ALGEBRAIC COMBINATORICS

Hiroshi Nozaki

Bounds for sets with few distances distinct modulo a prime ideal

Volume 6, issue 2 (2023), p. 539-545.
https://doi.org/10.5802/alco.272

Algebraic Combinatorics is published by The Combinatorics Consortium and is a member of the Centre Mersenne for Open Scientific Publishing
www.tccpublishing.org www.centre-mersenne.org
e-ISSN: 2589-5486

Algebraic Combinatorics
Volume 6, issue 2 (2023), p. 539–545
`https://doi.org/10.5802/alco.272`

Bounds for sets with few distances distinct modulo a prime ideal

Hiroshi Nozaki

Abstract Let $\mathcal{O}_K$ be the ring of integers of an algebraic number field K embedded into $\mathbb{C}$. Let X be a subset of the Euclidean space $\mathbb{R}^d$, and $D(X)$ be the set of the squared distances of two distinct points in X. In this paper, we prove that if $D(X) \subset \mathcal{O}_K$ and there exist s values $a_1, \ldots, a_s \in \mathcal{O}_K$ distinct modulo a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ such that each a_i is not zero modulo $\mathfrak{p}$ and each element of $D(X)$ is congruent to some a_i, then $|X| \leqslant \binom{d+s}{s} + \binom{d+s-1}{s-1}$.

1. Introduction

This paper is devoted to giving an upper bound on the cardinalities of certain finite sets X in a metric space M, that have some special properties of the values of distances appearing in X. A finite set X in M is called an *s-distance set* if the number of distances of two distinct points in X is equal to s. One of the major problems for s-distance sets is to determine the largest possible s-distance sets for given s, that is motivated from the extremal set theory. For this purpose, we need to give (or improve) upper bounds on the size and construct large sets. For small s, there are remarkable successful cases that can determine the largest sets, for example, 2-distance sets on a Euclidean sphere [9], sets of equiangular lines in Euclidean spaces [14], and several s-distance sets in the real, complex, or quaternionic projective spaces [17] or in polynomial association schemes [5, 6, 7].

In the literature of combinatorial geometry, upper bounds for s-distance sets for L-intersecting families have been obtained. An *L-intersecting family* $\mathfrak{F}$ is a family of subsets of a finite set F that satisfies $|A \cap B| \in L$ for any distinct $A, B \in \mathfrak{F}$ for some $L \subset \{0, 1, \ldots, n-1\}$, where $|F| = n$. An L-intersecting family $\mathfrak{F}$ is said to be *k-uniform* if $|A| = k$ for each $A \in \mathfrak{F}$ for some constant k. For k-uniform L-intersecting families $\mathfrak{F}$, Ray-Chaudhuri and Wilson [21] proved an upper bound $|\mathfrak{F}| \leqslant \binom{n}{s}$, where $|L| = s$. This case corresponds to s-distance sets in Johnson association schemes. After this work, Frankl and Wilson [8] obtained $|\mathfrak{F}| \leqslant \sum_{i=0}^{s} \binom{n}{i}$ without the assumption of k-uniform.

Frankl and Wilson [8] also proved a *modular version* of the upper bound for k-uniform L-intersecting families. Namely they interpreted the sizes of the intersections as elements of $\mathbb{Z}/p\mathbb{Z}$ for some prime number p. Suppose the set L has only s elements distinct modulo p, and note that $|L|$ may be greater than s. For k-uniform L-intersecting families $\mathfrak{F}$, if $k \not\equiv a \pmod{p}$ for each $a \in L$, then Frankl–Wilson [8] showed that $|\mathfrak{F}| \leqslant \binom{n}{s}$. Note that this is the same upper bound as that obtained

Manuscript received 24th March 2022, revised 7th October 2022, accepted 10th October 2022.

Keywords. s-distance set, algebraic number field.

under the assumption $|L| = s$. For L-intersecting families $\mathfrak{F}$ with r different sizes of elements of $\mathfrak{F}$ modulo p, Alon, Babai, and Suzuki [1] proved that $|\mathfrak{F}| \leqslant \sum_{i=0}^{r-1} \binom{n}{s-i}$ under a certain weak assumption which is simplified by [13]. The upper bound in [1] is proved by Koornwinder's method [15], which gives upper bounds on the size $|X|$ by proving the linear independence of some polynomial functions that have a bijective correspondence to X.

We have upper bounds for Euclidean s-distance sets with several conditions, which are counterparts of that of L-intersecting families. Let X be an s-distance set in the Euclidean space $\mathbb{R}^d$. For X in the unit sphere S^{d-1}, which corresponds to the condition of k-uniform, Delsarte, Goethals, and Seidel [6] proved that $|X| \leqslant \binom{d+s-1}{s} + \binom{d+s-2}{s-1}$. With no assumption, Bannai, Bannai, and Stanton [2] proved that $|X| \leqslant \binom{d+s}{s}$. For X in r concentric spheres, which corresponds to the condition of r different sizes, Bannai, Kawasaki, Nitamizu, and Sato [3] obtained that $|X| \leqslant \sum_{i=0}^{2r-1} \binom{d+s-1-i}{s-i}$. Recently simple alternative proofs of these upper bounds are given in [12, 20].

Blokhuis [4] gave a modular version of upper bounds for Euclidean sets, assuming that the squared distances are rational integers. Let $D(X)$ be the set of the squared Euclidean distances between two distinct points of X.

Theorem 1.1 (mod-p bound [4]). *Let X be a subset of $\mathbb{R}^d$, and p a prime number. Suppose $D(X)$ is a subset of rational integers $\mathbb{Z}$. If there exist $a_1, \ldots, a_s \in \mathbb{Z}$ distinct modulo p such that*

(1) *for each $i \in \{1, \ldots, s\}$, $a_i \not\equiv 0 \pmod p$ and*

(2) *for each $\alpha \in D(X)$, there exists $i \in \{1, \ldots, s\}$ such that $\alpha \equiv a_i \pmod p$,*

then

$$|X| \leqslant \binom{d+s}{s} + \binom{d+s-1}{s-1}.$$

For sets in a sphere, several projective spaces, or Q-polynomial association schemes, Theorem 1.1 can be analogously obtained. However, the r-concentric spherical version is still open. The assumption $D(X) \subset \mathbb{Z}$ in Theorem 1.1 is surely strong, and the sets to which the theorem can be applied are restricted.

In this paper, we extend Theorem 1.1 to the ring of integers $\mathcal{O}_K$ of an algebraic number field K, and any prime ideal $\mathfrak{p}$ of it. Note that throughout this paper, we fix an embedding of K into $\mathbb{C}$, and K is interpreted as a subfield of $\mathbb{C}$. We use Koornwinder's method to prove this mod-$\mathfrak{p}$ upper bound. However the method to prove the linear independence of polynomial functions is new. In the proof, the localization $A_\mathfrak{p}$ of $A = \mathcal{O}_K$ by a prime ideal $\mathfrak{p}$ plays a key role and Nakayama's lemma is applied for a certain finitely generated $A_\mathfrak{p}$-module. This method is purely algebraic and uniformly applicable to the polynomial spaces [10], [11, Sections 14–16], which includes the Euclidean sphere, the real, complex or quaternionic projective spaces (see [7, 17] for the theory of s-distance set in these projective spaces), or Q-polynomial association schemes (which include the theory of L-intersecting family as codes of Johnson or Hamming schemes) [5].

The paper is organized as follows. In Section 2, we introduce basic terminology and results about algebraic number fields. In Section 3, we prove a generalization of Theorem 1.1 (mod-$\mathfrak{p}$ bound) for the ring of integers $\mathcal{O}_K$ of an algebraic number field K and a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$. We also comment on the version of the theorem for an ideal that may not be prime. In Section 4, we extend the LRS type theorem proved in [16, 19]. Namely, if the cardinality of an s-distance set is relatively large, then a certain ratio of squared distances must be an algebraic integer (see Theorem 4.1). We explain the relationship between the LRS type theorem and mod-$\mathfrak{p}$ bound, which can refine an upper bound on the size of an s-distance set with given distances.

2. Preliminaries

An extension field K of rationals $\mathbb{Q}$ is an *algebraic number field* if the degree $[K:\mathbb{Q}]$ is finite. An algebraic number field K can be embedded into $\mathbb{C}$, and K is always identified with a fixed specific subfield of $\mathbb{C}$. The *ring of integers* $\mathcal{O}_K$ is the ring consisting of all algebraic integers in K, where an *algebraic integer* is a complex number which is a root of a monic polynomial with integer coefficients. It is well known that K is the quotient field of $\mathcal{O}_K$, a prime ideal of $\mathcal{O}_K$ is maximal, $\mathcal{O}_K$ is a finitely generated free $\mathbb{Z}$-module, and $\mathcal{O}_K$ may not be a principal ideal domain. For easy examples, if $K=\mathbb{Q}$, then $\mathcal{O}_K=\mathbb{Z}$. If $K=\mathbb{Q}(\sqrt{d})$ for a square-free integer d, then

$$\mathcal{O}_K=\begin{cases}\mathbb{Z}+\frac{1+\sqrt{d}}{2}\mathbb{Z} & \text{if } d\equiv 1 \pmod 4,\\ \mathbb{Z}+\sqrt{d}\mathbb{Z} & \text{if } d\equiv 2,3 \pmod 4).\end{cases}$$

Suppose a ring is commutative and contains the identity. For a ring A, $(A,\mathfrak{m})$ is a *local ring* if A has a unique maximal ideal $\mathfrak{m}$. It is well known that for a ring A and its maximal ideal $\mathfrak{p}\subset A$, we can construct a local ring $(A_\mathfrak{p},\mathfrak{p}A_\mathfrak{p})$. For $A=\mathcal{O}_K$, the local ring is

$$A_\mathfrak{p}=S^{-1}A=\{a/s\in K \mid a\in A, s\in S\},$$

where $S=A\setminus\mathfrak{p}$. Its unique maximal ideal is $\mathfrak{p}A_\mathfrak{p}$, which is the ideal of $A_\mathfrak{p}$ generated by the elements of $\mathfrak{p}$. Note that $A_\mathfrak{p}$ is a principal ideal domain. The natural map $f: A/\mathfrak{p}\to A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ is a field isomorphism.

The following theorem is called Nakayama's lemma, which plays a key role in a proof of the main theorem. For a local ring $(A,\mathfrak{m})$, the ideal I in Theorem 2.1 is $\mathfrak{m}$.

Theorem 2.1. *Let A be a ring. Let I be an ideal that is contained in all maximal ideals of A. Let M be a finitely generated A-module. If $IM=M$, then $M=\{0\}$.*

In order to prove the main theorem, we use the polynomial

$$f_{\boldsymbol{x}}(\boldsymbol{\xi})=\prod_{i=1}^{s}(||\boldsymbol{x}-\boldsymbol{\xi}||^2-a_i),$$

for $\boldsymbol{x}\in\mathbb{R}^d$, $a_i\in\mathbb{R}$, and variables $\boldsymbol{\xi}=(\xi_1,\ldots,\xi_d)$, where $||\boldsymbol{x}||$ is the Euclidean norm of $\boldsymbol{x}$. By proving the linear independence of $\{f_{\boldsymbol{x}}\}_{\boldsymbol{x}\in X}$ as polynomial functions, the cardinality $|X|$ can be bounded above by the dimension of a certain linear space that contains $f_{\boldsymbol{x}}$. We use the same polynomial space used in Bannai–Bannai–Stanton [2]. For $\xi_0=\xi_1^2+\cdots+\xi_d^2$, we define the polynomial space $P_s(\mathbb{R}^d)$ that consists of all real polynomial functions on $\mathbb{R}^d$ which are spanned by $\xi_0^{\lambda_0}\xi_1^{\lambda_1}\cdots\xi_d^{\lambda_d}$ with $\sum_{i=0}^d\lambda_i\leqslant s$. The dimension of $P_s(\mathbb{R}^d)$ is equal to $\binom{d+s}{s}+\binom{d+s-1}{s-1}$.

3. Bounds for s-distance sets modulo $\mathfrak{p}$

The following is the main theorem in this paper.

Theorem 3.1 (mod-$\mathfrak{p}$ bound). *Let X be a subset of $\mathbb{R}^d$, and $A=\mathcal{O}_K$ the ring of integers of an algebraic number field K. Let $\mathfrak{p}$ be a prime ideal of A. Suppose $D(X)\subset A_\mathfrak{p}$. If there exist $a_1,\ldots,a_s\in A_\mathfrak{p}$ distinct modulo $\mathfrak{p}A_\mathfrak{p}$ such that*

(1) *for each $i\in\{1,\ldots,s\}$, $a_i\not\equiv 0 \pmod{\mathfrak{p}A_\mathfrak{p}}$ and*
(2) *for each $\alpha\in D(X)$, there exists $i\in\{1,\ldots,s\}$ such that $\alpha\equiv a_i \pmod{\mathfrak{p}A_\mathfrak{p}}$,*

then

$$|X|\leqslant\binom{d+s}{s}+\binom{d+s-1}{s-1}.$$

Proof. For each $\boldsymbol{x} \in X$, we define the polynomial $f_{\boldsymbol{x}}(\boldsymbol{\xi}) \in P_s(\mathbb{R}^d)$ as

$$f_{\boldsymbol{x}}(\boldsymbol{\xi}) = \prod_{i=1}^{s}(||\boldsymbol{x} - \boldsymbol{\xi}||^2 - a_i),$$

where if needed, we replace a_i with a real value equivalent to a_i modulo $\mathfrak{p}A_{\mathfrak{p}}$. These polynomials satisfy

$$f_{\boldsymbol{x}}(\boldsymbol{x}) = (-1)^s \prod_{i=1}^{s} a_i \not\equiv 0 \pmod{\mathfrak{p}A_{\mathfrak{p}}}, \tag{3.1}$$

and

$$f_{\boldsymbol{x}}(\boldsymbol{y}) \equiv 0 \pmod{\mathfrak{p}A_{\mathfrak{p}}} \tag{3.2}$$

for $\boldsymbol{x} \neq \boldsymbol{y} \in X$.

We prove $\{f_{\boldsymbol{x}}\}_{\boldsymbol{x}\in X}$ is linearly independent as polynomial functions on $\mathbb{R}^d$. Assume there exist $m_{\boldsymbol{x}} \in \mathbb{R}$ such that

$$\sum_{\boldsymbol{x}\in X} m_{\boldsymbol{x}} f_{\boldsymbol{x}}(\boldsymbol{\xi}) = 0. \tag{3.3}$$

Let M be an $A_{\mathfrak{p}}$-module generated by a finite set $\{m_{\boldsymbol{x}}\}_{\boldsymbol{x}\in X}$, namely

$$M = \sum_{\boldsymbol{x}\in X} m_{\boldsymbol{x}} A_{\mathfrak{p}}.$$

From equalities (3.3) and (3.2), for each $\boldsymbol{y} \in X$,

$$m_{\boldsymbol{y}} f_{\boldsymbol{y}}(\boldsymbol{y}) = -\sum_{\boldsymbol{y}\neq\boldsymbol{x}\in X} m_{\boldsymbol{x}} f_{\boldsymbol{x}}(\boldsymbol{y}) \in \mathfrak{p}A_{\mathfrak{p}}M.$$

Since $f_{\boldsymbol{y}}(\boldsymbol{y}) \in A_{\mathfrak{p}} \setminus \mathfrak{p}A_{\mathfrak{p}}$ from equality (3.1), it follows that $f_{\boldsymbol{y}}(\boldsymbol{y}) \in A_{\mathfrak{p}}^{\times}$ and

$$m_{\boldsymbol{y}} = -\sum_{\boldsymbol{y}\neq\boldsymbol{x}\in X} m_{\boldsymbol{x}} f_{\boldsymbol{x}}(\boldsymbol{y})(f_{\boldsymbol{y}}(\boldsymbol{y}))^{-1} \in \mathfrak{p}A_{\mathfrak{p}}M.$$

This implies that $M \subset \mathfrak{p}A_{\mathfrak{p}}M$, and hence $M = \mathfrak{p}A_{\mathfrak{p}}M$. By Nakayama's lemma, $M = \{0\}$ and $m_{\boldsymbol{x}} = 0$ for each $\boldsymbol{x} \in X$. Therefore $\{f_{\boldsymbol{x}}\}_{\boldsymbol{x}\in X}$ is linearly independent, and

$$|X| = |\{f_{\boldsymbol{x}}\}_{\boldsymbol{x}\in X}| \leqslant \dim P_s(\mathbb{R}^d) = \binom{d+s}{s} + \binom{d+s-1}{s-1}$$

as desired. □

Corollary 3.2. *Let X be a subset of $\mathbb{R}^d$, and $\mathcal{O}_K$ the ring of integers of an algebraic number field K. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Suppose $D(X) \subset \mathcal{O}_K$. If there exist $a_1, \ldots, a_s \in \mathcal{O}_K$ distinct modulo $\mathfrak{p}$ such that*

(1) *for each $i \in \{1, \ldots, s\}$, $a_i \not\equiv 0 \pmod{\mathfrak{p}}$ and*
(2) *for each $\alpha \in D(X)$, there exists $i \in \{1, \ldots, s\}$ such that $\alpha \equiv a_i \pmod{\mathfrak{p}}$,*

then

$$|X| \leqslant \binom{d+s}{s} + \binom{d+s-1}{s-1}.$$

Proof. Since $A = \mathcal{O}_K \subset A_{\mathfrak{p}}$ and $A/\mathfrak{p} \cong A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$, this corollary is immediate from Theorem 3.1. □

Example 3.3. For $X = \{(0,0), (1,0), (-\sqrt{3}/2, 1/2), (-\sqrt{3}/2, -1/2)\} \subset \mathbb{R}^2$, the squared distances are $D(X) = \{1, 2+\sqrt{3}\}$. We take the algebraic number field $K = \mathbb{Q}(\sqrt{3})$. Then the ring of integers is $\mathcal{O}_K = \mathbb{Z} + \sqrt{3}\mathbb{Z}$, and $\mathfrak{p} = (1+\sqrt{3})$ is a prime ideal of $\mathcal{O}_K$. Since $1 \equiv 2+\sqrt{3} \pmod{\mathfrak{p}}$ holds, we have $|X| \leqslant \binom{d+1}{1} + \binom{d}{0} = 4$. The set X is an example attaining the upper bound in Corollary 3.2.

We can prove a similar theorem to Theorem 3.1 for an ideal $I \subset \mathcal{O}_K$ which may not be prime as follows.

Theorem 3.4. *Let X be a subset of $\mathbb{R}^d$, and $A = \mathcal{O}_K$ the ring of integers of an algebraic number field K. Let I be an ideal of A, and $I = \mathfrak{p}_1^{\lambda_1} \cdots \mathfrak{p}_r^{\lambda_r}$ the prime decomposition of I. Let $A_I = S^{-1}A = \{a/s \mid a \in A, s \in S\}$, where $S = \bigcup_{R \in (A/I)^\times} R$. Suppose $D(X) \subset A_I$. If there exist $a_1, \ldots, a_s \in A_I$ distinct modulo IA_I such that*

(1) *for each $i \in \{1, \ldots, s\}$, $a_i \in A_I^\times$ and*

(2) *for each $\alpha \in D(X)$, there exists $i \in \{1, \ldots, s\}$ such that $\alpha \equiv a_i \pmod{IA_I}$,*

then

$$|X| \leqslant \binom{d+s}{s} + \binom{d+s-1}{s-1}.$$

Proof. The proof is similar to that of Theorem 3.1, but we use $\mathfrak{p}_1 \cdots \mathfrak{p}_r A_I$ instead of $\mathfrak{p}A_\mathfrak{p}$ as the ideal that is contained in all maximal ideals in Nakayama's lemma. $\square$

For Theorem 3.4, we must choose squared distances a_i from $A_I^\times$. Such distances a_i can be expressed by $a_i = s_1/s_2$ for some $s_1, s_2 \in S = \bigcup_{R \in (A/I)^\times} R$. Since $S \subset \bigcup_{R \in (A/\mathfrak{p}_j)^\times} R$ for any j, the squared distances a_i are also elements of $A_{\mathfrak{p}_j}^\times = A \setminus \mathfrak{p}_j$. The natural homomorphisms

$$\begin{aligned} A_I/IA_I &\to A_I/\mathfrak{p}_1^{\lambda_1}A_I \times \cdots \times A_I/\mathfrak{p}_r^{\lambda_r}A_I \\ &\to A_I/\mathfrak{p}_1 A_I \times \cdots \times A_I/\mathfrak{p}_r A_I \\ &\to A_{\mathfrak{p}_1}/\mathfrak{p}_1 A_{\mathfrak{p}_1} \times \cdots \times A_{\mathfrak{p}_r}/\mathfrak{p}_r A_{\mathfrak{p}_r} \end{aligned}$$

imply that the number of squared distances distinct modulo IA_I is greater than or equal to that modulo $\mathfrak{p}_i A_{\mathfrak{p}_i}$ for any $i \in \{1, \ldots, r\}$. Therefore, Theorem 3.1 corresponding to the prime-ideal version gives the strongest upper bound for any ideal under our condition.

4. LRS type theorem

We now generalize the LRS type theorem proved in [19] as follows. The absolute bound $|X| \leqslant \binom{d+s}{s}$ is improved by this generalization.

Theorem 4.1. *Suppose $s \geqslant 2$. Let X be an s-distance set in $\mathbb{R}^d$ and $N = \dim P_{s-1}(\mathbb{R}^d) = \binom{d+s-1}{s-1} + \binom{d+s-2}{s-2}$. If $|X| \geqslant N + (N+1)/t$ for some $t \in \mathbb{N}$, then*

$$K_j = \prod_{i=1, i \neq j}^{s} \frac{\alpha_i}{\alpha_i - \alpha_j}$$

is an algebraic integer of degree at most t for each $j \in \{1, \ldots, s\}$.

Proof. Fix $j \in \{1, \ldots, s\}$. Define the polynomial

$$f(\boldsymbol{x}, \boldsymbol{\xi}) = \prod_{i=1, i \neq j}^{s} \frac{\alpha_i - ||\boldsymbol{x} - \boldsymbol{\xi}||^2}{\alpha_i - \alpha_j}$$

for each $\boldsymbol{x} \in X$. Since $f(\boldsymbol{x}, \boldsymbol{\xi}) \in P_{s-1}(\mathbb{R}^d)$, the rank of the matrix $M = (f(\boldsymbol{x}, \boldsymbol{y}))_{\boldsymbol{x}, \boldsymbol{y} \in X}$ is at most N [19]. The matrix can be expressed by

$$M = K_j I + A_j,$$

where I is the identity matrix and A_j is a $(0,1)$-matrix with off diagonals. Since the size of M is at least $N + (N+1)/t > N$, the matrix has 0 eigenvalue whose multiplicity is at least $(N+1)/t$. This implies $-K_j$ is the eigenvalue of A_j, and hence K_j is an algebraic integer.

Assume K_j is an algebraic integer of degree larger than t. Then the number of the conjugates of $-K_j$ is at least t, and the conjugates are also eigenvalues of A_j. Since A_j has the eigenvalue $-K_j$ with multiplicity at least $(N+1)/t$, the size of A_j is at least $(t+1)(N+1)/t = N+1+(N+1)/t$, which contradicts our assumption. Therefore K_j is an algebraic integer of degree at most t. □

For $t=1$, the values K_j are integers under the condition in Theorem 4.1, which is the previous result proved in [19]. The following corollaries are immediate from Theorem 4.1.

Corollary 4.2. *If K_j is not an algebraic integer for some $j \in \{1, \ldots, s\}$, then $|X| \leqslant N$.*

Corollary 4.3. *Suppose K_j is an algebraic integer for each $j \in \{1, \ldots, s\}$. Let t be the maximum value of the degrees of K_j. If $t > 1$ holds, then $|X| < N+(N+1)/(t-1)$.*

Corollary 4.3 is an improvement of the absolute bound for s-distance sets with the LRS ratios.

If there exist $\alpha_i, \alpha_j \in D(X) \subset \mathcal{O}_K$ such that α_i is congruent to α_j modulo some prime ideal $\mathfrak{p}$ and $\alpha \not\equiv 0 \pmod{\mathfrak{p}}$ for each $\alpha \in D(X)$, then the LRS ratio K_j is not an algebraic integer. Indeed, if $K_j \in \mathcal{O}_K$, then

$$0 \equiv K_j \prod_{i \neq j} (\alpha_i - \alpha_j) = \prod_{i \neq j} \alpha_i \not\equiv 0 \pmod{\mathfrak{p}}, \tag{4.1}$$

which is a contradiction. When K_j is not an algebraic integer for some j, we obtain the bound $|X| \leqslant N$ by Theorem 4.1, and we may obtain a better bound depending on the number of the elements of $D(X)$ distinct modulo $\mathfrak{p}$.

The results proved in this paper – mod-$\mathfrak{p}$ bound and LRS type theorem– are analogously obtained for the sphere S^{d-1} [6], several projective spaces [7, 17], or Q-polynomial association schemes [5, 7]. For spherical case, the LRS type theorem with $\mathcal{O}_K = \mathbb{Z}$ is useful to determine largest spherical s-distance sets for $s = 2, 3$. In [9, 18], several largest s-distance sets are determined by a computer assistance. The possibilities of choices of integers K_i are finite, and we can take the finite choices of distances from K_i. Reducing the number of the possible distances is helpful to cut the computational cost by a computer. However, Equation (4.1) implies that it is impossible to reduce the choices of distances by our results.

Remark 4.4. Akihiro Munemasa, one of the editors of the journal, communicated to the author the following idea to prove Theorem 3.1 without the use of Nakayama's lemma. Let $f_{\boldsymbol{x}}(\boldsymbol{\xi})$ be the same as in the proof of Theorem 3.1. We consider the matrix $M = (f_{\boldsymbol{x}}(\boldsymbol{y}))_{\boldsymbol{x},\boldsymbol{y} \in X}$, where X satisfies the condition of the theorem. In order to prove the linear independence of $\{f_{\boldsymbol{x}}\}_{\boldsymbol{x} \in X}$, it suffices to show that the determinant of M is non-zero. The entries of M are elements of $A_{\mathfrak{p}}$, and M is congruent to some diagonal matrix modulo $\mathfrak{p}A_{\mathfrak{p}}$ whose diagonal entries are units in $A_{\mathfrak{p}}$. The determinant M is not congruent to 0 modulo $\mathfrak{p}A_{\mathfrak{p}}$, in particular, it is non-zero.

Acknowledgements. The author thanks Akihiro Munemasa for providing the idea of an alternative proof of Theorem 3.1 as editor's comments. The author is supported by JSPS KAKENHI Grant Numbers 18K03396, 19K03445, 20K03527, and 22K03402.

References

[1] N. Alon, L. Babai, and H. Suzuki, *Multilinear polynomials and Frankl–Ray-Chaudhuri–Wilson type intersection theorems*, J. Combin. Theory, Ser. A **58** (1991), 165–180.

[2] 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** (1983), 147–152.

[3] 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** (2003), 535–557.
[4] A. Blokhuis, *Few-distance sets*, CWI Tract 7, CWI, Amsterdam (1984).
[5] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. No. 10 (1973).
[6] P. Delsarte, J.M. Goethals, and J.J. Seidel, *Spherical codes and designs*, Geom. Dedicata **6** (1977), 363–388.
[7] P. Delsarte and V. I. Levenshtein, *Association schemes and coding theory*, IEEE Trans. Inform. Theory **44** (1998), 2477–2504.
[8] P. Frankl and R.M. Wilson, *Intersection theorems with geometric consequences*, Combinatorica **1** (1981), 357–368.
[9] A. Glazyrin and W.-H. Yu, *Upper bounds for s-distance sets and equiangular lines*, Adv. Math. **330** (2018), 810–833.
[10] C.D. Godsil, *Polynomial spaces*, Discrete Math. **73** (1989), 71–88.
[11] ———, *Algebraic combinatorics*, Chapman and Hall Mathematics Series, Chapman & Hall, New York, 1993.
[12] G. Hegedüs and L. Rónyai, *An upper bound for the size of s-distance sets in real algebraic sets*, Electron. J. Combin. **28** (2021), #P3.27.
[13] K-W. Hwang and Y. Kim, *A proof of Alon–Babai–Suzuki's conjecture and multilinear polynomials*, European J. Combin. **43** (2015), 289–294.
[14] Z. Jiang, J. Tidor, Y. Yao, S. Zhang, and Y. Zhao, *Equiangular lines with a fixed angle*, Ann. of Math. **194** (2021), 729–743.
[15] T.H. Koornwinder, *A note on the absolute bound for systems of lines*, Proc. Ken. Nederl. Akad. Wetensch. Ser. A **79** (1977), 152–153.
[16] D.G. Larman, C.A. Rogers, and J.J. Seidel, *On two-distance sets in Euclidean space*, Bull. Lond. Math. Soc. **9** (1977), 261–267.
[17] V.I. Levenshtein, *Designs as maximum codes in polynomial metric spaces*, Acta Appl. Math. **29** (1992), 1–82.
[18] O.R. Musin and H. Nozaki, *Bounds on three- and higher-distance sets*, European J. Combin. **32** (2011), 1182–1190.
[19] H. Nozaki, *A generalization of Larman–Rogers–Seidel's theorem*, Discrete Math. **311** (2011), 792–799.
[20] F. Petrov and C. Pohoata, *A remark on sets with few distances in* $\mathbb{R}^d$, Proc. Amer. Math. Soc. **149** (2021), 569–571.
[21] D.K. Ray-Chaudhuri and R.M. Wilson, *On t-designs*, Osaka J. Math. **12** (1975), 737–744.

Hiroshi Nozaki, Aichi University of Education, Department of Mathematics Education, 1 Hirosawa, Igaya-cho, Kariya, Aichi, 448-8542 (Japan)
E-mail : `hnozaki@auecc.aichi-edu.ac.jp`