S}}^c|$. Now $PL^2 \in \mathcal{F}$ and $PL \in \mathcal{S}$, which is impossible, by our choice of $\mathcal{S}$.

We split our argument into two cases. Case A applies when for each $\lambda \in \lambda_{\mathcal{S}}^c$ we can find two distinct polynomials $L_1^{(\lambda)}, L_2^{(\lambda)}$, of degree at most 1, such that

$$f_{\lambda,1} = P(T-\lambda)L_1^{(\lambda)}, \quad f_{\lambda,2} = P(T-\lambda)L_2^{(\lambda)} \in \mathcal{F}. \tag{A.8}$$

Case B applies when there exists $\lambda \in \mathbb{F}_q$ for which there is only one

$$f_\lambda = P(T-\lambda)L_\lambda \in \mathcal{F}.$$

First consider Case A. For $\lambda \in \lambda_{\mathcal{S}}^c$ choose distinct $f_{\lambda,1}, f_{\lambda,2} \in \mathcal{F}$ as in (A.8) and add them to $\mathcal{C}$, with $L_{\lambda,1} = 1$ if $P(T-\lambda) \in \mathcal{F}$. Note that $\mathcal{S}$ and $\mathcal{C}$ are disjoint, and

$$2|\mathcal{S}| + |\mathcal{C}| \leqslant 2\left(1 + \frac{q^2+q}{2} - \ell\right) + 2\ell < (q+1)^2.$$

We proceed to confirm the hypotheses (A.5) of Lemma A.4. Let

$$f = P(T-\lambda_i)(T-\lambda_j) \in \mathcal{S}' \setminus \mathcal{C},$$

and observe that $\lambda_i \neq \lambda_j$, since we showed that if $PL^2 \in \mathcal{F}$ then $PL^2 \in \mathcal{S}$. If $\lambda_i, \lambda_j \in \lambda_{\mathcal{S}}$ then we can find $f_i = P(T-\lambda_i)L_i$ and $f_j = P(T-\lambda_j)L_j$

in $\mathcal{S}$, whereupon (A.5) holds. If $\lambda_i \in \lambda_{\mathcal{S}}$ and $\lambda_j \in \lambda_{\mathcal{S}}^{\mathrm{c}}$, then we can find $f_i = P(T-\lambda_i)L_i \in \mathcal{S}$ and

$$f_{\lambda_j,1} = P(T-\lambda_j)L_1^{(\lambda_j)}, \quad f_{\lambda_j,2} = P(T-\lambda_j)L_2^{(\lambda_j)} \in \mathcal{C}.$$

Choose $m \in \{1,2\}$ such that $L_m^{(\lambda_j)} \neq L_i$ and define $f_j := f_{\lambda_j,m}$ to get (A.5) again, noting that $f \in \mathcal{S}' \setminus \mathcal{C}$ implies $f_j \neq f$. Since we proved that there is no polynomial in $\mathcal{F}$ for which $\lambda_i, \lambda_j \in \lambda_{\mathcal{S}}^{\mathrm{c}}$, this analysis covers all possibilities.

To conclude Case A it remains to consider $f = P(T-\lambda_i) \in \mathcal{S}' \setminus \mathcal{C}$, and show that it satisfies (A.5) for some $f_i, f_j \in \mathcal{S} \cup \mathcal{C}$. As $L_1^{(\lambda_i)} = 1$ had priority over genuinely linear polynomials in the construction of $\mathcal{C}$, we see that $P(T-\lambda_i) \in \mathcal{S}' \setminus \mathcal{C}$ only if $\lambda_i \in \lambda_{\mathcal{S}}$. Hence there exists $f_i = P(T-\lambda_i)L_i \in \mathcal{S}$. If there were no linear $L$ such that $PL \in \mathcal{S}$, then we could have chosen $P(T-\lambda_i)$ to place in $\mathcal{S}$ instead of $f_i$, and this contradicts the minimality of $|\lambda_{\mathcal{S}}|$. Therefore there exists $L_j \neq T-\lambda_i$, at most linear, such that $f_j = PL_j \in \mathcal{S}$, giving (A.5).

Putting everything together, we see that $\mathcal{S}$ and $\mathcal{C}$ satisfy the assumptions of Lemma A.4, which implies $R \geqslant q^2+q+1$ as desired.

Finally, suppose that we are in Case B, so that there exists $\lambda \in \mathbb{F}_q$ such that there is a unique $f_\lambda = P(T-\lambda)L_\lambda$ in $\mathcal{F}$. Then, by (A.6), there is at most one polynomial from the set

$$X := \{PQ \colon (T-\lambda) \nmid Q, \deg Q \leqslant 2\}$$

that is not in $\mathcal{F}$, as $|X| = q^2$. We initially choose

$$\mathcal{C} = \begin{cases} \{f_\lambda\} \setminus \mathcal{S}, & \text{if } P \in \mathcal{F} \\ \{f_\lambda\} \cup \{P(T-\kappa) \in \mathcal{F} : \kappa \in \mathbb{F}_q\} \setminus \mathcal{S}, & \text{if } P \notin \mathcal{F}. \end{cases}$$

If $P(T-\lambda')^2 \notin \mathcal{F}$ for some $\lambda' \neq \lambda$, then for some $\lambda'' \notin \{\lambda, \lambda'\}$ we replace $P(T-\lambda'')^2$ by $P(T-\lambda')(T-\lambda'')$ in $\mathcal{S}$, and also append $P(T-\lambda'')^2$ to $\mathcal{C}$. When $P \notin \mathcal{F}$, we note that

$$2|\mathcal{S}| + |\mathcal{C}| \leqslant (q^2+q) + q < (q+1)^2.$$

The inequality (A.4) also holds when $P \in \mathcal{F}$.

We showed in Case A that if $L$ is at most linear then $PL^2 \notin \mathcal{F} \setminus \mathcal{S}$; the argument still works in Case B—wherein $\mathcal{S}$ has possibly been modified—unless $L = T-\lambda''$, and in the latter case $PL^2 \in \mathcal{C}$. Thus, if $f \in \mathcal{S}' \setminus \mathcal{C}$ then either

(i) $f = P(T-\lambda_i)(T-\lambda_j)$ with $\lambda_i, \lambda_j, \lambda \in \mathbb{F}_q$ pairwise distinct, or
(ii) $f = P(T-\lambda_j)$ for some $\lambda_j \neq \lambda$.

In scenario (i) we obtain (A.5) by choosing $f_i = P(T-\lambda_i)^2$ and $f_j = P(T-\lambda_j)^2$, or instead $f_j = P(T-\lambda')(T-\lambda'')$ if say $\lambda_j \in \{\lambda', \lambda''\}$. In scenario (ii) we must have $P \in \mathcal{F}$, by our choice of $\mathcal{C}$, and so $P \in \mathcal{S}$. We may therefore choose $f_i = P$ and $f_j = P(T-\lambda_j)^2$, as long as $\lambda_j \notin \{\lambda', \lambda''\}$. If $\lambda_j \in \{\lambda', \lambda''\}$ then we may choose $f_j = P(T-\lambda')(T-\lambda'')$ instead.

Therefore $\mathcal{S}$ and $\mathcal{C}$ satisfy the hypotheses of Lemma A.4, which finishes the proof of Proposition A.1. □

Sam Chow, Department of Mathematics, University of York, Heslington, York YO10 5DD, United Kingdom

*E-mail address*: sam.chow@york.ac.uk

Luka Rimanić, School of Mathematics, University of Bristol, University Walk, Bristol BS8 1TW, United Kingdom

*E-mail address*: luka.rimanic@bristol.ac.uk