On a Problem Involving Strongly Orthogonal Roots

Qëndrim R. Gashi

Department of Mathematics
University of Prishtina

4 July 2023

Table of Contents

Root systems

Definition

Let V be a vector space over $\mathbb{R}$ and let $(\,,\,)$ be an inner product on V. A finite subset R of non-zero elements of V is called a root system if it satisfies the following:

- R spans V;
- For any $\alpha, \beta \in R$, we have $m_{\alpha,\beta} = 2\frac{(\beta,\alpha)}{(\alpha,\alpha)} \in \mathbb{Z}$;
- For any $\alpha, \beta \in R$, we have $\beta - m_{\alpha,\beta}\alpha \in R$.

Elements of R are called roots.

Root systems

Definition

Let V be a vector space over $\mathbb{R}$ and let $(\,,\,)$ be an inner product on V. A finite subset R of non-zero elements of V is called a root system if it satisfies the following:

- R spans V;
- For any $\alpha, \beta \in R$, we have $m_{\alpha,\beta} = 2\frac{(\beta,\alpha)}{(\alpha,\alpha)} \in \mathbb{Z}$;
- For any $\alpha, \beta \in R$, we have $\beta - m_{\alpha,\beta}\alpha \in R$.

Elements of R are called roots.

Introduced by Killing in the 19th century in order to classify simple Lie algebras, they have since become an important tool and object of study in representation theory and many other areas of mathematics.

Root systems

If for any $\alpha \in R$ and $k \in \mathbb{Z}$ we have $k\alpha \in R$ only for $k = \pm 1$, then we say that R is *reduced*.

Root systems

If for any $\alpha \in R$ and $k \in \mathbb{Z}$ we have $k\alpha \in R$ only for $k = \pm 1$, then we say that R is *reduced*.

The root system R is called *irreducible* if it is not the direct sum of two root systems.

Root systems

If for any $\alpha \in R$ and $k \in \mathbb{Z}$ we have $k\alpha \in R$ only for $k = \pm 1$, then we say that R is *reduced*.

The root system R is called *irreducible* if it is not the direct sum of two root systems.

The *rank* of R is the dimension of the subspace $\mathbb{R}(R)$ that is spanned by all roots.

Root systems

If for any $\alpha \in R$ and $k \in \mathbb{Z}$ we have $k\alpha \in R$ only for $k = \pm 1$, then we say that R is *reduced*.

The root system R is called *irreducible* if it is not the direct sum of two root systems.

The *rank* of R is the dimension of the subspace $\mathbb{R}(R)$ that is spanned by all roots.

The combinatorial structure of irreducible, reduced root systems is encoded in Dynkin diagrams, which can be shown to be only of the following types:

$$A_\ell, B_\ell, C_\ell, D_\ell, E_6, E_7, E_8, F_4 \text{ or } G_2,$$

where the index denotes the corresponding rank.

Root systems

Example: root systems of type A.

Root systems

Example: root systems of type A.

Let V be the hyperplane in $\mathbb{R}^{\ell+1}$ consisting of elements whose sum of coordinates is zero.

Root systems

Example: root systems of type A.

Let V be the hyperplane in $\mathbb{R}^{\ell+1}$ consisting of elements whose sum of coordinates is zero.

Roots of A_ℓ are of the type $\varepsilon_i - \varepsilon_j$, with $1 \leq i \neq j \leq \ell + 1$, and where (ε_i) is the canonical basis of $\mathbb{R}^{\ell+1}$.

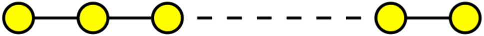
Root systems

Example: root systems of type A.

Let V be the hyperplane in $\mathbb{R}^{\ell+1}$ consisting of elements whose sum of coordinates is zero.

Roots of A_ℓ are of the type $\varepsilon_i - \varepsilon_j$, with $1 \leq i \neq j \leq \ell + 1$, and where (ε_i) is the canonical basis of $\mathbb{R}^{\ell+1}$.

A natural basis of roots of A_ℓ is given by $\alpha_i = \varepsilon_i - \varepsilon_{i+1}\,(i = 1, 2, \ldots, \ell)$. The corresponding Dynkin diagram in this case is a string of ℓ vertices, corresponding to the α_i's, linked as follows:



Strongly orthogonal roots

Definition

In a given a root system R, two distinct roots α and β are said to be strongly orthogonal if neither $\alpha + \beta$ nor $\alpha - \beta$ is a root.

Strongly orthogonal roots

Definition

In a given a root system R, two distinct roots α and β are said to be strongly orthogonal if neither $\alpha + \beta$ nor $\alpha - \beta$ is a root.

One can check immediately that *strongly orthogonal* roots are also *orthogonal* (with respect to the initial inner product), but the converse does not hold in general.

Strongly orthogonal roots

Definition

In a given a root system R, two distinct roots α and β are said to be strongly orthogonal if neither $\alpha + \beta$ nor $\alpha - \beta$ is a root.

One can check immediately that *strongly orthogonal* roots are also *orthogonal* (with respect to the initial inner product), but the converse does not hold in general.

However, in the type A root systems, which will interest us the most, the two notions coincide.

Strongly orthogonal roots

The notion of strongly orthogonal roots first appeared in the classical works of Harish-Chandra in the study of holomorphic discrete series representations and of Kostant and Sugiura in the study of conjugacy classes of real Cartan subalgebras. It has since appeared in many articles in different fields.

Some of the properties of strongly orthogonal roots have been studied in some detail by Agaoka and Kaneda.

Statement of the problem

Let R be a root system. A subset of R consisting of mutually-strongly orthogonal roots is called a strongly orthogonal subset (SOS). Denote the set of all SOS's in R that have exactly k-elements by $SOS_k(R)$. If $\Gamma \in SOS_k(R)$, we denote by $|\Gamma|$ the sum of the elements of Γ.

Statement of the problem

Let R be a root system. A subset of R consisting of mutually-strongly orthogonal roots is called a strongly orthogonal subset (SOS). Denote the set of all SOS's in R that have exactly k-elements by $SOS_k(R)$. If $\Gamma \in SOS_k(R)$, we denote by $|\Gamma|$ the sum of the elements of Γ.

We would like to understand the following general problem: Find the maximal number $\mu = \mu_k(R)$ such that there exist $\Gamma_i \in SOS_k(R)$ $(i = 1, \ldots, \mu)$ with the property that for any two distinct i, j there exists $\Gamma_{i,j} \in SOS_k(R)$ such that

$$|\Gamma_i| - |\Gamma_j| = |\Gamma_{i,j}|. \tag{S}$$

Statement of the problem

Another interpretation of the problem using graph theory: let us consider an undirected graph whose vertices are the elements of $SOS_k(R)$. We write an edge between two vertices Γ_i and Γ_j if and only if (S) holds.

Statement of the problem

Another interpretation of the problem using graph theory: let us consider an undirected graph whose vertices are the elements of $SOS_k(R)$. We write an edge between two vertices Γ_i and Γ_j if and only if (S) holds.

Now, our problem becomes: find a maximum clique (i.e., complete subgraph) for such a graph for any root system. The number of vertices in such a clique is denoted by $\mu = \mu_k(R)$.

Results

Let us first remark that we already know when $\mu_k(R) = 0$ from the fact that maximal strongly orthogonal subsets have already been studied and it was established when $SOS_k(R) = \emptyset$. The point is to calculate $\mu_k(R)$ in other cases.

Known results

Various authors (Y. Agaoka and E. Kaneda; L. Bedullia, A. Gorib and F. Podestà) have contributed to the following result:
The number $\mu_k(R)$ is zero in the following and only following cases:

(i) For $k > \left\lfloor \frac{\ell+1}{2} \right\rfloor$ when $R = A_\ell$;
(ii) For $k > \ell$ when $R = B_\ell$;
(iii) For $k > \ell$ when $R = C_\ell$;
(iv) For $k > 2\left\lfloor \frac{\ell}{2} \right\rfloor$ when $R = D_\ell$;
(v) For $k > 3$ when $R = F_4$;
(vi) For $k > 4$ when $R = E_6$;
(vii) For $k > 7$ when $R = E_7$;
(viii) For $k > 8$ when $R = E_8$;
(ix) For $k > 2$ when $R = G_2$.

Main result

Theorem

Fix $k \in \mathbb{N}$. There exists $N = N(k) \in \mathbb{N}$ such that

$$\mu_k(A_\ell) = \left\lfloor \frac{\ell - (k-1)}{k} \right\rfloor$$

holds for all $\ell \geq N$.

Main result

Theorem

Fix $k \in \mathbb{N}$. *There exists* $N = N(k) \in \mathbb{N}$ *such that*

$$\mu_k(A_\ell) = \left\lfloor \frac{\ell - (k-1)}{k} \right\rfloor$$

holds for all $\ell \geq N$.

For $k = 1$ or 2, we have a complete answer:

Theorem

We have that $\mu_1(A_\ell) = \ell$. *The sequence* $\mu_2(A_\ell)$, *with* $\ell \in \mathbb{N}$, *is equal to* $\lfloor (\ell - 1)/2 \rfloor$ *for* $\ell \geq 13$, *and for* $\ell < 13$ *its terms are* $0, 0, 1, 1, 3, 6, 6, 6, 6, 6, 6, 6$.

More results

Theorem

(B1) *For* $\ell \gg 0$, $\mu_1(B_\ell) = \ell$.

(B2) *For* $\ell \gg 0$,

$$\mu_2(B_\ell) = \begin{cases} \ell - 2 & \text{if } \ell \text{ is even} \\ \ell - 1 & \text{if } \ell \text{ is odd.} \end{cases}$$

(C1) *For* $\ell \gg 0$, $\mu_1(C_\ell) = 2(\ell - 1)$.

(C2) *For* $\ell \gg 0$, $\mu_2(C_\ell) = \ell - 1$.

(D1) $\mu_1(D_\ell) = \ell - 1, \forall \ell \geq 3$.

(D2) *For* $\ell \gg 0$,

$$\mu_2(D_\ell) = \begin{cases} \ell - 1 & \text{if } \ell \text{ is even} \\ \ell - 2 & \text{if } \ell \text{ is odd.} \end{cases}$$

More results

Theorem

(D3) *For* $\ell \gg 0$, *we have*

$$\mu_3(D_\ell) = \begin{cases} 4\left\lfloor \frac{\ell-4}{4} \right\rfloor + 2 & \textit{if } \ell \equiv 3(\textit{mod}4), \\ 4\left\lfloor \frac{\ell-4}{4} \right\rfloor + 1 & \textit{otherwise.} \end{cases}$$

(D4) *For* $\ell \gg 0$, $\mu_4(D_\ell) = \ell - 1$.

(E) $\mu_4(E_6) = 2$, $\mu_k(E_6) = 0$ *for* $k \geq 5$.

(F) $\mu_1(F_4) = 4$, $\mu_2(F_4) = 3$, $\mu_3(F_4) = 3$, $\mu_4(F_4) = 3$, *and* $\mu_k(F_4) = 0$ *for* $k \geq 5$.

(G) $\mu_1(G_2) = 3$, $\mu_2(G_2) = 2$, *and* $\mu_k(G_2) = 0$ *for* $k \geq 3$.

Finite projective planes

Let us recall that a finite projective plane of order n ($n \in \mathbb{N}$) is a collection of lines and points such that:

- every line contains $n + 1$ points,
- every point is on $n + 1$ lines,
- any two distinct lines intersect at exactly one point, and
- any two distinct points lie on exactly one line.

Finite projective planes

Let us recall that a finite projective plane of order n ($n \in \mathbb{N}$) is a collection of lines and points such that:

- every line contains $n + 1$ points,
- every point is on $n + 1$ lines,
- any two distinct lines intersect at exactly one point, and
- any two distinct points lie on exactly one line.

From these conditions it follows that if a plane of order n exists, then there must be exactly $n^2 + n + 1$ points and $n^2 + n + 1$ lines.

Finite projective planes

The existence of finite projective planes of order n can be reduced to the existence of the corresponding incidence matrix $X = (x_{ij})$, where

(i) X is a square matrix of order $n^2 + n + 1$,

(ii) For each i, j we have $x_{i,j} \in \{0, 1\}$,

(iii) The sum of all entries in any row as well as in any column is $n + 1$,

(iv) The inner product of any two distinct rows as well as of any two distinct columns is 1.

Finite projective planes

A well-known conjecture states that finite projective planes exist only for prime power order.

The conjecture remains open, although there are some quite general partial results, like the Bruck-Ryser Theorem which states that if a finite projective plane of order n exists and n is congruent to 1 or 2 $(mod\, 4)$, then n can be written as a sum of two squares.

Many years ago C. Lam proved the non-existence of projective planes of order 10 using a computer, but even the case $n = 12$ remains elusive thus far.

Finite projective planes

If a finite projective plane of order n exists, then we can consider its incidence matrix, take the differences between the first (or any fixed row) and all other rows.

Finite projective planes

If a finite projective plane of order n exists, then we can consider its incidence matrix, take the differences between the first (or any fixed row) and all other rows.

Illustrative example: The incidence matrix, up to permutation, of the projective plane of order 2 is

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Finite projective planes

If we fix the first row and take its difference with each of the other rows, we get the following matrix

$$\begin{pmatrix} 0 & 1 & 1 & -1 & -1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & -1 & -1 \\ 1 & 0 & 1 & -1 & 0 & -1 & 0 \\ 1 & 0 & 1 & 0 & -1 & 0 & -1 \\ 1 & 1 & 0 & -1 & 0 & 0 & -1 \\ 1 & 1 & 0 & 0 & -1 & -1 & 0 \end{pmatrix}$$

Finite projective planes

So, if a finite projective plane of order n exists, we get $n(n+1)$ elements of $SOS_n(A_{n(n+1)})$, which satisfy the property (S) above.

Thus, in this case, $\mu_n(A_{n(n+1)}) \geq n(n+1)$. And we conclude that if $\mu_n(A_{n(n+1)}) < n(n+1)$, then there is no finite projective plane of order n.

We can formulate the following:

Conjecture

For n not equal to a prime-power, it holds that $\mu_n(A_{n(n+1)}) < n(n+1)$.

Remarks

We attempt to better understand the sequences $\mu_k(R)$ not just for the root systems of type A, but for general root systems. Much remains to be done to understand these sequences in general.

Remarks

We attempt to better understand the sequences $\mu_k(R)$ not just for the root systems of type A, but for general root systems. Much remains to be done to understand these sequences in general.

It is not unusual for some phenomena in mathematics to showcase *obstruction* in low dimensions. The question we have posed belongs to that category of problems. So, for a fixed k, we have an *erratic* behavior of $\mu_k(A_\ell)$ for small values of ℓ and eventually that sequence stabilizes for large enough ℓ.

Note: We have fixed the size of the *SOS*'s and allowed the rank of the root systems to vary as opposed to fixing a particular root system of a fixed rank and looking into the finite sequence of numbers associated to it via the procedure dictated by condition (S).

Relations to EKR

These results can be interpreted in the framework of Erdős-Ko-Rado-theory.

And in the context of generalizations to $\{0, \pm 1\}$-vectors (already studied by Deza and Frankl in the '70s).

Let us see this.

EKR approach

Notation: $[n] := \{1, 2, \ldots, n\}$. For $F \subset [n]$, denote $v(F) := (x_i)_{i=1}^n$ the vector where $x_i = 1$ for $i \in F$ and $x_i = 0$ otherwise.

Let $\mathcal{V}(n, k, l) \subset \mathbb{R}^n$ be the set of all $\{0, \pm 1\}$-vectors having exactly k coordinates equal to 1 and l coordinates equal to -1.

Then in our case we focused in type A on the case $\mathcal{V}(n, k, k)$.

EKR approach continued

Alternatively, interested in families of pairs (F_i, G_i), $i = 1, \ldots, m$. Then the condition $\Gamma_i \in SOS_k(A_{n-1})$ is interpreted as:

- $F_i, G_i \in \mathcal{V}(n, k, 0)$;
- $\langle v(F_i), v(G_i) \rangle = 0$.

And condition (S) is restated (only in type A) as:

- $\langle v(F_i), v(G_j) \rangle = 0$, $\forall i \neq j$;
- $\langle v(F_i), v(F_j) \rangle + \langle v(G_i), v(G_j) \rangle = k$, $\forall i \neq j$.

Note: In Deza and Frankl, this is $\langle b_i, b_j \rangle = k$, but here we have two families of k-sets.

New version of (S)

We would like to understand the following general problem: Find the maximal number $\mu = \mu'_k(R)$ such that there exist $\Gamma_i \in SOS_k(R)$ $(i = 1, \ldots, \mu')$ with the property that for any two distinct i, j there exists $\Gamma'_{i,j} \in SOS_{\leq k}(R)$ such that

$$|\Gamma_i| - |\Gamma_j| = |\Gamma'_{i,j}|. \tag{S'}$$

Final remarks

One could attempt to tackle this problem not just from a combinatorial perspective, but also from a geometric perspective, making use of the fact that strong-orthogonality is a condition implying the commutativity of Cayley transforms between Cartan subalgebras. But, that is beyond the scope of the current presentation.

Thank you

Thank you. Hvala.