

Rational normal curves as no- $(d + 2)$ -on- Q -quadric sets

Dávid R. Szabó*

6th November 2025

Abstract

For every $d \geq 2$, we construct a subset $D \subseteq \{1, 2, \dots, n\}^d$ of size $n - o(n)$ such that every affine hyperplane of \mathbb{R}^d intersects D in at most d points, and every hypersphere of \mathbb{R}^n intersects D in at most $d + 1$ points. This construction is the largest one currently known, and strongly builds on ideas of Dong, Xu, and also of Thiele. More generally, we prove that the role of hyperspheres can be replaced by Q -quadrics, i.e. by quadratic surfaces given by an equation whose degree two homogeneous part equals a fixed quadratic form Q . We formulate analogous statements in affine spaces over (finite) fields. Essentially, every construction is given by a suitable rational normal curve in a d -dimensional projective space.

Contents

| | | |
|----------|--|-----------|
| 1 | Introduction | 2 |
| 1.1 | History | 2 |
| 1.2 | Main results | 2 |
| 1.3 | Idea of the construction | 4 |
| 1.4 | Structure of the paper | 5 |
| 1.5 | Acknowledgement | 5 |
| 2 | Preliminaries and tools | 5 |
| 2.1 | Notation | 5 |
| 2.2 | Classical algebraic geometry | 5 |
| 2.3 | Classical number theory | 7 |
| 3 | Q-quadrics | 8 |
| 4 | Constructions and proof of theorems | 9 |
| 4.1 | Over arbitrary fields | 9 |
| 4.2 | Over finite fields | 10 |
| 4.3 | In finite square grids of \mathbb{R}^d | 11 |
| 5 | Open problems | 12 |

*HUN-REN Alfréd Rényi Institute of Mathematics (Hungary, 1053 Budapest, Reáltanoda u. 13-15.) and ELTE Linear Hypergraphs Research Group. The author is supported by the University Excellence Fund of Eötvös Loránd University. E-mail: szabo.r.david@gmail.com

1 Introduction

1.1 History

The no-three-in-line problem In 1917, Dudeney asked at most how many points can be selected from an $n \times n$ grid of the Euclidean plane so that no three of these points lie on the same line [Dud17]. The so-called **no-three-in-line** problem of determining this maximum value is still open in general (apart from small values of n [Fla98]) despite receiving considerable attention. The best known upper bound is still the obvious $2n$ obtained by considering the rows. The current best known lower bound of $\frac{3}{2}n - o(n)$ by Hall, Jackson, Sudbery and Wild stands since 1975 [HJSW75]. This construction uses degree 2 algebraic curves over finite fields. Several conjectures were formulated concerning the asymptotic value [GK68; BMP05; Epp18; Gre].

Variations on a theme Many variants of the **no-three-in-line** problem have been studied. For example, for the **no- $(k+1)$ -in-line** problem (where at most k points are allowed on every line), the obvious upper bound kn was recently shown to be sharp by Kovács, Nagy and Szabó for $k > C\sqrt{n \log(n)}$ [KNS25b] which was extended by Grebennikov and Kwan to $n \geq k \geq 10^{37}$ [GK25], while close to optimal constructions are known for smaller values of k [KNS25a]. See for example [BK03] by Braß and Knauer, [Lef08] by Lefmann, [PW07] by Pór and Wood or [SZ25] by Suk and Zeng for a higher dimensional generalisation. Nagy, Nagy and Woodroffe considered the extensible version of the problem to \mathbb{Z}^2 [NNW23]. For more related general position problems, see the survey [KT+25] by Klavžar, Tuite et al.

The no-four-on-a-circle problem Another related theme additionally involves quadratic hypersurfaces. Erdős and Purdy asked to determine the maximum number of points that can be selected from an $n \times n$ grid so that no 4 of them are on a line or on a circle, known as the **no-four-on-a-circle** problem [Guy04, §F6]. Thiele in 1995 showed this number is between $\frac{1}{4}n$ and $\frac{5}{2}n - \frac{3}{2}$ [Thi95a, §1.1] or [Thi95b]. In his construction, actually, no line contains three points. Thiele [Thi95a, §1.2] and Brass, Moser and Pach [BMP05, §10.1, Problem 4] posed to determine the maximum number of points from $[n] := \{1, \dots, n\}^d \subset \mathbb{R}^d$ such that no $d+2$ points are contained in a hyperplane or in a hypersphere, known as the **no- $(d+2)$ -on-a-sphere** problem. Considering parallel hyperplanes, we see that at most $(d+1)n$ points may be selected. The first non-trivial construction was given in 1995, Thiele [Thi95a, §1.2] gave an algebraic construction of size $\Omega(n^{1/(d-1)})$. Recently, Suk and White [SW24, Theorem 1.1] gave a construction based on VC-dimensions of size $n^{3/(d+1)-o(n)}$. In turn, this was improved further by Ghosal, Goenka and Keevash [GGK25, Corollary 1.6] using randomised constructions to $\Omega(n^{(\min\{d,4\})/(d+1)-c/\log \log n})$. The best known construction of size $n - o(n)$ is due to Dong and Xu [DX25, Theorem 2] and uses algebraic curves.

1.2 Main results

The sharp no- $(d+2)$ -on-a-sphere problem Following [Thi95a, §1.2], in this paper, we consider the following slightly sharper (and maybe more natural) version of the previous problem.

Problem 1.1 (The sharp no- $(d+2)$ -on-a-sphere problem). *For $n \in \mathbb{N}$ and $d \geq 2$, determine the size, say $f([n]^d, \mathbb{R}^d)$, of the largest subset $D \subseteq [n]^d \subset \mathbb{R}^d$ satisfying the **sharp no- $(d+2)$ -on-a-sphere** condition in \mathbb{R}^d , i.e.*

- *no $d+1$ points of D lie on a common affine hyperplane in \mathbb{R}^d , and*
- *no $d+2$ points of D lie on a common hypersphere in \mathbb{R}^d .*

By considering parallel hyperplanes, we see that $f([n]^d, \mathbb{R}^d) \leq d \cdot n$. The aforementioned construction of Thiele from 1995 actually shows that $\frac{3}{32}n^{1/(d-1)} \leq f([n]^d, \mathbb{R}^d)$, see [Thi95a, §1.2] or [Thi95b, footnote]. Recently, this was improved to $n/(d+1) - o(n) \leq f([n]^d, \mathbb{R}^d)$ by Dong and Xu [DX25, Theorem 2]. (Note that in [DX25], the notation $\text{ex}([n]^d; (d+1)_\square, (d+2)_\circ)$ is used for our $f([n]^d, \mathbb{R}^d)$.) Both constructions used algebraic curves over finite fields in a similar way. The following main result of this paper improves the previous best lower bound by a factor of $d+1$.

Theorem 1.2 (The sharp no- $(d+2)$ -on-a-sphere problem). *For every $d \geq 2$, as $n \rightarrow \infty$, we have*

$$n - o(n) \leq f([n]^d, \mathbb{R}^d) \leq d \cdot n.$$

The no- $(d+2)$ -on- Q -quadric problem Note that the equation of every hypersphere in \mathbb{R}^d is a quadratic polynomial $F \in \mathbb{R}[X_1, \dots, X_d]$ whose degree 2 *homogeneous* part is the fixed polynomial $Q = X_1^2 + \dots + X_d^2$. Extending this, for an arbitrary *quadratic form* (i.e. homogeneous degree 2 polynomial) $Q \neq 0$, a surface is said to be a Q -*quadric* (cf. Definition 3.1) if its equation is a degree 2 polynomial whose homogeneous degree 2 part is exactly Q (up to scalar multiples). Similarly to hyperspheres, a Q -quadric is uniquely determined by $d+1$ general position points (see Lemma 3.4), which motivates the following problem.

Problem 1.3 (The no- $(d+2)$ -on- Q -quadric problem). *For $n \in \mathbb{N}$, $d \geq 2$ and quadratic form $0 \neq Q \in \mathbb{Q}[X_1, \dots, X_d]$, determine the size, say $f_Q([n]^d, \mathbb{R}^d)$, of the largest subset $D \subseteq [n]^d \subset \mathbb{R}^d$ satisfying the no- $(d+2)$ -on- Q -quadric condition in \mathbb{R}^d , i.e.*

- *no $d+1$ points of D lie on a common affine hyperplane in \mathbb{R}^d , and*
- *no $d+2$ points of D lie on a common Q -quadric in \mathbb{R}^d .*

The next statement is the other main result of this paper, which immediately implies the previous Theorem 1.2 as a special case, which we prove in §4.3.

Theorem 1.4 (The no- $(d+2)$ -on- Q -quadric problem). *For every $d \geq 2$ and ever quadratic form $0 \neq Q \in \mathbb{Q}[X_1, \dots, X_d]$, we have*

$$n - o(n) \leq f_Q([n]^d, \mathbb{R}^d) \leq d \cdot n.$$

Finite field analogues In turn, Theorem 1.4 is actually a consequence of an analogous statement over finite fields \mathbb{F} . In this setup, we pick the points from the full affine space \mathbb{F}^d so that every affine hyperplane in \mathbb{F}^d can contain at most d selected points, and every Q -quadric in \mathbb{F}^d can contain at most $d+1$ selected points. Such configurations are said to be Q -*generic* (see Definition 3.5), and its minimal size denoted by $f_Q(\mathbb{F}^d, \mathbb{F}^d)$.

Theorem 1.5 (The no- $(d+2)$ -on- Q -quadric problem over finite fields). *Let \mathbb{F} be a finite field and $2 \leq d \in \mathbb{N}$ with $d \leq |\mathbb{F}| + 1$. Let $0 \neq Q \in \mathbb{F}[X_1, \dots, X_d]$ be any quadratic form which is not irreducible of rank 2. Then*

$$|\mathbb{F}| + 1 - d \leq f_Q(\mathbb{F}^d, \mathbb{F}^d) \leq d \cdot |\mathbb{F}|.$$

We prove this statement in §4.2 by considering the affine part of a suitably constructed rational normal curve over \mathbb{F} . It is worth specialising the previous statement to the case of hyperspheres by taking $Q = X_1^2 + \dots + X_d^2$.

Theorem 1.6 (The sharp no- $(d+2)$ -on-a-sphere problem over finite fields). *Let \mathbb{F} be a finite field and $d \in \mathbb{N}$ with $d \leq |\mathbb{F}| + 1$. If $d = 2$, assume further that $|\mathbb{F}| \not\equiv 3 \pmod{4}$. Then there is a $C_0 \subseteq \mathbb{A}_{\mathbb{F}}^d$ of size $|\mathbb{F}| + 1 - d$ satisfying the **sharp no- $(d+2)$ -on-a-sphere** condition in $\mathbb{A}_{\mathbb{F}}^d$.*

1.3 Idea of the construction

Following most algebraic constructions, we will mostly work over a field of prime order. We mix the most useful ideas from [Thi95a] and [DX25].

Motivation from Thiele: degree d algebraic curves [Thi95a] considered the degree d modular momentum curve which automatically solved every hypersphere. Since hyperspheres intersect this curve in too many points, he systematically deleted many points of his curve so that at most $d + 1$ points remained on every hypersphere.

Motivation from Dong and Xu: hiding intersection points at infinity This idea is from [DX25] (but similar phenomena have appeared much less explicitly in [HJSW75]). By Bézout’s theorem, every projective curve of degree d (not contained in a hypersphere) intersects every hypersphere in exactly $2d+2$ points (counted with multiplicity, over the algebraic closure, and considering points of the ideal hyperplane). [DX25] carefully constructed such a curve whose $d + 1$ points of intersection with the ideal hyperplane (at infinity) actually are points of *every* hypersphere, hence leaving at most $d + 1$ intersection points in the affine space. They constructed the parametrisation for such a curve by a relatively long computation, where they also had to ensure that the curve is not contained in any hyperspheres. The degree of the curve may produce too many intersection points with hyperplanes, so (similarly to [Thi95a]), [DX25] also removed many points of the curve so that every hyperplane contains at most d points.

For example, in the case $d = 2$, every circle intersects the ideal line in exactly the same two fixed points P_1 and P_2 . The degree 3 curve constructed in [DX25] passes through P_i with multiplicity i . This tangential property at P_2 shows that the curve is not contained in any circle. The geometric picture in higher dimensions in [DX25] is analogous.

Our construction We present a structural construction that is almost free of computations and works as well to arbitrary Q -quadrics, not just to hyperspheres.

We aim to choose the degree of our curve to be as small as possible without being contained in any hyperplane. It is a classical algebraic geometry fact (see Remark 2.10) the smallest possible degree is d (if the dimension of the ambient space is d) and that up to projective linear transformations, there is a *unique* irreducible non-degenerate degree d curve in the d -dimensional projective space, the so called *rational normal curve*. (This characterisation is not used in our proof, but it helped to find the construction.)

We start with the moment curve (i.e. the Veronese embedding) of [Thi95a], which, by above, is just a special instance of rational normal curves. Next, we apply a suitable (projective) linear transformation to it that enables keeping the whole (affine) curve in our construction without the need to delete additional points. This is the step where our construction beats in size the former ones.

To find this suitable transform, we pick points P_1, \dots, P_d in general position from the ideal hyperplane such that P_1, \dots, P_{d-1} are contained in the projective closure of *every* Q -quadric, and P_d is not contained in none of them. Such a choice exploits the fact that – similarly to hyperspheres – every Q -quadric intersects the ideal hyperplane in exactly the same points. Using the transitivity automorphism group of projective spaces on points in general position, we can freely take the transform of the Veronese curve passing through the points P_1, \dots, P_d , see Lemma 2.11. The choice of P_d ensures that this curve is not contained in any Q -quadrics. Bézout’s theorem then applies and shows that our curve intersects every Q -quadric in at most $2d$ points. However, exactly $d - 1$ of these points were constructed to be in the ideal hyperplane, leaving at most $d + 1$ intersection points in the affine space as required.

1.4 Structure of the paper

In §2 we introduce some notation, review standard facts from algebraic geometry and number theory. In §3, as a generalisation of hyperspheres, we introduce the notion of a Q -quadric for any quadratic form Q over a field and discuss its basic properties. Finally, in §4, we prove the main statements in a constructive way first over arbitrary fields (§4.1), then over finite fields (§4.2), and finally in finite grids on \mathbb{R}^d (§4.3).

We start every section with a short summary to help the reader with the structure and the goals of the current section.

1.5 Acknowledgement

The author is grateful to Zoltán Lóránt Nagy and Benedek Kovács for the fruitful discussions.

2 Preliminaries and tools

In this section, we fix some notations and collect all the necessary tools for this paper. The first toolkit is algebraic geometry: elementary affine and projective varieties, Bézout's theorem, Warning's theorem about the cardinality of affine varieties over finite fields. The other technical toolkit is classical number theory: quadratic residues, the Prime number theorem, and Dirichlet's theorem on primes in arithmetic progressions.

2.1 Notation

Denote by \mathbb{N} , \mathbb{Q} and \mathbb{R} the set of natural, rational and real numbers, respectively. For $0 < n \in \mathbb{N}$, write $[n] := \{1, 2, \dots, n\}$.

\mathbb{F} denotes an arbitrary field (finite or infinite, algebraically closed or not). \mathbb{F}^\times is the multiplicative group of \mathbb{F} . For a prime power q , we denote by \mathbb{F}_q the finite field of order q . We write $\sqrt{a} \in \mathbb{F}$ to mean that $a \in \mathbb{F}$ is a square, i.e. there exists $x \in \mathbb{F}$ with $x^2 = a$. In this paper, it will cause no confusion to write \sqrt{a} for any of $\pm x$.

$\mathbb{F}[X_1, \dots, X_d]$ denotes the polynomial ring over \mathbb{F} in d indeterminates. Typically, we have $d \geq 2$. For $\delta \in \mathbb{N}$, let $\mathbb{F}[X_1, \dots, X_d]_\delta$ denote the set of homogeneous polynomials $f \in \mathbb{F}[X_1, \dots, X_d]$ of degree δ , i.e. every monomial in f with nonzero coefficient has total degree exactly δ . Denote the *homogenisation* $f^* \in \mathbb{F}[X_0, \dots, X_d]_\delta$ of $f \in \mathbb{F}[X_1, \dots, X_d]$ of degree δ by $x_0^\delta f(x_1/x_0, \dots, x_d/x_0) = f^*(x_0, \dots, x_d)$. Conversely, the *dehomogenisation* $F_* \in \mathbb{F}[X_1, \dots, X_d]$ of $F \in \mathbb{F}[X_0, \dots, X_d]_\delta$ is given by $F_*(x_1, \dots, x_d) = F(1, x_1, \dots, x_d)$.

2.2 Classical algebraic geometry

For completeness, we recall some standard material that can be found for example in [Har95].

Affine and projective varieties Let \mathbb{F} be an arbitrary field and $d \in \mathbb{N}$.

Definition 2.1 (Affine varieties). Write $\mathbb{A}_{\mathbb{F}}^d := \mathbb{F}^d$ for the d -dimensional affine space over \mathbb{F} . For a subset $I \subseteq \mathbb{F}[X_1, \dots, X_d]$, define the affine variety by $V(I | \mathbb{A}_{\mathbb{F}}^d) := \{x \in \mathbb{A}_{\mathbb{F}}^d : \forall f \in I \quad f(x) = 0\}$. For $f \in \mathbb{F}[X_1, \dots, X_d]$ of degree δ , we call $V(f | \mathbb{A}_{\mathbb{F}}^d) := V(\{f\} | \mathbb{A}_{\mathbb{F}}^d)$ a *hypersurface* of degree δ . *Hyperplanes* are hypersurfaces of degree 1.

Definition 2.2 (Projective varieties). Define the *projective space of dimension d over \mathbb{F}* to be $\mathbb{P}_{\mathbb{F}}^d := (\mathbb{F}^{d+1} \setminus \{0\}) / \sim$ where $x \sim y$ if there is $\lambda \in \mathbb{F}^\times$ so that $x = \lambda y$. Denote the \sim -equivalence class of $(x_0, \dots, x_d) \in \mathbb{F}^{d+1} \setminus \{0\}$ by $[x_0 : \dots : x_d] \in \mathbb{P}_{\mathbb{F}}^d$. For a set $I \subseteq \mathbb{F}[X_0, \dots, X_d]$ of

homogeneous polynomials, write $V(I|\mathbb{P}_{\mathbb{F}}^d) := \{[x_0 : \dots : x_d] \in \mathbb{P}_{\mathbb{F}}^d : \forall f \in I \quad f(x_0, \dots, x_1) = 0\}$ for the projective variety. Hypersurfaces and hyperplanes are defined analogously.

Definition 2.3. For a projective variety $Z = V(I|\mathbb{P}_{\mathbb{F}}^d)$, write $Z_0 := V(\{F_* : F \in I\}|\mathbb{A}_{\mathbb{F}}^d)$ for the corresponding affine variety. Write $Z_{\infty} := \overline{Z} \cap V(X_0|\mathbb{P}_{\mathbb{F}}^d) = \{[x_0 : \dots : x_d] \in \overline{Z} : x_0 = 0\}$ for the *ideal point* of Z . Inversely, for an affine variety $Y := V(I|\mathbb{A}_{\mathbb{F}}^d)$, write $\overline{Y} := V(\{f_* : f \in I\}|\mathbb{P}_{\mathbb{F}}^d)$ for the *projective closure* of Y . Let $Y_{\infty} := (\overline{Y})_{\infty}$. If the name of the affine variety is Y_0 (to emphasise its affine nature), we sometimes implicitly mean $Y := \overline{Y}$ and consequently $Y_{\infty} := (Y_0)_{\infty}$. For any field extension $\mathbb{F} \leq \mathbb{K}$, write $Y(\mathbb{K}) := V(I|\mathbb{P}_{\mathbb{K}}^d)$.

Remark 2.4. The two constructions are inverses of each other: $Y = (\overline{Y})_0$ and $\overline{Z_0} = Z$. Furthermore, there is a bijection $Z_0 \rightarrow Z \setminus Z_{\infty}$ given by $(x_1, \dots, x_d) \mapsto [1 : x_1 : \dots : x_d]$, whose inverse is $[x_0 : \dots : x_d] \mapsto (x_1/x_0, \dots, x_d/x_0)$.

Bézout's theorem We need to bound the number of intersection points of varieties. Denote the degree of a variety Z by $\deg(Z)$, i.e. the number of points of intersection of Z and a generic $\dim(Z)$ -codimensional subspace.

Theorem 2.5 (Bézout's theorem in complementary dimension, [Har95, Theorem 18.4]). *Let \mathbb{F} be an algebraically closed field. Let $C, S \subseteq \mathbb{P}_{\mathbb{F}}^d$ be irreducible varieties with $\dim(C) + \dim(S) = d$ and $\dim(C \cap S) = 0$. Then $\sum_{P \in C \cap S} m(P) = \deg(C) \cdot \deg(S)$ where $m(P) \in \mathbb{Z}_+$ is the multiplicity of the intersection point P .*

We need the following special case about the intersection of affine curves and hypersurfaces.

Corollary 2.6. *Let \mathbb{F} be an arbitrary field. Let $C_0 \subseteq \mathbb{A}_{\mathbb{F}}^d$ be an irreducible curve and $S_0 \subset \mathbb{A}_{\mathbb{F}}^d$ be a hypersurface. If $C_0 \not\subseteq S_0$, then*

$$|C_0 \cap S_0| \leq \deg(C_0) \cdot \deg(S_0) - |C_{\infty} \cap S_{\infty}|.$$

Proof. Write $C := \overline{C_0}$ and $S := \overline{S_0}$ for the projective closures, and $\overline{\mathbb{F}}$ for an algebraic closure of \mathbb{F} . Note that $\dim(C(\overline{\mathbb{F}})) + \dim(S(\overline{\mathbb{F}})) = d$ and $\dim(C(\overline{\mathbb{F}}) \cap S(\overline{\mathbb{F}})) = 0$ as $C_0 \not\subseteq S_0$. Then Definition 2.3, Remark 2.4 and Theorem 2.5 shows that $|C_0 \cap S_0| + |C_{\infty} \cap S_{\infty}| = |C \cap S| \leq |C(\overline{\mathbb{F}}) \cap S(\overline{\mathbb{F}})| \leq \deg(C(\overline{\mathbb{F}})) \cdot \deg(S(\overline{\mathbb{F}})) = \deg(C_0) \cdot \deg(S_0)$ and the statement follows. \square

Rational normal curves Our construction uses the following standard properties of the rational normal curves. For completeness, we include a short proof for the ones we actually need. For further details, see [Har95, §1, §18].

Definition 2.7 (Rational normal curve, [Har95, Example 1.14.]). The image of the so called, *Veronese map*

$$\nu_d : \mathbb{P}_{\mathbb{F}}^1 \rightarrow \mathbb{P}_{\mathbb{F}}^d, \quad [x_0 : x_1] \mapsto [x_0^d : x_0^{d-1}x_1 : x_0^{d-2}x_1^2 : \dots : x_1^d]$$

is a degree d irreducible rational curve $\text{im}(\nu_d) \subseteq \mathbb{P}_{\mathbb{F}}^d$. A curve $C \subseteq \mathbb{P}_{\mathbb{F}}^d$ is *rational normal*, if it is projectively equivalent to $\text{im}(\nu_d)$, i.e. if there is a linear automorphism $\varphi \in \text{PGL}(d+1, \mathbb{F})$ of $\mathbb{P}_{\mathbb{F}}^d$ such that $C = \text{im}(C_d)$.

Remark 2.8. This curve is given by $\text{im}(\nu_d) = V(\{X_i X_j - X_{i-1} X_{j+1} : 1 \leq i \leq j \leq d-1\}|\mathbb{P}_{\mathbb{F}}^d)$, see [Har95, Exercise 5.4].

Points $P_0, \dots, P_k \in \mathbb{P}_{\mathbb{F}}^d$ are *in general position*, if there is no (linear) subspace Y of dimension $k-1$ with $P_i \in Y$ for all $0 \leq i \leq k$.

Lemma 2.9 (Standard properties of rational normal curves). *Any rational normal curve $C \subseteq \mathbb{P}_{\mathbb{F}}^d$ satisfies the following properties.*

1. *Arbitrary (pairwise different) points $P_0, \dots, P_d \in C$ are in general position, i.e. they generate $\mathbb{P}_{\mathbb{F}}^d$. Equivalently, we have $|C \cap H| \leq d$ for any hyperplane $H \subset \mathbb{P}_{\mathbb{F}}^d$.*
2. *The Veronese map $\nu_d: \mathbb{P}_{\mathbb{F}}^1 \rightarrow \mathbb{P}_{\mathbb{F}}^d$ is injective. In particular $|C| = |\mathbb{F}| + 1$.*

Proof. Let $Q_i = \nu_d([a_i, b_i])$ (for $0 \leq i \leq d$) for pairwise different $[a_i : b_i] \in \mathbb{P}_{\mathbb{F}}^1$. Then Q_0, \dots, Q_d are in general position if and only if the matrix $A = (a_i^j b_i^{d-j}) \in \mathbb{F}^{(d+1) \times (d+1)}$ (for $0 \leq i, j \leq d$) is invertible. To conclude both parts, note that this Vandermonde-like determinant factorises as $\det(A) = \prod_{i \neq k} \det \begin{pmatrix} a_i & b_i \\ a_k & b_k \end{pmatrix}$. \square

Remark 2.10. If $K \subseteq \mathbb{P}_{\mathbb{F}}^d$ is an irreducible non-degenerate (not contained in any hyperplane) curve, then $\deg(K) \geq d$ with equality if and only if K is a rational normal curve, [Har95, Proposition 18.9]. In particular, Point 1 of Lemma 2.9 actually characterises rational normal curves.

Since lower degree curves give better constructions for our main problem, Remark 2.10 motivates the study of rational normal curves. Fortunately, one can interpolate such a curve to given points rather freely.

Lemma 2.11. *If $|\mathbb{F}| \geq d - 1$ and $P_1, \dots, P_d \in \mathbb{P}_{\mathbb{F}}^d$ are points in general position, then there exists a rational normal curve $C \subseteq \mathbb{P}_{\mathbb{F}}^d$ such that $P_i \in C$ for every $1 \leq i \leq d$.*

Proof. If $|\mathbb{F}| + 1 = |\mathbb{P}_{\mathbb{F}}^1| \geq d$, then we may pick pairwise different points $R_1, \dots, R_d \in \mathbb{P}_{\mathbb{F}}^1$. Then $Q_i = \nu_d(R_i) \in \text{im}(\nu_d)$ (for $1 \leq i \leq d$) are pairwise different points in general position by Lemma 2.9. Then there is $\varphi \in \text{PGL}(d+1, \mathbb{F})$ such that $\varphi(Q_i) = P_i$ for every $1 \leq i \leq d$. This means that $C = \varphi(\text{im}(\nu_d))$ satisfies the statement. \square

Remark 2.12. Actually, any $d+3$ points of $\mathbb{P}_{\mathbb{F}}^d$ in general position determines a *unique* rational normal curve in $\mathbb{P}_{\mathbb{F}}^d$, see [Har95, Theorem 1.18].

Affine varieties over finite fields The next statement controls the cardinality of varieties over finite fields.

Theorem 2.13 (Warning's second theorem, [CW35, Satz 3]). *Let \mathbb{F} be a finite field. Let $f_1, \dots, f_m \in \mathbb{F}[X_1, \dots, X_d]$ with $\delta = \sum_{i=1}^m \deg(f_i)$. Then $V(\{f_1, \dots, f_m\} | \mathbb{A}_{\mathbb{F}}^d)$ is either empty or has cardinality at least $|\mathbb{F}|^{d-\delta}$.*

Corollary 2.14. *If \mathbb{F} is a finite field and $Q \in \mathbb{F}[X_1, \dots, X_d]_2$, then $|V(Q | \mathbb{A}_{\mathbb{F}}^d)| \geq |\mathbb{F}|^{d-2}$*

Proof. If $Q = 0$, then the statement is clear. Otherwise note that $(0, \dots, 0) \in V(Q | \mathbb{A}_{\mathbb{F}}^d)$ as Q is homogeneous. Thus Theorem 2.13 implies the statement as $\delta = \deg(Q) = 2$. \square

2.3 Classical number theory

Quadratic residues As a technical tool, we need the following exercise.

Lemma 2.15. *Let $\Delta \in \mathbb{Z} \setminus \{0\}$, and $p \in \mathbb{N}$ be a prime with $p \equiv 1 \pmod{4|\Delta|}$. Then $\sqrt{\Delta} \in \mathbb{F}_p$.*

Proof. Note that $p \equiv 1 \pmod{4}$ by assumption, hence $\sqrt{-1} \in \mathbb{F}_p$ by [Apo76, Theorem 9.4]. Let ℓ be a prime divisor of Δ with odd multiplicity. To finish, we claim that $\sqrt{\ell} \in \mathbb{F}_p$. Indeed, if $\ell = 2$, then $8 \mid 4\Delta \mid p-1$, in which case $\sqrt{\ell} = \sqrt{2} \in \mathbb{F}_p$ by [Apo76, Theorem 9.5]. Otherwise, ℓ is an odd prime, so the quadratic reciprocity ([Apo76, Theorem 9.8]) gives $\left(\frac{\ell}{p}\right) = \left(\frac{p}{\ell}\right)$ keeping in mind that $p \equiv 1 \pmod{4}$. But $\ell \mid 4\Delta \mid p-1$, i.e. $p \equiv 1 \pmod{\ell}$, thus the Legendre symbol evaluates to $\left(\frac{p}{\ell}\right) = \left(\frac{1}{\ell}\right) = 1$. This means that $\sqrt{\ell} \in \mathbb{F}_p$ as claimed. \square

Distribution of prime numbers We use the following weak form of distribution of primes (in arithmetic progressions).

Theorem 2.16 (Weak form of the Prime number theorem, cf. [Apo76, §4]). *For every $\varepsilon > 0$, there exists N_ε , such that for every $n \geq N_\varepsilon$, there is a prime number p satisfying $(1 - \varepsilon)n \leq p \leq n$.*

Theorem 2.17 (Weak form of Dirichlet's theorem, cf. [Apo76, §7]). *For every $\varepsilon > 0$, $1 \leq m \in \mathbb{Z}$, and $a \in \mathbb{N}$ with $\gcd(m, a) = 1$, there is $N_{\varepsilon, a, m} \in \mathbb{N}$ such that for every $n \geq N_{\varepsilon, a, m}$, there is a prime number p satisfying $(1 - \varepsilon)n \leq p \leq n$ with $p \equiv a \pmod{m}$.*

3 Q -quadrics

This section introduces a fundamental notion for this paper. We generalise the notion of hyperspheres to Q -quadrics where Q is a quadratic form. (Various choices of Q produce families of quadratic hypersurfaces ‘similar’ to each other, e.g. hyperspheres, hyperellipsoids and hyperparaboloids with given axes direction and ratios.) We discuss some properties of Q -quadrics that will be used in §4 in the constructions.

Definition 3.1. Let $Q \in \mathbb{F}[X_1, \dots, X_d]$ be a quadratic form. A subset $S \subseteq \mathbb{A}_{\mathbb{F}}^d$ is called a Q -quadric (over \mathbb{F}) if there is $f \in \mathbb{F}[X_1, \dots, X_d]$ of degree at most 1 such that $S = V(Q + f | \mathbb{A}_{\mathbb{F}}^d)$.

Remark 3.2. Note that for any $\lambda \in \mathbb{F}^\times$, the notion of Q -quadrics and (λQ) -quadrics coincide.

Geometrically, the set of all Q -quadrics contains all scaled and translated images of $V(Q | \mathbb{F})$ and $V(Q - 1 | \mathbb{F})$, but, for example, when the characteristic of \mathbb{F} is 2, it may contain further elements.

The motivating example is $Q = X_1^2 + \dots + X_d^2$, in which case every hypersphere is a Q -quadric. Other Q 's specify certain ellipsoids (with axes pointing to given directions and with given ratios), paraboloids, amongst others.

0-quadrics are hyperplanes and the whole space, so we usually assume $Q \neq 0$.

Remark 3.3. Recall Definition 2.3. For any Q -quadric S , we have $S_\infty = V(\{Q, X_0\} | \mathbb{P}_{\mathbb{F}}^d)$. Note that this is independent of S , and only depends on Q itself. In other words, all Q -quadrics intersect the ideal hyperplane $V(X_0 | \mathbb{P}_{\mathbb{F}}^d)$ in exactly the same points. This will be a crucial property for our construction.

Any $d + 1$ points in general position determine a unique Q -quadric.

Lemma 3.4. *Let $\mathbb{F} \leq \mathbb{K}$ be fields, $Q \in \mathbb{F}[X_1, \dots, X_d]_2$, and $P_0, \dots, P_d \in \mathbb{A}_{\mathbb{F}}^d$ be points in general position. Then there is a unique Q -quadric $S_{\mathbb{K}} \subseteq \mathbb{A}_{\mathbb{K}}^d$ (over the larger field \mathbb{K}) containing every P_i . In fact, $S_{\mathbb{K}} = V(Q + f | \mathbb{A}_{\mathbb{K}}^d)$ for a (unique) $f \in \mathbb{F}[X_1, \dots, X_d]$ of degree at most 1 defined over the smaller field \mathbb{F} .*

Proof. Write $P_i = (a_{i,1}, \dots, a_{i,d}) \in \mathbb{A}_{\mathbb{F}}^d$, let $a_{i,0} := 1$, and define the matrix $A := (a_{i,j}) \in \mathbb{F}^{(d+1) \times (d+1)}$ (for $0 \leq i, j \leq d$). Define $b_i := -Q(P_i) \in \mathbb{F}$ for $0 \leq i \leq d$, and define the vector $b := (b_0, \dots, b_d) \in \mathbb{F}^{d+1}$. For any $f := \alpha_0 + \alpha_1 X_1 + \dots + \alpha_d X_d \in \mathbb{K}[X_1, \dots, X_d]$, assign the vector $x_f := (\alpha_0, \dots, \alpha_d) \in \mathbb{K}^{d+1}$. Now $Ax_f = b$ if and only if $P_i \in V(Q + f | \mathbb{K})$ for every $0 \leq i \leq d$. But since P_0, \dots, P_d are in general position (over \mathbb{F}), the matrix A is invertible (over \mathbb{F}), hence there is a unique solution of the previous equation given by $x_f = A^{-1}b \in \mathbb{F}^{d+1}$ as required. \square

The fact that any d points of $\mathbb{A}_{\mathbb{F}}^d$ lie on a hyperplane together with Lemma 3.4 motivates the following definition.

Definition 3.5. Given a quadratic form $Q \in \mathbb{F}[X_1, \dots, X_d]$, a subset $D \subseteq \mathbb{A}_{\mathbb{F}}^d$ is said to be *Q-generic (over \mathbb{F})* if $|D \cap H| \leq d$ for every hyperplane $H \subset \mathbb{A}_{\mathbb{F}}^d$, and $|D \cap S| \leq d + 1$ for every Q -quadric $S \subset \mathbb{A}_{\mathbb{F}}^d$.

Remark 3.6. A Q -generic set $D \subseteq \mathbb{A}_{\mathbb{F}}^d$ for $Q = X_1^2 + \dots + X_d^2$ is a **sharp no- $(d + 2)$ -on-a-sphere** set, i.e. no $d + 2$ points of S lie on any sphere and no $d + 1$ points lie in a hypersurface.

The next statement is useful when switching to larger fields.

Lemma 3.7. *Let $Q \in \mathbb{F}[X_1, \dots, X_d]_2$. If $D \subseteq \mathbb{A}_{\mathbb{F}}^d$ is Q -generic, then it is also Q -generic over any larger field $\mathbb{K} \geq \mathbb{F}$.*

Proof. By assumption, any distinct points $P_0, \dots, P_d \in D$ are in general positions over \mathbb{F} , but then they are automatically in general position over \mathbb{K} from standard linear algebra.

For the other condition, assume $|D \cap S_{\mathbb{K}}| \geq d + 1$ for some Q -quadric $S_{\mathbb{K}} \subset \mathbb{A}_{\mathbb{K}}^d$ over \mathbb{K} . Now any distinct points $P_0, \dots, P_d \in D \cap S_{\mathbb{K}}$ are in general position over \mathbb{F} by Definition 3.5, so Lemma 3.4 implies that $S_{\mathbb{K}} = V(Q + f | \mathbb{A}_{\mathbb{K}}^d)$ for some $f \in \mathbb{F}[X_1, \dots, X_d]$ defined over the smaller field \mathbb{F} . Thus for the Q -quadric $S_{\mathbb{F}} := V(Q + f | \mathbb{A}_{\mathbb{F}}^d) = S_{\mathbb{K}} \cap \mathbb{A}_{\mathbb{F}}^d$, we have $D \cap S_{\mathbb{K}} = D \cap S_{\mathbb{F}}$. Hence $|D \cap S_{\mathbb{K}}| = |D \cap S_{\mathbb{F}}| \leq d + 1$ by Definition 3.5 as required. \square

4 Constructions and proof of theorems

In this section, we prove the main statements of the paper: Theorem 1.2, Theorem 1.4, Theorem 1.5, and Theorem 1.6. All constructions are based on a carefully chosen rational normal curve. We first discuss the general construction over arbitrary fields (§4.1). Then we show the applicability of this construction for finite fields (§4.2). Finally, from suitable prime fields, we lift back the construction to square grids of the Euclidean space (§4.3).

4.1 Over arbitrary fields

In this section, using projective spaces, we discuss a sufficient condition on the quadratic form Q such that a suitably chosen rational normal curve satisfies the **no- $(d + 2)$ -on- Q -quadric** property. More concretely, this condition is the existence of d independent points from the ideal hyperplane such that every Q -quadric passes through exactly $d - 1$ of these points. Then we show using Bézout's theorem, that any rational normal curve passing through these points has the desired property, as in the affine space, there can be at most $2d - (d - 1) = d + 1$ intersection points left.

Definition 4.1. Call a quadratic form $0 \neq Q \in \mathbb{F}[X_1, \dots, X_d]_2$ is called *rich*, if there exists a vector space basis v_1, \dots, v_d of \mathbb{F}^d such that $Q(v_1) = \dots = Q(v_{d-1}) = 0 \neq Q(v_d)$.

Remark 4.2. Richness is equivalent to the existence of general position points $P_1, \dots, P_d \in V(X_0 | \mathbb{P}_{\mathbb{F}}^d)$ in the ideal hyperplane such that $P_1, \dots, P_{d-1} \in V(Q | \mathbb{P}_{\mathbb{F}}^d)$ and $P_d \notin V(Q | \mathbb{P}_{\mathbb{F}}^d)$, as we may assign $P_i = [0 : v_{i,1} : \dots : v_{i,d}] \in V(X_0 | \mathbb{P}_{\mathbb{F}}^d)$ to the vector $v_i = (v_{i,1}, \dots, v_{i,d}) \in \mathbb{F}^p$.

Remark 4.3. If \mathbb{F} is algebraically closed, then by Hilbert's Nullstellensatz every $0 \neq Q \in \mathbb{F}[X_1, \dots, X_d]$ is rich. However, this is not true in general. For example, in the case $\mathbb{F} = \mathbb{R}$, $d \geq 2$, pick $m \geq 1$, and $0 < \lambda_i \in \mathbb{R}$, $L_i \in \mathbb{R}[X_1, \dots, X_d]_1$ arbitrarily for any $i \in \{1, \dots, m\}$. Then the quadratic form $Q = \sum_{i=1}^m \lambda_i L_i^2$ is not rich (as $V(Q | \mathbb{A}_{\mathbb{R}}^d)$ contains a single point).

We can construct Q -generic sets for rich Q 's of linear size in $|\mathbb{F}|$.

Proposition 4.4 (Constructing Q -generic sets). *Let \mathbb{F} be an arbitrary field, and $0 \neq Q \in \mathbb{F}[X_1, \dots, X_d]_2$ be a rich quadratic form where $d \leq |\mathbb{F}| + 1$. Then there is a Q -generic subset $C_0 \subseteq \mathbb{A}_{\mathbb{F}}^d$ with $|C_0| = |\mathbb{F}| + 1 - d$.*

In fact, C_0 may be taken to be the affine part of a suitable rational normal curve over \mathbb{F} .

Proof. Let $P_1, \dots, P_d \in V(X_0 | \mathbb{P}_{\mathbb{F}}^d)$ be the general position points as in Remark 4.2. Let C be the degree d rational normal curve through these P_1, \dots, P_d provided by Lemma 2.11. We claim that the affine part $C_0 \subseteq \mathbb{A}_{\mathbb{F}}^d$ satisfies the statement.

Indeed, to check the first condition of condition of Definition 3.5, let $H_0 \subset \mathbb{A}_{\mathbb{F}}^d$ be a hyperplane (which is a hypersurface of degree 1). Then $|C_0 \cap H_0| \leq \deg(C_0) \cdot \deg(H_0) = d$ by Corollary 2.6 and Lemma 2.9.

To check the other condition, let $S_0 \subseteq \mathbb{A}_{\mathbb{F}}^d$ be a Q -quadric. We have $S_{\infty} = V(\{Q, X_0\} | \mathbb{P}_{\mathbb{F}}^d)$ by Remark 3.3, so Remark 4.2 implies that $P_1, \dots, P_{d-1} \in S_{\infty}$ and $P_d \notin S_{\infty}$, therefore we have $\overline{C_0} \not\subseteq \overline{S_0}$, i.e. $C_0 \not\subseteq S_0$. Next note that $C_{\infty} = \{P_1, \dots, P_d\}$ by construction and Lemma 2.11, hence $C_{\infty} \cap S_{\infty} = \{P_1, \dots, P_{d-1}\}$. Thus, Corollary 2.6 gives $|C_0 \cap S_0| \leq \deg(C_0) \cdot \deg(S_0) - |C_{\infty} \cap S_{\infty}| = 2d - |\{P_1, \dots, P_{d-1}\}| = d + 1$ as required.

Finally, note that $|\overline{C_0}| = |\mathbb{P}_{\mathbb{F}}^1| = |\mathbb{F}| + 1$ by Definition 2.7 and $|C_{\infty}| = |\{P_1, \dots, P_d\}| = d$ by above, so $|C_0| = |\overline{C_0}| - |C_{\infty}| = |\mathbb{F}| + 1 - d$ by Remark 2.4 as required. \square

4.2 Over finite fields

In this section, we show that the sufficient condition of §4.1 for finite fields is almost always satisfied. The only exception is when the quadratic form is irreducible and has rank 2. In every other case, we use the general construction of §4.1 to obtain **no- $(d+2)$ -on- Q -quadric** and **sharp no- $(d+2)$ -on-a-sphere** sets of linear size over finite fields, thereby proving Theorem 1.5 and Theorem 1.6.

If we consider only hyperspheres, i.e. $Q = X_1^2 + \dots + X_d^2$, then it is easy to show that if $\sqrt{-1} \in \mathbb{F}$, then Q is rich by considering the cyclic permutations of the point $(1, \sqrt{-1}, 0, \dots, 0) \in V(Q | \mathbb{A}_{\mathbb{F}}^d)$, cf. CITE. Classifying rich quadratic forms over finite fields is not much harder.

Lemma 4.5. *If \mathbb{F} is finite, then every quadratic form $0 \neq Q \in \mathbb{F}[X_1, \dots, X_d]_2$ is either rich or is irreducible of rank 2.*

Remark 4.6. Irreducible rank 2 quadratic forms can be given explicitly by $Q = \lambda_{1,1}L_1^2 + \lambda_{1,2}L_1L_2 + \lambda_{2,2}L_2^2$ for \mathbb{F} -linearly independent $L_1, L_2 \in \mathbb{F}[X_1, \dots, X_d]_1$ and $\lambda_{i,j} \in \mathbb{F}$ such that $\sqrt{\Delta} \notin \mathbb{F}$ for the the discriminant $\Delta = \lambda_{1,2}^2 - 4\lambda_{1,1}\lambda_{2,2} \in \mathbb{F}$.

Proof. Let $V_Q := V(Q | \mathbb{A}_{\mathbb{F}}^d)$. By Corollary 2.14, we have $|V_Q| \geq |\mathbb{F}|^{d-2}$. Considering the cardinalities show that $\dim(\text{span}_{\mathbb{F}}(V_Q)) \geq d - 2$ with equality if and only if $V_Q \subseteq \mathbb{A}_{\mathbb{F}}^d$ is a $(d - 2)$ -dimensional linear subspace. Thus Q fails to be rich if and only if V_Q is a 2-codimensional subspace. In this case, after an appropriate change of base of $\mathbb{F}[X_1, \dots, X_d]$ from $\{X_1, \dots, X_d\}$ to degree 1 homogeneous polynomials $\{L_1, \dots, L_d\}$, we may assume that this subspace is given by $L_1 = L_2 = 0$. Denote by $Q_1 \in \mathbb{F}[L_1, \dots, L_d]$ the resulting quadratic form in the new basis. Then i.e. that $Q_1(y_1, \dots, y_d) = 0$ if and only if $y_1 = y_2 = 0$. Write

$$Q_1 = \sum_{1 \leq i \leq j \leq d} \lambda_{i,j} L_i L_j$$

for suitable $\lambda_{i,j} \in \mathbb{F}$. Let $e_i \in \mathbb{A}_{\mathbb{F}}^d$ where the i th entry is 1, all others are 0 (in the new basis). Note that $Q_1(e_i + \mu e_j) = \lambda_{i,i} + \mu \lambda_{i,j} + \mu^2 \lambda_{j,j}$ for every $i < j$ and $\mu \in \mathbb{F}$. Using this with $3 \leq i < j$ and $\lambda \in \{0, 1\}$, we see that $\lambda_{i,j} = 0$ for every $3 \leq i \leq j$. Then for $i \in \{1, 2\}$, $3 \leq j$ and arbitrary $\mu \in \mathbb{F}$, we have $0 \neq Q_1(e_i, \mu e_j) = \lambda_{i,i} + \mu \lambda_{i,j}$ which forces $\lambda_{i,j} = 0$. Now $Q_1 = \lambda_{1,1}L_1^2 + \lambda_{1,2}L_1L_2 + \lambda_{2,2}L_2^2$. Finally $0 \neq Q_1(e_1 + \mu e_2) = \lambda_{1,1} + \mu \lambda_{1,2} + \mu^2 \lambda_{2,2}$ holds for every $\mu \in \mathbb{F}$, i.e. the discriminant $\lambda_{1,2}^2 - 4\lambda_{1,1}\lambda_{2,2} \in \mathbb{F}$ (of this quadratic expression in μ) must not be a square in \mathbb{F} . Going back to the original basis gives the statement. \square

We are ready to prove the main statements about finite fields.

Proof of Theorem 1.5. Q is rich by Lemma 4.5, so Proposition 4.4 gives the statement. \square

Proof of Theorem 1.6. Let $Q = X_1^2 + \dots + X_d^2$. Note that Q -quadrics are the hyperspheres in $\mathbb{A}_{\mathbb{F}}^d$, see Remark 3.2. Since $\sqrt{-1} \notin \mathbb{F}$ if and only if $|\mathbb{F}| \not\equiv 3 \pmod{4}$, Remark 4.6 and Theorem 1.5 give the statement. \square

4.3 In finite square grids of \mathbb{R}^d

In this final section, we prove the remaining main statements of the paper (Theorem 1.2, Theorem 1.4). We consider a large prime $p \leq n$ (satisfying some technical conditions) and work in a d -dimensional grid of size p^d . We show that the solutions for $\mathbb{A}_{\mathbb{F}_p}^d$ can be lifted to the Euclidean plane, such that every hyperplane and Q -quadric with rational or real coefficients intersect our construction in more points than prescribed.

Definition 4.7. Let p be a prime. Write $\mathbb{F}_p := \mathbb{Z}/(p)$ and let $\pi_p: \mathbb{Z} \rightarrow \mathbb{F}_p$ be the natural projection. Write $\pi_p^d: \mathbb{Z}^d \rightarrow \mathbb{A}_{\mathbb{F}_p}^d$ for the induced map. Define a map (of sets) $\varrho_p: \mathbb{Q}[X_1, \dots, X_d] \rightarrow \mathbb{F}_p[X_1, \dots, X_d]$ as follows. Let $\varrho_p(0) := 0$. For $0 \neq F$, let $r \in \mathbb{Q}^\times$ be (the unique rational) so that rF has integer coefficients whose greatest common divisor is 1. We obtain $\varrho_p(F) \neq 0$ from rF by replacing the coefficients by their image under π_p .

Lemma 4.8. Let p be a prime number. Assume that $D_p \subseteq \mathbb{A}_{\mathbb{F}_p}^d$ is a Q_p -generic for some $Q_p \in \mathbb{F}_p[X_1, \dots, X_d]_2$. Define $D \subseteq \{1, 2, \dots, p\}^d$ by $\pi_p^d(D) = D_p$ and pick $Q \in \mathbb{Q}[X_1, \dots, X_d]$ so that $\varrho_p(Q) = Q_p$. Then $D \subset \mathbb{R}^d$ is Q -generic over \mathbb{R} with $|D| = |D_p|$.

Proof. By Lemma 3.7, it is enough to show that D is Q -generic over \mathbb{Q} . To prove the latter one, we claim that for any $F \in \mathbb{Q}[X_1, \dots, X_d]$, we have $|\{x \in D : F(x) = 0\}| \leq |\{y \in D_p : \varrho_p(F)(y) = 0\}|$. Indeed, if $F(x) = 0 \in \mathbb{Q}^d$, then $rF(x) = 0 \in \mathbb{Z}^d$, so $\varrho_p(F)(y) = 0 \in \mathbb{A}_{\mathbb{F}_p}^d$ for $y := \pi_p^d(x) \in D_p$ which is uniquely determined by x .

Let $H = V(f|_{\mathbb{A}_{\mathbb{Q}}^d})$ be an arbitrary hyperplane (in $\mathbb{A}_{\mathbb{Q}}^d$) given by the degree 1 polynomial $f \in \mathbb{Q}[X_1, \dots, X_d]$. If $\deg(\varrho_p(f)) = 1$, then $H_p := V(\varrho_p(f)|_{\mathbb{A}_{\mathbb{F}_p}^d})$ is also hyperplane (in $\mathbb{A}_{\mathbb{F}_p}^d$), so the claim shows that $|D \cap H| \leq |D_p \cap H_p| \leq d$ using the assumption of D_p being Q_p -generic. Otherwise, by Definition 4.7, $\varrho_p(f)$ is a non-zero constant polynomial, hence f has no solution on \mathbb{Z}^d , thus we have $|D \cap H| = 0 \leq d$ in this case as well.

Finally, $S = V(Q + f|_{\mathbb{A}_{\mathbb{Q}}^d})$ be an arbitrary Q -quadric (over \mathbb{Q}) given by the polynomial $f \in \mathbb{Q}[X_1, \dots, X_d]$ of degree at most 1. Let $F := Q + f$ and define $F_p := \varrho_p(F)$. If $\deg(\varrho_p(Q + f)) = 2$, then $S_p := V(\varrho_p(Q + f)|_{\mathbb{A}_{\mathbb{F}_p}^d})$ is a Q_p -quadric (as $\varrho_p(Q + f) = \varrho_p(Q) + \varrho_p(f)$), so $|D \cap S| \leq |D_p \cap S_p| \leq d + 1$ as above using that D_p is Q_p -generic. If $\deg(\varrho_p(Q + f)) \leq 1$, then $S_p = V(\varrho_p(f)|_{\mathbb{A}_{\mathbb{F}_p}^d})$, so we have $|D \cap S| \leq d \leq d + 1$ as above. \square

Proposition 4.9. Fix a quadratic form $0 \neq Q \in \mathbb{Q}[X_1, \dots, X_d]_2$. Then for every $0 < \varepsilon \leq 1$ there exists $N = N(\varepsilon, Q, d) \in \mathbb{N}$ such that whenever $n \geq N$, there is Q -generic set $D \subseteq \{1, 2, \dots, n\}^d$ over \mathbb{Q} of size $|D| \geq (1 - \varepsilon)n$.

Proof. First, consider the case when Q is not irreducible of rank 2, see Remark 4.6. By Remark 3.2, we may assume that $Q = \sum_{1 \leq i \leq j \leq d} \lambda_{i,j} X_i X_j \in \mathbb{Z}[X_1, \dots, X_d]_2$. Let $C_Q := \{2|\lambda_{i,j}| + 1 : 1 \leq i \leq j \leq d\}$. We claim that $N := \max\{N_{\varepsilon/2}, C_Q, 2(d-1)/\varepsilon\}$ satisfies the statement where $N_{\varepsilon/2}$ is from Theorem 2.16.

Indeed, let $n \geq N$. By Theorem 2.16, pick a prime number p with $(1 - \varepsilon/2)n \leq p \leq n$. As $n \geq C_Q$, the quadratic form $Q_p := \varrho_p(Q) \in \mathbb{F}_p[X_1, \dots, X_d]_2$ is not irreducible of rank 2, because Q is not. Since $n \geq 2(d-1)/\varepsilon$, we see that $|\mathbb{F}_p| + 1 - d \geq (1 - \varepsilon/2)n + (\varepsilon/2)n = (1 - \varepsilon)n \geq 0$, hence Theorem 1.5 produces a Q_p -generic set $D_p \subseteq \mathbb{A}_{\mathbb{F}_p}^d$ of size $|D_p| = p + 1 - d$. Thus Lemma 4.8 produces a Q -generic set $D \subseteq \{1, \dots, p\}^d$ over \mathbb{R} of size $|D| = |D_p| = p + 1 - d \geq (1 - \varepsilon)n$ as required.

The case when Q is irreducible of rank 2 is analogous to the following slight variation. Write Δ for the discriminant of Q from Remark 4.6, and this time use Theorem 2.17 to get a suitable prime p satisfying $p \equiv 1 \pmod{4|\Delta|}$ with $(1 - \varepsilon/2)n \leq p \leq n$ $p \leq (1 - \varepsilon = 2)n$. Now Lemma 2.15 and Remark 4.6 shows that the quadratic form $Q_p \in \mathbb{F}_p[X_1, \dots, X_d]$ is of degree 2, but is reducible. Thus Theorem 1.5 is applicable and finishes the proof as above. \square

With this, the proof of the main statements are complete.

Proof of Theorem 1.4. This is a reformulation of Proposition 4.9. \square

Proof of Theorem 1.2. This follows from Theorem 1.4 in the case $Q = X_1^2 + \dots + X_d^2$. \square

5 Open problems

It is a natural open problem to find the exact value of $f([n]^d, \mathbb{R}^d)$ from Problem 1.1, or more generally, the exact value of $f_Q([n]^d, \mathbb{R}^d)$ from Problem 1.3. In fact, any improvement in the bounds of Theorem 1.2 and Theorem 1.4 would be interesting and quite possibly requires new ideas. Similar questions arise for the finite field analogue (Theorem 1.5), where improving the bounds to $f_Q(\mathbb{F}^d, \mathbb{F}^d)$ may be easier.

References

- [Apo76] Tom M Apostol. *Introduction to analytic number theory*. en. 2nd ed. Undergraduate texts in mathematics. Berlin, Germany: Springer, Jan. 1976 (cit. on pp. 7, 8).
- [BK03] Peter Braß and Christian Knauer. ‘On counting point-hyperplane incidences’. In: *Computational Geometry* 25.1-2 (2003), pp. 13–20 (cit. on p. 2).
- [BMP05] Peter Brass, William O. J. Moser and János Pach. ‘Lattice Point Problems’. In: *Research Problems in Discrete Geometry*. New York, NY: Springer New York, 2005, pp. 417–433. ISBN: 978-0-387-29929-7. DOI: 10.1007/0-387-29929-7_11. URL: https://doi.org/10.1007/0-387-29929-7_11 (cit. on p. 2).
- [CW35] Herrn Chevalley and Ewald Warning. ‘Bemerkung zur vorstehenden Arbeit’. de. In: *Abh. Math. Semin. Univ. Hambg.* 11.1 (Dec. 1935), pp. 76–83 (cit. on p. 7).
- [DX25] Zichao Dong and Zijian Xu. *Large grid subsets without many cospherical points*. 2025. arXiv: 2506.18113 [math.CO]. URL: <https://arxiv.org/abs/2506.18113> (cit. on pp. 2–4).
- [Dud17] Henry E Dudeney. *Amusements in mathematics*. Vol. 473. Courier Corporation, 1917 (cit. on p. 2).
- [Epp18] David Eppstein. *Forbidden configurations in discrete geometry*. Cambridge University Press, 2018 (cit. on p. 2).
- [Fla98] Achim Flammenkamp. ‘Progress in the no-three-in-line problem, II’. In: *Journal of Combinatorial Theory, Series A* 81.1 (1998), pp. 108–113 (cit. on p. 2).
- [GGK25] Anubhab Ghosal, Ritesh Goenka and Peter Keevash. *On subsets of lattice cubes avoiding affine and spherical degeneracies*. 2025. arXiv: 2509.06935 [math.CO]. URL: <https://arxiv.org/abs/2509.06935> (cit. on p. 2).
- [GK25] Alexandr Grebennikov and Matthew Kwan. *No-(k+1)-in-line problem for large constant k*. 2025. arXiv: 2510.17743 [math.CO]. URL: <https://arxiv.org/abs/2510.17743> (cit. on p. 2).
- [Gre] Ben Green. ‘100 open problems’. Manuscript, available on request to Professor Green (cit. on p. 2).

- [Guy04] Richard Guy. *Unsolved problems in number theory*. Vol. 1. Springer Science & Business Media, 2004 (cit. on p. 2).
- [GK68] Richard K. Guy and Patrick A. Kelly. ‘The no-three-in-line problem’. In: *Canadian Mathematical Bulletin* 11 (1968), pp. 527–531. ISSN: 0008-4395. DOI: 10.4153/CMB-1968-062-3. URL: <https://doi.org/10.4153/CMB-1968-062-3> (cit. on p. 2).
- [HJSW75] Richard R Hall, Terence H Jackson, Anthony Sudbery and Ken Wild. ‘Some advances in the no-three-in-line problem’. In: *Journal of Combinatorial Theory, Series A* 18.3 (1975), pp. 336–341 (cit. on pp. 2, 4).
- [Har95] Joe Harris. *Algebraic geometry*. en. 1st ed. Graduate Texts in Mathematics. New York, NY: Springer, Dec. 1995 (cit. on pp. 5–7).
- [KT+25] Sandi Klavžar, James Tuite et al. ‘The General Position Problem: A Survey’. In: *arXiv preprint arXiv:2501.19385* (2025) (cit. on p. 2).
- [KNS25a] Benedek Kovács, Zoltán Lóránt Nagy and Dávid R. Szabó. *Randomised algebraic constructions for the no- $(k + 1)$ -in-line problem*. 2025. arXiv: 2508.07632 [math.CO]. URL: <https://arxiv.org/abs/2508.07632> (cit. on p. 2).
- [KNS25b] Benedek Kovács, Zoltán Lóránt Nagy and Dávid R. Szabó. *Settling the no- $(k + 1)$ -in-line problem when k is not small*. 2025. arXiv: 2502.00176 [math.CO]. URL: <https://arxiv.org/abs/2502.00176> (cit. on p. 2).
- [Lef08] Hanno Lefmann. ‘No 1 Grid-Points in Spaces of Small Dimension’. In: *Algorithmic Aspects in Information and Management*. Ed. by Rudolf Fleischer and Jinhui Xu. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 259–270. ISBN: 978-3-540-68880-8 (cit. on p. 2).
- [NNW23] Dániel T Nagy, Zoltán Lóránt Nagy and Russ Woodroffe. ‘The extensible No-Three-In-Line problem’. In: *European Journal of Combinatorics* 114 (2023), p. 103796 (cit. on p. 2).
- [PW07] Attila Pór and David R Wood. ‘No-Three-in-Line-in-3D’. In: *Algorithmica* 47.4 (2007), pp. 481–488 (cit. on p. 2).
- [SW24] Andrew Suk and Ethan Patrick White. *A note on the no- $(d + 2)$ -on-a-sphere problem*. 2024. arXiv: 2412.02866 [math.CO]. URL: <https://arxiv.org/abs/2412.02866> (cit. on p. 2).
- [SZ25] Andrew Suk and Ji Zeng. *On higher dimensional point sets in general position*. 2025. arXiv: 2211.15968 [math.CO]. URL: <https://arxiv.org/abs/2211.15968> (cit. on p. 2).
- [Thi95a] Torsten Thiele. ‘Geometric selection problems and hypergraphs’. PhD thesis. Freie Universität Berlin, 1995 (cit. on pp. 2–4).
- [Thi95b] Torsten Thiele. ‘The no-four-on-circle problem’. In: *Journal of Combinatorial Theory, Series A* 71.2 (1995), pp. 332–334 (cit. on pp. 2, 3).