Erdős–Ko–Rado type problems in root systems.

P. Ó Catháin[1],Q. R. Gashi[2],P.J. Browne[3†].

[1]DCU, Ireland.
[2]University of Prishtina, Kosovo.[3]TUS, Ireland.

8th Workshop on Design Theory, Hadamard Matrices and Applications, Sevilla, 2025.

†Supported by the National Forum for Enhancement of Teaching and Learning and TUS who supported this work through Strategic Alignment of Teaching and Learning Enhancement funding

Motivation

- This work stems from the problem of isometric immersions of Riemannian symmetric spaces into Euclidean spaces.
- It is known that any Riemann manifold can be isometrically immersed into the Euclidean spaces of sufficiently large dimension.
- Y. Agaoka & E. Kaneda ('83) gave bounds on these dimensions for the case of Riemannian symmetric spaces.
- Moreover, they showed that this amounts to a question on the roots of a Lie algebra.
- We give a (very) quick introduction to the basic geometry, before recasting their problem in the appropriate combinatorial setting and expanding on their results.

Symmetric spaces

Definition

A connected Riemannian manifold M is called a symmetric space if for each $p \in M$ there exists a unique isometry $j_p : M \to M$ such that $j_p(p) = p$ and $(dj_p)_p = -Id_p$.

The map j_p is called a (global) symmetry of M at p, the above can also be stated as $j_p^2 = Id$ and p is an isolated fixed point of j_p.

Example

Euclidean space $\mathbb{R}^n$, with $j_p(x) = 2p - x$.

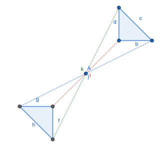


Figure: Point reflection in $\mathbb{R}^2$

Example

The sphere S^n is symmetric. It's metric is inherited from it's embedding, and we know its isometry group acts transitively on S^n. Suffices to give an example about its north pole, $p = (1, 0, \cdots, 0)$, with $j_p(x^1, x^2, \cdots, x^n) = (x^1, -x^2, \cdots, -x^n)$.

Theorem

A symmetric Riemannian manifold M is homogeneous.

Is is know that $I(M)$, the group of isometries on M is a Lie group and act transitively, hence we can identify a symmetric space with the homogeneous space G/K where K is the isotropy subgroup of a point $p \in M$.

Remark

Many questions can now be formulated in terms of $\mathfrak{g}$ and $\mathfrak{k}$, the Lie algebras of G and K.

Theorem (Y. Agaoka & E. Kaneda ('83))

Assume that $s :=$ rank $G/K -$ rank $G +$ rank $K > 0$. Then there exists a subset of roots $\Gamma = \{\beta_1, \cdots, \beta_s\}$, known as strongly orthogonal roots.

Much of their paper is concerned with constructing these sets of roots for various cases. These sets of roots help prove the main result, Theorem 1.4.
We now give a more combinatorial description of these sets of roots and generalise their problem to an EKR type problem.

Root space decomposition

Given a Lie algebra $\mathfrak{g}$ we can decompose it via the root space decomposition:

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in R} \mathfrak{g}_\alpha, \ \mathfrak{g}_0 = \mathfrak{h}$$

The eigenspaces

$$\mathfrak{g}_\alpha := \{x \in \mathfrak{g} | [h, x] = \alpha(h)x \text{ for all } h \in \mathfrak{h}\},$$

for non zero $\alpha \in \mathfrak{h}^*$, known as the root subspaces. The set $\{\alpha \in \mathfrak{h}^*\}$ is called the root system of $\mathfrak{g}$.

$\mathfrak{sl}(n, \mathbb{C})$

The Lie algebra of $\mathfrak{sl}(n, \mathbb{C})$ is an illustrative example to showcase the above decomposition.

Definition

$\mathfrak{g} = \mathfrak{sl}(n, \mathbb{C})$ is comprised of matrices over $\mathbb{C}$ having zero trace.

Then $\mathfrak{h}$ is the subalgebra of diagonal matrices with trace 0. We can define a linear functional as

$$e_i : \mathfrak{h} \to \mathbb{C}, \begin{pmatrix} h_1 & & & \\ & h_2 & & \\ & & \ddots & \\ & & & h_n \end{pmatrix} \to h_i,$$

with $e_1 + \cdots + e_n(\mathfrak{h}) = 0$.

With elementary matrices E_{ij} it is a simple calculation to show that

$$[h, E_{ij}] = (h_i - h_j)E_{ij} = (e_i(h) - e_j(h)) \cdot E_{ij}.$$

Hence the root spaces $\mathfrak{g}_\alpha = \mathfrak{g}_{e_i - e_j}$. The root system is:

$$R := \{e_i - e_j | i \neq j\} \subset \mathfrak{h}^*.$$

At this point we have a set of vectors and if we also include the Killing form we can give a geometric picture to these roots:

A_2 root system

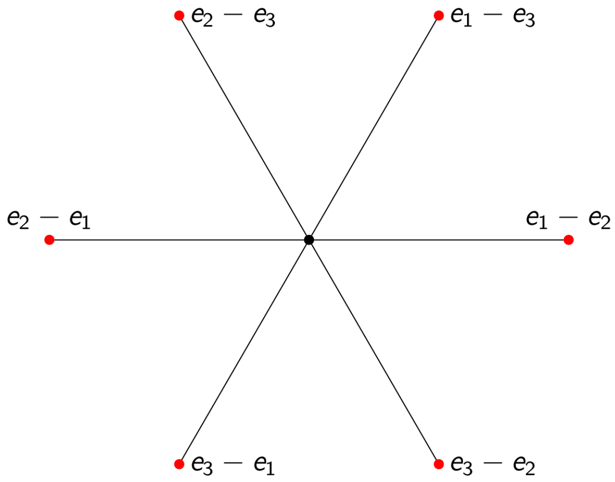


Figure: A_2

Abstract root systems

While the above serves as motivation, today we will be only concerned with combinatorial questions on the root system.

Definition

A subset R of Euclidean space E is called a root system in E if the following hold:

1. R spans E and does not contain $\{0\}$.
2. $\alpha \in R$, then the only multiples of α in R are $\pm\alpha$.
3. Reflections in a hyperplane orthogonal to α leave R invariant.
4. The term $2\frac{(\beta,\alpha)}{(\alpha,\alpha)}$ is in $\mathbb{Z}$.

All irreducible root systems can be classified via their Dynkin diagrams.

Theorem

If R is an irreducible root system of rank ℓ, its Dynkin Diagram is one of the following:

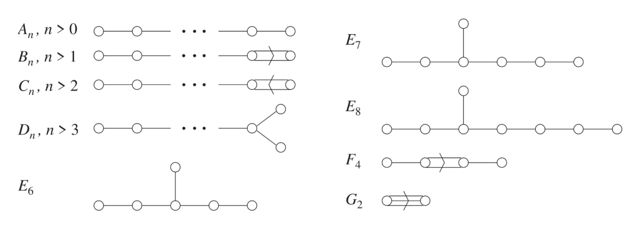


Figure: *A, B, C, D the classical and the exceptional E_6, E_7, E_8, F_4, F_4*

Strongly Orthogonal roots

Our questions will involve strongly orthogonal roots, which we recall here.

Lemma

Let $\alpha, \beta \in R$*, if* $(\alpha, \beta) < 0$ *then* $\alpha + \beta \in R$*. Similarly if* $(\alpha, \beta) > 0$ *then* $\alpha - \beta \in R$.

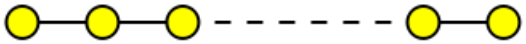
Definition

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

Examples

Consider the root system for A_5, spanned by $\alpha_1, \cdots, \alpha_5$.

$$
\begin{aligned}
\alpha_1 &= (1, 0, \cdots, 0), \; e_1 - e_2, \\
&\vdots \\
\alpha_6 &= (1, 1, 0, 0, 0), \; e_1 - e_3, \\
&\vdots \\
\alpha_{10} &= (1, 1, 1, 0, 0), \; e_1 - e_4, \\
&\vdots \\
\alpha_{13} &= (1, 1, 1, 1, 0), \; e_1 - e_5, \\
\alpha_{14} &= (0, 1, 1, 1, 1), \; e_2 - e_6, \\
\alpha_{15} &= (1, 1, 1, 1, 1), \; e_1 - e_6.
\end{aligned}
$$

A_n 

Examples of Strongly orthogonal sets of roots are

$$
\{\alpha_2, \alpha_4\}, \{\alpha_6, \alpha_9\}
$$
$$
\{\alpha_1, \alpha_8\}, \{\alpha_1, \alpha_5\}.
$$

Set systems

Motivation for the EKR Theorem. Consider a base set $\{1, \cdots, 7\}$.
An intersecting 3-set from the base set:

$$\{1,2,3\},\{1,2,4\},\{1,2,5\},\{1,2,6\},\{1,2,7\}$$
$$\{1,3,4\},\{1,3,5\},\{1,3,6\},\{1,3,7\},\{2,3,4\},$$
$$\{2,3,5\},\{2,3,6\},\{2,3,7\}.$$

Another intersecting 3-set where every set always has $\{1\}$.

$$\{1,2,3\},\{1,2,4\},\{1,2,5\},\{1,2,6\},\{1,2,7\}$$
$$\{1,3,4\},\{1,3,5\},\{1,3,6\},\{1,3,7\},\{1,4,5\}$$
$$\{1,4,6\},\{1,4,7\},\{1,5,7\},\{1,5,6\},\{1,6,7\}.$$

EKR Problem

Question

What is the largest intersecting set system ?

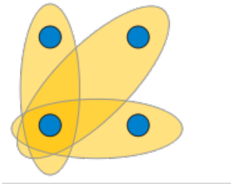


Figure: Sunflower/Dictatorship/Pencil point.

Erdős–Ko–Rado theorem

Let $n, k \in \mathbb{N}$ and write $[n] := \{1, 2, \ldots, n\}$. Denote by $\mathcal{V}(n, k) := \{X \subseteq [n] : |X| = k\}$ the set of k-element subsets of $[n]$.

Theorem (EKR)

Let $\mathcal{F} \subseteq \mathcal{V}(n, k)$ and suppose that $X \cap Y \neq \emptyset$ for all $X, Y \in \mathcal{F}$. Then

$$|\mathcal{F}| \leq \binom{n-1}{k-1}.$$

Moreover, if $n > 2k$, equality holds if and only if $\mathcal{F}$ consists of all elements of $\mathcal{V}(n, k)$ that contain a given element from $[n]$.

Graphs

Equivalently, let $\Gamma_{(n,k)}$ be the graph which has as vertex $V(n,k)$, with an edge between two $k-$subsets when they have non-trivial intersection. The EKR result gives us an upper bound on the size of maximal cliques in $\Gamma_{(n,k)}$. Moreover it classifies the maximal cliques.

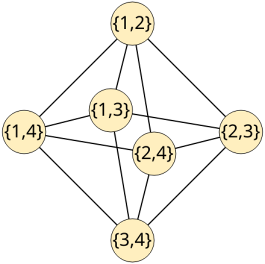


Figure: The Johnson graph $J(4,2)$

Our Problem

Given a root system R, a subset of pairwise strongly orthogonal roots is called a strongly orthogonal subset or SOS. Denote the set of $SOS's$ of k elements in R by $SOS_k(R)$.

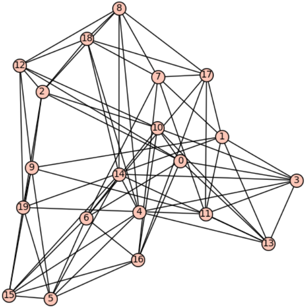


Figure: Strongly Orthogonal roots in A_4.

Definition

Letting $\Gamma \in SOS_k(R)$, we write $|\Gamma| = \sum_{\gamma \in \Gamma} \gamma$ for the sum of the roots in Γ. A subset $\mathcal{F} \subseteq SOS_k(R)$ is a *SOS-clique* if and only if for every $\Gamma_i, \Gamma_j \in \mathcal{F}$ there exists some $\Gamma_{i,j} \in \mathcal{F}$ such that

$$|\Gamma_i| - |\Gamma_j| = |\Gamma_{i,j}|. \tag{1}$$

The maximal size of an SOS-clique in $SOS_k(R)$ will be denoted $\mu_k(R)$.

This is a problem of Erdős–Ko–Rado type:

- Construct a graph in which vertices are labelled by the vectors $|\Gamma|$ for $\Gamma \in SOS_k(R)$, with an edge between $|\Gamma_i|$ and $|\Gamma_j|$ if and only if the difference of their vectors is again the label of a vertex in the graph.
- The SOS-clique of the definition is a clique in this graph. We give both an upper bound on the size of maximal clique and a characterisation of all maximal cliques when ℓ is sufficiently large in terms of k.

Example

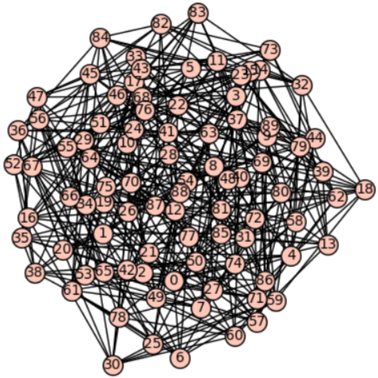
In the above example with A_5, we have

$$\begin{aligned} |\Gamma_1| =& |\{\alpha_6, \alpha_9\}| && = (1,1,0,1,1), \\ |\Gamma_2| =& |\{\alpha_2, \alpha_4\}| && = (0,1,0,1,0), \\ |\Gamma_{1,2}| = |\Gamma_1| - |\Gamma_2| =& |\{\alpha_1, \alpha_5\}| && = (1,0,0,0,1). \end{aligned}$$

While harder for sets of more than three roots, the computations follow a nice pattern due to the easy nature of A_n.

```
89 : [] }
g=Graph(dict)
```

In [2]:
```
g.show()
```



In [3]:
```
g.clique_number()
```

Out[3]: 3

Figure: $SOS_2(A_5)$

A starting point

Recall the Dynkin diagram for A type systems,

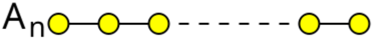


Figure: A type

Independent nodes will help us construct examples of $SOS's$.
Define $\beta_j = \sum_{i=1}^{k} \alpha_{i+j}$, then $\Gamma_1 = \{\beta_j : j = 0, \ldots, k-1\}$ is such a set. The sum $|\Gamma_1| = \sum_{j=0}^{k-1} \beta_j$ is a vector with the first k entries equal to $+1$ followed by k entries equal to -1.
Let $\mathcal{F}$ be a SOS clique, and we can assume wlog that $\Gamma_1 \in \mathcal{F}$. The supports of Γ_1 and Γ_i intersect in exactly k positions if Γ_i also belongs to $\mathcal{F}$.

Definition

Given an SOS clique, $\mathcal{F}$. If for all $\Gamma_i, \Gamma_j \in \mathcal{F}$ the sets $S(\Gamma_i, \Gamma_j)$ are equal, we say $\mathcal{F}$ is a sunflower.

The following lemmas are needed:

Lemma

Suppose that $\mathcal{F} \subset SOS_k(A_l)$ is a sunflower. Then $|\mathcal{F}| \leq \lfloor \frac{l+1}{k} \rfloor - 1$.

Proof.

- Consider the set of indices on which $|\Gamma_i|$ and $|\Gamma_j|$ agree, call this set X, and we know $|X| = k$.
- $|\Gamma_i| = X_i \cup X$,
- $k|\mathcal{F}| + k \leq \ell + 1$.

$\square$

Lemma

For an SOS clique $\mathcal{F}$, suppose that $S(\Gamma_i, \Gamma_j) = S(\Gamma_x, \Gamma_y)$, if and only if $\{\Gamma_i, \Gamma_j\} = \{\Gamma_x, \Gamma_y\}$. Then $|\mathcal{F}| \leq \binom{2k}{k} + 1$.

Proof.

- Fix $\Gamma_1 \in \mathcal{F}$, the support of some Γ_i agrees in exactly k positions.
- By assumption these are all distinct. A choice of $2k$ positions.

$\square$

Results

Theorem

For any $k \in \mathbb{N}$, we have $\mu_k(A_\ell) \leq \ell + 1$. For $\ell > k4^k$,

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

If $\ell > k4^k$ and $|\mathcal{F}| = \mu_k(A_\ell)$ then $\mathcal{F}$ is a sunflower.

Proof.

- Consider a maximal sunflower $\{\Gamma_1, \cdots, \Gamma_m\} \in \mathcal{F}$, The support of each $|\Gamma_i|$ is $X \cup X_i$ all disjoint. Assuming the second lemma is not in effect, $|\mathcal{F}| = m + 1$. Also $\ell + 1 \geq k(m+1)$ and we have our result.
- Suppose there exists $\Gamma_{m+1} \in \mathcal{F}$ such that $S(\Gamma_1, \Gamma_{m+1}) \neq X$. We know it intersects the m, X_i's non trivially, so that $k \geq m - 1$.
- At most $\binom{2k}{k} - 1$ possible intersections with support of Γ_1, distinct from X. Hence $|\mathcal{F}| \leq k\binom{2k}{k} + 1$.
- By a theorem of *Ray-Chaudhuri & Wilson*, the number of $2k$-sets such that all pairwise intersections have size k is bounded by $\ell + 1$, for any choice of ℓ and k. This gives the general upper bound.

$\square$

Theorem

The sequence $\mu_2(A_\ell)$ *is* $0, 0, 1, 1, 3$ *for* $1 \leq \ell \leq 5$. *For* $6 \leq \ell \leq 13$, *it is equal to* 6 *and for* $\ell \geq 13$, *its value is* $\lfloor (\ell - 1)/2 \rfloor$.

Exceptional cases

For the the remaining finite cases, we can employ computational methods. A Python script to find all pairs of strongly orthogonal roots was written and with the aid of the cliquer method in SAGE we have some partial results to present.

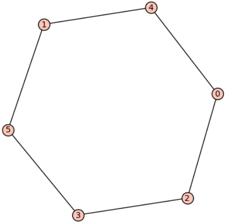


Figure: G_2, μ_2

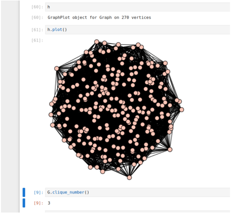


Figure: E_6, μ_2

Exceptional cases

Theorem (preliminary)

- $G_2: \;\; \mu_2 = 2,$
- $E_6: \;\; \mu_2, \mu_3, \mu_4 = 3, 5, 5$

Next steps

- Motivated by *I. Landjev, A. Rousseva, K. Vorobev*, to improve the bounds seen in *'On binary codes with distances d and $d+2$'*, - Landjev & Vorob'ev.
- A better geometric interpretation of the results we have.
- Projective planes and designs.

Thank you,
Questions?