# An upper bound for the size of $s$-distance sets in real algebraic sets

Gábor Hegedüs

John von Neumann Faculty of Informatics
Óbuda University
Budapest, Hungary

hegedus.gabor@uni-obuda.hu

Lajos Rónyai*

Institute of Computer Science and Control, Eötvös Loránd Research Network
and Department of Algebra
Budapest University of Technology
Budapest, Hungary

lajos@info.ilab.sztaki.hu

Submitted: Jul 14, 2020; Accepted: Jun 8, 2021; Published: Jul 30, 2021



**Abstract**

In a recent paper, Petrov and Pohoata developed a new algebraic method which combines the Croot-Lev-Pach Lemma from additive combinatorics and Sylvester's Law of Inertia for real quadratic forms. As an application, they gave a simple proof of the Bannai-Bannai-Stanton bound on the size of $s$-distance sets (subsets $\mathcal{A} \subseteq \mathbb{R}^n$ which determine at most $s$ different distances). In this paper we extend their work and prove upper bounds for the size of $s$-distance sets in various real algebraic sets. This way we obtain a novel and short proof for the bound of Delsarte-Goethals-Seidel on spherical $s$-distance sets and a generalization of a bound by Bannai-Kawasaki-Nitamizu-Sato on $s$-distance sets on unions of spheres. In our arguments we use the method of Petrov and Pohoata together with some Gröbner basis techniques.

**Mathematics Subject Classifications:** 52C45, 13P10, 05D99

*Part of this work has been supported by the Hungarian Scientific ResearchFund (grant No. OTKA K115288), and the Hungarian Ministry of Innovation and the National Research, Development and Innovation Office within the framework of the Artificial Intelligence National Laboratory Programme.

## 1 Introduction

Let $\mathcal{A} \subseteq \mathbb{R}^n$ be an arbitrary set. Denote by $d(\mathcal{A})$ the set of non-zero euclidean distances among the points of $\mathcal{A}$:

$$d(\mathcal{A}) := \{d(\mathbf{p}_1, \mathbf{p}_2);\ \mathbf{p}_1, \mathbf{p}_2 \in \mathcal{A},\ \mathbf{p}_1 \neq \mathbf{p}_2\}.$$

An *s-distance set* is a subset $\mathcal{A} \subseteq \mathbb{R}^n$ such that $|d(\mathcal{A})| \leqslant s$. Here we mention just two theorems from the rich area of sets with few distances, more information can be found for example in [14], [3]. Bannai, Bannai and Stanton proved the following upper bound for the size of an $s$-distance set in [4, Theorem 1].

**Theorem 1.** *Let $n, s \geqslant 1$ be integers and suppose that $\mathcal{A} \subseteq \mathbb{R}^n$ is an $s$-distance set. Then*

$$|\mathcal{A}| \leqslant \binom{n+s}{s}.$$

Delsarte, Goethals and Seidel investigated $s$-distance sets on the unit sphere $\mathbb{S}^{n-1} \subseteq \mathbb{R}^n$. These are the *spherical s-distance sets.* They proved a general upper bound for the size of a spherical $s$-distance set in [11]. In their proof they used Delsarte's method (see [3, Subsection 2.2]).

**Theorem 2.** *(Delsarte, Goethals, and Seidel) Let $n, s \geqslant 1$ be integers and suppose that $\mathcal{A} \subseteq \mathbb{S}^{n-1}$ is an $s$-distance set. Then*

$$|\mathcal{A}| \leqslant \binom{n+s-1}{s} + \binom{n+s-2}{s-1}.$$

Before stating our results, we introduce some notation. Let $\mathbb{F}$ be a field. In the following $S = \mathbb{F}[x_1, \ldots, x_n] = \mathbb{F}[\mathbf{x}]$ denotes the ring of polynomials in commuting variables $x_1, \ldots, x_n$ over $\mathbb{F}$. Note that polynomials $f \in S$ can be considered as functions on $\mathbb{F}^n$. For a subset $Y$ of the polynomial ring $S$ and a natural number $s$ we denote by $Y_{\leqslant s}$ the set of polynomials from $Y$ with degree at most $s$. Let $I$ be an ideal of $S = \mathbb{F}[\mathbf{x}]$. The *(affine) Hilbert function* of the factor algebra $S/I$ is the sequence of non-negative integers $h_{S/I}(0), h_{S/I}(1), \ldots,$ where $h_{S/I}(s)$ is the dimension over $\mathbb{F}$ of the factor space $\mathbb{F}[x_1, \ldots, x_n]_{\leqslant s}/I_{\leqslant s}$ (see [8, Section 9.3]). Our main technical result gives an upper bound for the size of an $s$-distance set, which is contained in a given real algebraic set.

**Theorem 3.** *Let $I \subseteq \mathbb{R}[\mathbf{x}]$ be an ideal in the polynomial ring, and let $\mathcal{A} \subseteq \mathbb{R}^n$ be an $s$-distance set such that every polynomial from $I$ vanishes on $\mathcal{A}$. Then*

$$|\mathcal{A}| \leqslant h_{\mathbb{R}[\mathbf{x}]/I}(s).$$

The proof is based on Gröbner basis theory and an improved version of the Croot-Pach-Lev Lemma (see [9] Lemma 1) over the reals. Petrov and Pohoata proved this in [20, Theorem 1.2] and used it to give a new proof of Theorem 1. We generalize their result to give a new upper bound for the size of an $s$-distance set, which is contained in a given affine algebraic set in the real affine space $\mathbb{R}^n$.

We give several corollaries, where Theorem 3 is applied to specific ideals of the polynomial ring $\mathbb{R}[\mathbf{x}]$, the first ones being the principal ideals $I = (F)$, with $F \in \mathbb{R}[\mathbf{x}]$.

**Corollary 4.** *Let $F \in \mathbb{R}[\mathbf{x}]$ be a polynomial of degree $d$. Suppose that $s \geqslant d$. Let $\mathcal{A}$ be an $s$-distance set such that $F$ vanishes on $\mathcal{A}$. Then*

$$|\mathcal{A}| \leqslant \binom{n+s}{n} - \binom{n+s-d}{n}.$$

For example, when $n = 2$, then $F$ defines a plane curve of degree $d$. Then for $s \geqslant d$ we obtain

$$|\mathcal{A}| \leqslant \binom{2+s}{2} - \binom{2+s-d}{2} = ds - \frac{d(d-3)}{2}.$$

In particular, when $F(x, y) = y^2 - f(x)$ gives a Weierstrass equation of an elliptic curve, then $|\mathcal{A}| \leqslant 3s$ for $s \geqslant 3$.

*Remark* 5. We can now easily derive Theorem 2 for $s > 1$. Indeed, consider the real polynomial

$$F(x_1, \ldots, x_n) = 1 - \sum_{i=1}^{n} x_i^2 \in \mathbb{R}[x_1, \ldots, x_n]$$

of degree 2 which vanishes on $\mathbb{S}^{n-1}$. Corollary 4 and the hockey-stick identity gives

$$|\mathcal{A}| \leqslant \binom{n+s}{n} - \binom{n+s-2}{n} = \binom{n+s-1}{s} + \binom{n+s-2}{s-1}.$$

Next, assume that $V = \cup_{i=1}^{p} \mathcal{S}_i$, where the $\mathcal{S}_i$ are spheres in $\mathbb{R}^n$. E. Bannai, K. Kawasaki, Y. Nitamizu, and T. Sato proved the following result in [5, Theorem 1] for the case when the spheres $\mathcal{S}_i$ are *concentric*. We have a much shorter approach to the same bound, in a more general setting, without the assumption on the centers.

**Corollary 6.** *Let $\mathcal{A}$ be an $s$-distance set on the union $V$ of $p$ spheres in $\mathbb{R}^n$. Then*

$$|\mathcal{A}| \leqslant \sum_{i=0}^{2p-1} \binom{n+s-i-1}{s-i}.$$

Let $T_i \subseteq \mathbb{R}$ be given finite sets, where $|T_i| = q \geqslant 2$ for each $i$ with $1 \leqslant i \leqslant n$. A *box* is a direct product

$$\mathcal{B} := \prod_{i=1}^{n} T_i \subseteq \mathbb{R}^n.$$

We can easily apply Theorem 3 to obtain an upper bound for the size of $s$-distance sets in boxes.

**Corollary 7.** *Let $\mathcal{B} \subseteq \mathbb{R}^n$ be a box as above, and $\mathcal{A} \subseteq \mathcal{B}$ an $s$-distance set. Then*

$$|\mathcal{A}| \leqslant |\{x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} : \ 0 \leqslant \alpha_i \leqslant q-1 \textit{ for each } i, \textit{ and } \sum_i \alpha_i \leqslant s\}|.$$

*Remark* 8. In the special case $q = 2$ we have

$$|\{x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} :\ 0 \leqslant \alpha_i \leqslant 1 \text{ for each } i, \text{ and } \sum_i \alpha_i \leqslant s\}| = \sum_{j=0}^{s} \binom{n}{j},$$

hence we obtain the upper bound

$$|\mathcal{A}| \leqslant \sum_{j=0}^{s} \binom{n}{j}. \tag{1}$$

In the case when $T_i = T$ for $1 \leqslant i \leqslant n$ and $|T| = 2$, the Euclidean distance is essentially the same as the Hamming distance. For this case (1) was proved by Delsarte [10], see also [2, Theorem 1].

*Remark* 9. The bound is sharp, when $q = 2$, $n = 2m$ and $s = m$. Then the 0,1 vectors of even Hamming weight give an extremal family $\mathcal{A} \subseteq \mathbb{R}^n$.

*Remark* 10. The bound of Corollary 7 can be nicely formulated in terms of extended binomial coefficients (see [12, Example 8] or [7, Exercise 16]):

$$|\mathcal{A}| \leqslant \sum_{j=0}^{s} \binom{n}{j}_q.$$

Here $\binom{n}{j}_q$ is an extended binomial coefficient giving the number of restricted compositions of $j$ with $n$ terms (summands), where each term is from the set $\{0, 1, \ldots, q-1\}$. In particular, we have $\binom{n}{j}_2 = \binom{n}{j}$.

*Remark* 11. In [16] a weaker, but similar upper bound was given for the size of $s$-distance sets in boxes:

$$|\mathcal{A}| \leqslant 2|\{x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} :\ 0 \leqslant \alpha_i \leqslant q-1 \text{ for each } i, \text{ and } \sum_i \alpha_i \leqslant s\}|.$$

The bound appearing in Corollary 7 presents an improvement by a factor of 2.

Let $\alpha_1, \ldots, \alpha_n$ be $n$ different elements of $\mathbb{R}$, and $X_n = X_n(\alpha_1, \ldots, \alpha_n) \subseteq \mathbb{R}^n$ be the set of permutations of $\alpha_1, \ldots, \alpha_n$, where each permutation is considered as vector of length $n$. It was proved in [17, Section 2] that for $s \geqslant 0$

$$h_{X_n}(s) = \sum_{i=0}^{s} I_n(i),$$

where $I_n(i)$ is the number of permutations of $n$ symbols with precisely $i$ inversions. Using this, Theorem 3 implies the following bound:

**Corollary 12.** *Let $\mathcal{A} \subseteq X_n$ be an $s$-distance set. Then*

$$|\mathcal{A}| \leqslant \sum_{i=0}^{s} I_n(i).$$

In [19, Section 5.1.1] Knuth gives a generating function for $I_n(i)$ and some explicit formulae for the values $I_n(i)$, $i \leqslant n$.

Let $0 \leqslant d \leqslant n$ be integers and $Y_{n,d} \subseteq \mathbb{R}^n$ denote the set of 0,1-vectors of length $n$ which have exactly $d$ coordinate values of 1. The following (sharp) bound was obtained by Ray-Chaudhuri and Wilson in [21, Theorem 3], formulated in terms of intersections rather than distances.

**Corollary 13.** *Let $0 \leqslant d \leqslant n$ and $s$ be integers, with $0 \leqslant s \leqslant \min(d, n-d)$. Suppose that $\mathcal{A} \subseteq Y_{n,d}$ is an $s$-distance set. Then*

$$|\mathcal{A}| \leqslant \binom{n}{s}.$$

In some cases data about the complexification of a real affine algebraic set can be used to give a bound. We give next a statement of this type. For a subset $X \subseteq \mathbb{F}^n$ of the affine space we write $I(X)$ for the ideal of all polynomials $f \in \mathbb{F}[\mathbf{x}]$ which vanish on $X$.

**Corollary 14.** *Let $V \subseteq \mathbb{C}^n$ be an affine variety such that the projective closure $\overline{V}$ of $V$ has dimension $d$ and degree $k$. Suppose also that the ideal $I(V)$ of $V$ is generated by polynomials over $\mathbb{R}$. Let $\mathcal{A} \subseteq V \cap \mathbb{R}^n$ be an $s$-distance set. Then we have*

$$|\mathcal{A}| \leqslant \frac{k \cdot s^d}{d!} + O(s^{d-1}).$$

For instance, when in Corollary 14 the projective variety $\overline{V}$ is a curve of degree $k$, then the bound is $ks + b$ for large $s$, where $b$ is an integer. More specifically, when $\overline{V}$ is an elliptic curve such that $V \subseteq \mathbb{C}^2$ is the set of zeroes of $y^2 - f(x)$, where $f(x) \in \mathbb{R}[x]$ is a cubic polynomial without multiple roots, then in fact, the preceding bound becomes $|\mathcal{A}| \leqslant 3s + b$ for $s$ large (see also the remark after Corollary 4).

The rest of the paper is organized as follows. Section 2 contains some preliminaries on Gröbner bases, Hilbert functions, and related notions. Section 3 contains the proofs of the main theorem and the proof of the corollaries.

## 2 Preliminaries

A total ordering $\prec$ on the monomials $x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$ composed from variables $x_1, x_2, \ldots, x_n$ is a *term order*, if 1 is the minimal element of $\prec$, and $uw \prec vw$ holds for any monomials $u, v, w$ with $u \prec v$. Two important term orders are the lexicographic order $\prec_l$ and the deglex order $\prec_{dl}$. We have

$$x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \prec_l x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}$$

iff $i_k < j_k$ holds for the smallest index $k$ such that $i_k \neq j_k$. As for the deglex order, we have $u \prec_{dl} v$ iff either $\deg u < \deg v$, or $\deg(u) = \deg(v)$, and $u \prec_l v$.

Let $\prec$ be a fixed term order. The *leading monomial* $\mathrm{lm}(f)$ of a nonzero polynomial $f$ from the ring $S = \mathbb{F}[\mathbf{x}]$ is the largest (with respect to $\prec$) monomial which occurs with nonzero coefficient in the standard form of $f$.

Let $I$ be an ideal of $S$. A finite subset $G \subseteq I$ is a *Gröbner basis* of $I$ if for every $f \in I$ there exists a $g \in G$ such that $\mathrm{lm}(g)$ divides $\mathrm{lm}(f)$. It can be shown that $G$ is in fact a basis of $I$. A fundamental result is (cf. [6, Chapter 1, Corollary 3.12] or [1, Corollary 1.6.5, Theorem 1.9.1]) that every nonzero ideal $I$ of $S$ has a Gröbner basis with respect to $\prec$.

A monomial $w \in S$ is a *standard monomial* for $I$ if it is not a leading monomial of any $f \in I$. Let $\mathrm{Sm}(\prec, I, \mathbb{F})$ denote the set of all standard monomials of $I$ with respect to the term-order $\prec$ over $\mathbb{F}$. It is known (see [6, Chapter 1, Section 4]) that for a nonzero ideal $I$ the set $\mathrm{Sm}(\prec, I, \mathbb{F})$ is a basis of the factor space $S/I$ over $\mathbb{F}$. Hence every $g \in S$ can be written uniquely as $g = h + f$ where $f \in I$ and $h$ is a unique $\mathbb{F}$-linear combination of monomials from $\mathrm{Sm}(\prec, I, \mathbb{F})$.

If $X \subseteq \mathbb{F}^n$ is a finite set, then an interpolation argument gives that every function from $X$ to $\mathbb{F}$ is a polynomial function. The latter two facts imply that

$$|\mathrm{Sm}(\prec, I(X), \mathbb{F})| = |X|, \tag{2}$$

where $I(X)$ is the ideal of all polynomials from $S$ which vanish on $X$, and $\prec$ is an arbitrary term order.

The *initial ideal* $\mathrm{in}(I)$ of $I$ is the ideal in $S$ generated by the set of monomials $\{\mathrm{lm}(f) : f \in I\}$.

It is easy to see [8, Propositions 9.3.3 and 9.3.4] that the value at $s$ of the Hilbert function $h_{S/I}$ is the number of standard monomials of degree at most $s$, where the ordering $\prec$ is deglex:

$$h_{S/I}(s) = |\mathrm{Sm}(\prec_{dl}, I, \mathbb{F}) \cap \mathbb{F}[\mathbf{x}]_{\leqslant s}|. \tag{3}$$

In the case when $I = I(X)$ for some $X \subseteq \mathbb{F}^n$, then $h_X(s) := h_{S/I}(s)$ is the dimension of the space of functions from $X$ to $\mathbb{F}$ which are polynomials of degree at most $s$.

Next we recall a known fact about the Hilbert function. It concerns the change of the coefficient field. Let $\mathbb{F} \subset \mathbb{K}$ be fields and let $I \subseteq \mathbb{F}[\mathbf{x}]$ be an ideal, and consider the corresponding ideal $J = I \cdot \mathbb{K}[\mathbf{x}]$ generated by $I$ in $\mathbb{K}[\mathbf{x}]$.

**Lemma 15.** *For the respective affine Hilbert functions for $s \geqslant 0$ we have*

$$h_{\mathbb{F}[\mathbf{x}]/I}(s) = h_{\mathbb{K}[\mathbf{x}]/J}(s).$$

For the convenience of the reader we outline a simple proof.

*Proof.* It follows from Buchberger's criterion [8, Theorem 2.6.6] that a deglex Gröbner basis of $I$ in $\mathbb{F}[\mathbf{x}]$ will be a deglex Gröbner basis of $J$ in $\mathbb{K}[\mathbf{x}]$, implying that the initial ideals $\mathrm{in}(I)$ and $\mathrm{in}(J)$ contain exactly the same set of monomials, hence their respective factors have the same Hilbert function $h_{\mathbb{F}[\mathbf{x}]/\mathrm{in}(I)}(s) = h_{\mathbb{K}[\mathbf{x}]/\mathrm{in}(J)}(s)$, see [8, Proposition 9.3.3]. Then by [8, Proposition 9.3.4] we have

$$h_{\mathbb{F}[\mathbf{x}]/I}(s) = h_{\mathbb{F}[\mathbf{x}]/\mathrm{in}(I)}(s) = h_{\mathbb{K}[\mathbf{x}]/\mathrm{in}(J)}(s) = h_{\mathbb{K}[\mathbf{x}]/J}(s),$$

for every integer $s \geqslant 0$. □

The projective (homogenized) version of the next statement is discussed in [13, Example 6.10].

**Proposition 16.** *Let $F \in \mathbb{F}[\mathbf{x}]$ be a polynomial of degree $d$. Then for $s \geqslant d$ we have*

$$h_{\mathbb{F}[\mathbf{x}]/(F)}(s) = \binom{n+s}{n} - \binom{n+s-d}{n}.$$

*If $0 \leqslant s < d$, then*

$$h_{\mathbb{F}[\mathbf{x}]/(F)}(s) = \binom{n+s}{n}.$$

*Proof.* By definition

$$\begin{aligned} h_{\mathbb{F}[\mathbf{x}]/(F)}(s) &= \dim \mathbb{F}[\mathbf{x}]_{\leqslant s}/(F)_{\leqslant s} = \\ &= \dim \mathbb{F}[\mathbf{x}]_{\leqslant s} - \dim (F)_{\leqslant s}. \end{aligned}$$

Clearly

$$\dim \mathbb{F}[\mathbf{x}]_{\leqslant s} = \binom{n+s}{n}.$$

Moreover

$$(F)_{\leqslant s} = \{G \in \mathbb{F}[\mathbf{x}]_{\leqslant s} : \text{ there exists an } H \in \mathbb{F}[\mathbf{x}] \text{ such that } FH = G\}.$$

Using the fact that $\mathbb{F}[\mathbf{x}]$ is a domain, we see that the dimension of the latter subspace is

$$\dim\{H \in \mathbb{R}[\mathbf{x}] : \deg(H) \leqslant s-d\} = \dim \mathbb{F}[\mathbf{x}]_{\leqslant (s-d)}.$$

The statement now follows from the fact that if $s \geqslant d$, then

$$\dim \mathbb{F}[\mathbf{x}]_{\leqslant (s-d)} = \binom{n+s-d}{n},$$

while for $s < d$ we have

$$\dim \mathbb{F}[\mathbf{x}]_{\leqslant (s-d)} = 0.$$

□

# 3 Proofs

## 3.1 Proof of the main result

Petrov and Pohoata proved the following result [20, Theorem 1.2]. They used it to give a short proof of Theorem 1. This improved version of the Croot-Lev-Pach Lemma has a crucial role in the proof of our results.

**Theorem 17.** *Let $W$ be an $n$-dimensional vector space over a field $\mathbb{F}$ and let $\mathcal{A} \subseteq W$ be a finite set. Let $s \geqslant 0$ be an integer an let $p(\mathbf{x}, \mathbf{y}) \in \mathbb{F}[\mathbf{x}, \mathbf{y}]$ be a $2n$-variate polynomial of degree at most $2s+1$. Consider the matrix $M(\mathcal{A}, p)_{\mathbf{a},\mathbf{b}\in A}$, where*

$$M(\mathcal{A}, p)(\mathbf{a}, \mathbf{b}) = p(\mathbf{a}, \mathbf{b}).$$

*This matrix corresponds to a bilinear form on $\mathbb{F}^{\mathcal{A}}$ by the formula*

$$\Phi_{\mathcal{A},p}(f, g) = \sum_{\mathbf{a},\mathbf{b}\in\mathcal{A}} p(\mathbf{a}, \mathbf{b})f(\mathbf{a})g(\mathbf{b}),$$

*for each $f, g : \mathcal{A} \to \mathbb{F}$. This $\Phi_{\mathcal{A},p}$ defines a quadratic form $\Phi_{\mathcal{A},p}(f, f)$. In the case $\mathbb{F} = \mathbb{R}$ denote by $r_+(\mathcal{A}, p)$ and $r_-(\mathcal{A}, p)$ the inertia indices of the quadratic form $\Phi_{\mathcal{A},p}(f, f)$. Then*

*(i)* $\operatorname{rank}(M(\mathcal{A}, p)) \leqslant 2h_{\mathcal{A}}(s)$,

*(ii) if $\mathbb{F} = \mathbb{R}$, then* $\max(r_+(\mathcal{A}, p), r_-(\mathcal{A}, p)) \leqslant h_{\mathcal{A}}(s)$.

By combining Theorem 17 with facts about standard monomials, we have the following simple and elegant upper bound for the degree of deglex standard monomials of an $s$-distance set.

**Theorem 18.** *Let $\mathcal{A} \subseteq \mathbb{R}^n$ be an $s$-distance set. Then*

$$Sm(\prec_{dl}, I(\mathcal{A}), \mathbb{F}) \subseteq \mathbb{R}[\mathbf{x}]_{\leqslant s}.$$

*Proof.* We follow the argument of [20, Theorem 1.1]. Let $\mathcal{A} \subseteq \mathbb{R}^n$ denote an $s$-distance set. Recall that $d(\mathcal{A})$ denotes the set of (non-zero) distances among points of $\mathcal{A}$. Define the $2n$–variate polynomial by:

$$p(\mathbf{x}, \mathbf{y}) = \prod_{t\in d(\mathcal{A})} \left(t^2 - \|\mathbf{x} - \mathbf{y}\|^2\right) \in \mathbb{R}[\mathbf{x}, \mathbf{y}].$$

Then we can apply Theorem 17 for $p(\mathbf{x}, \mathbf{y})$ whose degree is $2s$. The matrix $M(\mathcal{A}, p)$ is a positive diagonal matrix, giving that

$$r_+(\mathcal{A}, p) = |\mathcal{A}|.$$

It follows from Theorem 17 (ii) that

$$|\mathcal{A}| = r_+(\mathcal{A}, p) \leqslant h_{\mathcal{A}}(s).$$

But equations (3), (2) and the finiteness of $\mathcal{A}$ imply that

$$|\mathcal{A}| \leqslant h_{\mathcal{A}}(s) = |\mathrm{Sm}(\prec_{dl}, I(\mathcal{A}), \mathbb{R}) \cap \mathbb{R}[\mathbf{x}]_{\leqslant s}| \leqslant |\mathrm{Sm}(\prec_{dl}, I(\mathcal{A}), \mathbb{R})| = |\mathcal{A}|.$$

We infer that

$$|\mathrm{Sm}(\prec_{dl}, I(\mathcal{A}), \mathbb{R}) \cap \mathbb{R}[\mathbf{x}]_{\leqslant s}| = |\mathrm{Sm}(\prec_{dl}, I(\mathcal{A}), \mathbb{R})|,$$

and hence

$$\mathrm{Sm}(\prec_{dl}, I(\mathcal{A}), \mathbb{R}) \subseteq \mathbb{R}[\mathbf{x}]_{\leqslant s}.$$

□

*Proof of Theorem 3.* Theorem 18 gives that

$$\mathrm{Sm}(\prec_{dl}, I(\mathcal{A}), \mathbb{R}) \subseteq \mathbb{R}[\mathbf{x}]_{\leqslant s}.$$

Since $I$ vanishes on $\mathcal{A}$, we have $I \subseteq I(\mathcal{A})$, hence

$$\mathrm{Sm}(\prec_{dl}, I(\mathcal{A}), \mathbb{R}) \subseteq \mathrm{Sm}(\prec_{dl}, I, \mathbb{R}).$$

The preceding two relations imply that

$$\mathrm{Sm}(\prec_{dl}, I(\mathcal{A}), \mathbb{R}) \subseteq \mathrm{Sm}(\prec_{dl}, I, \mathbb{R}) \cap \mathbb{R}[\mathbf{x}]_{\leqslant s}.$$

Now it follows from (3) and (2) that

$$|\mathcal{A}| = |\mathrm{Sm}(\prec_{dl}, I(\mathcal{A}), \mathbb{R})| \leqslant |\mathrm{Sm}(\prec_{dl}, I, \mathbb{R}) \cap \mathbb{R}[\mathbf{x}]_{\leqslant s}| = h_{\mathbb{R}[\mathbf{x}]/I}(s).$$

□

### 3.2 Proofs of the Corollaries

*Proof of Corollary 4.* From Theorem 3 we obtain the bound $|\mathcal{A}| \leqslant h_{\mathbb{R}[\mathbf{x}]/(F)}(s)$, therefore for $s \geqslant d$ we have

$$|\mathcal{A}| \leqslant h_{\mathbb{R}[\mathbf{x}]/(F)}(s) = \binom{n+s}{n} - \binom{n+s-d}{n},$$

by Proposition 16. □

*Proof of Corollary 6.* It is easy to verify that

$$\sum_{i=0}^{2p-1} \binom{n+s-i-1}{s-i} = \binom{n+s}{s} - \binom{n+s-2p}{n}.$$

Let $V = \cup_{i=1}^{p} \mathcal{S}_i$, and assume, that the center of the sphere $\mathcal{S}_i$ is the point $(a_{1,i}, \ldots, a_{n,i}) \in \mathbb{R}^n$, and the radius of $\mathcal{S}_i$ is $r_i \in \mathbb{R}$ for $i = 1, \ldots, p$. Next consider the polynomials

$$F_i(x_1, \ldots, x_n) = (\sum_{m=1}^{n} (x_m - a_{m,i})^2) - r_i^2 \in \mathbb{R}[x_1, \ldots, x_n]$$

for each $i$ and put $F := \prod_i F_i$. Then $\deg(F) = 2p$ and $F$ vanishes on $V$. We may apply Corollary 4 for the polynomial $F$. Then for $s \geqslant 2p$ we obtain the desired bound

$$|\mathcal{A}| \leqslant \binom{n+s}{n} - \binom{n+s-2p}{n}.$$

When $s < 2p$, the bound follows from the Bannai-Bannai-Stanton theorem. □

*Proof of Corollary 7.* It is well-known and easily proved that the following set of polynomials is a (reduced) Gröbner basis of the ideal $I(\mathcal{B})$ (with respect to any term order):

$$\left\{\prod_{t\in T_i}(x_i-t):\ 1\leqslant i\leqslant n\right\}.$$

This readily gives the (deglex) standard monomials for $I(\mathcal{B})$:

$$\mathrm{Sm}(\prec_{dl}, I(\mathcal{B}), \mathbb{R}) = \{x_1^{\alpha_1}\cdot\ldots\cdot x_n^{\alpha_n}:\ 0\leqslant\alpha_i\leqslant q-1 \text{ for each } i\}.$$

It follows from Theorem 3 and equation (3) that

$$|\mathcal{A}|\leqslant h_{\mathcal{B}}(s) = |\mathrm{Sm}(\prec_{dl}, I(\mathcal{B}), \mathbb{R})\cap\mathbb{R}[\mathbf{x}]_{\leqslant s}| =$$

$$= |\{x_1^{\alpha_1}\cdot\ldots\cdot x_n^{\alpha_n}:\ 0\leqslant\alpha_i\leqslant q-1 \text{ for each } i,\quad\text{and } \sum_i\alpha_i\leqslant s\}|.$$ □

*Proof of Corollary 13.* The statement follows at once from the result

$$h_{Y_{n,d}}(s) = \binom{n}{s} \tag{4}$$

proved by Wilson in [22] (formulated there in the language of inclusion matrices, see also [18, Corollary 3.1]), and Theorem 3. □

*Proof of Corollary 14.* Write $I = I(V)\cap\mathbb{R}[\mathbf{x}]$ and $J = I(V)\subseteq\mathbb{C}[\mathbf{x}]$. It follows from Theorem 3 and Proposition 15 that

$$|\mathcal{A}|\leqslant h_{\mathbb{R}[\mathbf{x}]/I}(s) = h_{\mathbb{C}[\mathbf{x}]/J}(s).$$

From [8, Theorem 9.3.12] we obtain that the affine Hilbert function $h_{\mathbb{C}[\mathbf{x}]/J}(s)$ is the same as the projective Hilbert function $h_{\overline{V}}(s)$ of the projective variety $\overline{V}$. Now [15, Proposition 13.2] and the subsequent remark imply that for $s$ large the Hilbert function will be the same as the Hilbert polynomial: $h_{\overline{V}}(s) = p_{\overline{V}}(s)$, moreover

$$p_{\overline{V}}(s) = \frac{k}{d!}\cdot s^d + \text{ terms of degree at most } d-1 \text{ in } s.$$

This proves the statement. □

## References


[1] W. W. Adams, and P. Loustaunau. *An Introduction to Gröbner bases.* AMS, Providence, 1994.

[2] L. Babai, H. Snevily, and R. M. Wilson. A new proof of several inequalities on codes and sets. *Journal of Combinatorial Theory, Series A*, **71(1)**, 146-153 (1995).

[3] E. Bannai, and E. Bannai. A survey on spherical designs and algebraic combinatorics on spheres. *European Journal of Combinatorics*, **30**, 1392-1425 (2009).

[4] E. Bannai, E. Bannai, and D. Stanton. An upper bound for the cardinality of an $s$-distance subset in real Euclidean space II. *Combinatorica*, **3(2)**, 147-152 (1983).

[5] E. Bannai, K. Kawasaki, Y. Nitamizu, and T. Sato. An upper bound for the cardinality of an $s$-distance set in Euclidean space. *Combinatorica*, **23(4)**, 535-557 (2003).

[6] A. M. Cohen, H. Cuypers, and H. Sterk (eds.). *Some tapas of computer algebra.* Springer-Verlag, Berlin, Heidelberg, 1999.

[7] L. Comtet. *Advanced Combinatorics.* D. Reidel Publishing Company, Dordrect, 1974.

[8] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms.* Springer-Verlag, Berlin, Heidelberg, 1992.

[9] E. Croot, V. Lev, and P. Pach. Progression-free sets in $\mathbb{Z}_4^n$. *Annals of Mathematics*, **185**, 331-337 (2017).

[10] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Research Reports Supplements*, **10**, 1-97 (1973).

[11] P. Delsarte, J. M. Goethals, and J. J. Seidel. Spherical codes and designs. *Geometriae Dedicata*, **6(3)**, 363-388 (1977).

[12] S. Egger. Restricted weighted integer compositions and extended binomial coefficients. *Journal of Integer Sequences*, **16**, Article 13.1.3 (2013).

[13] D. Eisenbud, and J. Harris. *3264 and all that: A second course in algebraic geometry.* Cambridge University Press, Cambridge, 2016.

[14] A. Glazyrin, and W. H. Yu. Upper bounds for $s$-distance sets and equiangular lines. *Advances in Mathematics*, **330**, 810-833 (2018).

[15] J. Harris. *Algebraic geometry: a first course.* Springer Science and Business Media, New York, 2013.

[16] G. Hegedüs. A new upper bound for the size of $s$-distance sets in boxes. *Acta Mathematica Hungarica*, **160**, 168–174 (2020).

[17] G. Hegedüs, A. Nagy and L. Rónyai. Gröbner bases for permutations and oriented trees. *Annales Univ. Sci. Budapest., Sectio Computatorica*, **23**, 137-148 (2004).

[18] G. Hegedüs, and L. Rónyai. Gröbner bases for complete uniform families. *Journal of Algebraic Combinatorics*, **17(2)**, 171-180 (2003).

[19] D. E. Knuth. *The art of computer programming, Volume 3, Sorting and searching.* Second. ed., Addison-Wesley, Upper Saddle River, 1998.

[20] F. Petrov, and C. Pohoata. A remark on sets with few distances in $\mathbb{R}^d$. *Proceedings of the American Mathematical Society*, **149(2)**, 569-571 (2021).

[21] D. K. Ray-Chaudhuri, and R. M. Wilson. On $t$-designs. *Osaka Journal of Mathematics*, **12**, 737-744 (1975).

[22] R. M. Wilson. A diagonal form for the incidence matrices of $t$-subsets vs. $k$-subsets. *European Journal of Combinatorics*, **11**, 609–615 (1990).