Classifying Generalized Symmetric Spaces for Unipotent and Semisimple Elements in $SO(3, p)$

Hanson Hao, Jake Sutter

Illinois Mathematics and Science Academy
Mentor: Dr. Ellen Ziliak (Benedictine University)

IMSAloquium, April 26, 2019

Special Orthogonal Group

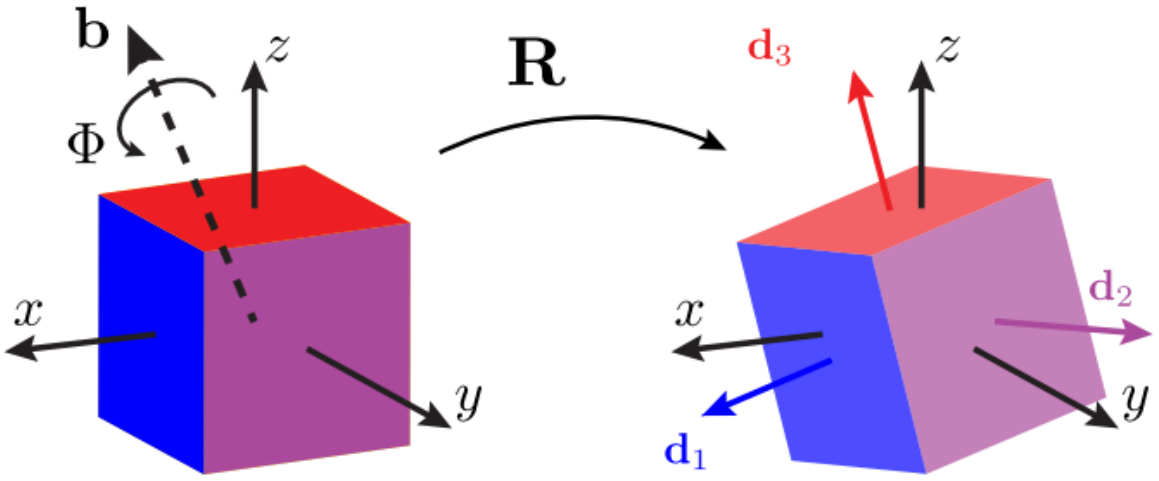
Definition

The **Special Orthogonal Group** $SO(n, p)$ is the group of $n \times n$ matrices in a finite field $\mathbb{F}_p$ that are both determinant 1 and orthogonal. We can think of this as a set of rectangular prisms whose volumes are all congruent to $1 \mod p$.

Example of some elements in $SO(3, 5)$: $\left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 2 \\ 1 & 2 & 1 \\ 2 & 1 & 1 \end{bmatrix} \right\}$

Motivations

- Software can be optimized with symmetric matrices.
- Special orthogonal matrices are also rotation matrices.



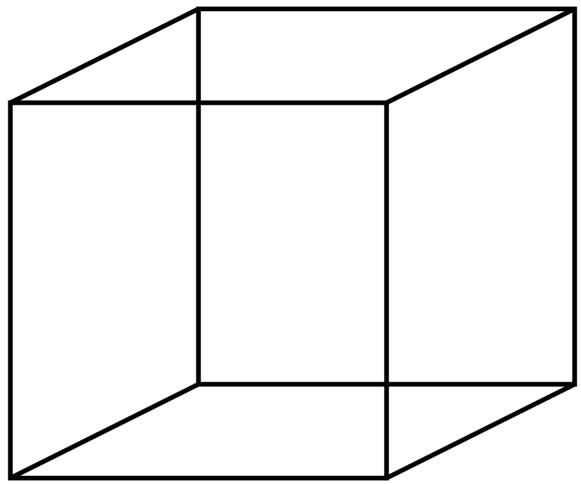
- Symmetric matrices connected to 3-pauli matrices, used in quantum mechanics.
- Future use: nobody could have predicted the extent to which calculus would be used.

Generating $SO(3, p)$ - The Bad Way

- Loop over all elements of $M_3(\mathbb{F}_p)$.
  - Uses 9 embedded loops, one for each variable.
- Check for both special and orthogonal condition.
- Has complexity of $O(p^9)$.
- For example, $p = 13$ means testing $13^9 = 10604499373$ matrices.

How To Improve Our Method

- Geometric interpretation of both special and orthogonal.
- Matrix represents parallelepiped.
- Vectors are pairwise orthogonal.
- Volume contained is 1.
- $|\mathbf{v}|^2 \equiv 1 \mod p$.



Generating $SO(3, p)$ - A Better Way

- List all vectors **v** such that $|\mathbf{v}|^2 \equiv 1 \mod p$. $O(p^3)$

Generating $SO(3, p)$ - A Better Way

- List all vectors **v** such that $|\mathbf{v}|^2 \equiv 1 \mod p$. $O(p^3)$
- List the pairs of vectors that are pairwise orthogonal, $\mathbf{u} \cdot \mathbf{v} \equiv 0 \mod p$. $O(p^4)$

Generating $SO(3, p)$ - A Better Way

- List all vectors **v** such that $|\mathbf{v}|^2 \equiv 1 \mod p$. $O(p^3)$
- List the pairs of vectors that are pairwise orthogonal, $\mathbf{u} \cdot \mathbf{v} \equiv 0 \mod p$. $O(p^4)$
- Use the two lists to find a third vector pairwise orthogonal to all pairs of orthogonal vectors. $O(p^5)$

Further improvements

- We proved that there is exactly one vector pairwise orthogonal to a pair of vectors.

$$A = \begin{bmatrix} a & b & c \\ d & e & f \\ bf - ce & cd - af & ae - bd \end{bmatrix}$$

- Thus our final complexity is equal to the 'slowest' step, $O(p^4)$.

Symmetric Spaces: Introduction

- A matrix is symmetric if $B = B^T$.

$$\begin{bmatrix} a & d & e \\ d & b & f \\ e & f & c \end{bmatrix}^T = \begin{bmatrix} a & d & e \\ d & b & f \\ e & f & c \end{bmatrix}$$

- In $\mathbb{R}$ the set of all symmetric matrices $R_T = \{B \in GL_3(\mathbb{R}) | B = B^T\}$ is a symmetric space.
- We are interested in the function $\theta : SO(3,p) \to SO(3,p)$ where $\theta(X) = AXA^{-1}$ for some $A \in O(3,p)$.
- We observe that, $\theta(\theta(X)) = X$ so θ is an *involution*.

Symmetric Spaces: Introduction

- Define sets R and Q such that
  $R = \{X \in SO(3,p) | \theta(X)^{-1} = X\}$
  and $Q = \{X\theta(X)^{-1} | X \in SO(3,p)\}$.
- We will call R the *Extended Symmetric Space* and Q the *General Symmetric Space*.

Symmetric Spaces: Introduction

- Define sets R and Q such that
  $R = \{X \in SO(3,p) | \theta(X)^{-1} = X\}$
  and $Q = \{X\theta(X)^{-1} | X \in SO(3,p)\}$.
- We will call R the *Extended Symmetric Space* and Q the *General Symmetric Space*.
- As one might guess from their names, $Q \subseteq R$.
- R generalizes the idea of a symmetric matrix $B = B^T$, while Q generalizes the idea of the set of symmetric matrices expressible as BB^T.

Symmetric Spaces: Introduction

- For the Special Orthogonal Group, we have four different involutions θ.

Theorem (Benim et al)

If $\theta(X) = AXA^{-1}$ *is an involution then* $A^2 = \pm I$.

	$A^2 = I$	$A^2 = -I$
$\mathbb{F}_p$	Type 1	Type 3
$\mathbb{F}_p[\sqrt{\alpha}]$	Type 2	Type 4

Symmetric Spaces: Introduction

- For Type 1 involutions, we define 2 isomorphic subclassses (Benim et al):
  - Class 1: Represented by

$$A_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

  - This is the involution subclass on which we made the most progress.

Symmetric Spaces: Introduction

- For Type 1 involutions, we define 2 isomorphic subclassses (Benim et al):
  - Class 2: Represented by

$$\begin{bmatrix} 1-2\frac{a^2}{M_p} & 0 & \frac{2ab}{M_p} \\ 0 & 1 & 0 \\ \frac{2ab}{M_p} & 0 & 1-2\frac{b^2}{M_p} \end{bmatrix}$$

where M_p is nonsquare in $\mathbb{F}_p$ and $a^2+b^2=M_p$, as described by Benim et al. This is an example of the below form when 2 is not a square:

$$A_2 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

A_2 is the specific case obtained by setting $a=1$, $b=1$ and $M_p=2$. The general form is required in a field where 2 is a square.

- For Type 2 we only have preliminary data at this point.

Symmetric Spaces: Introduction

Theorem

There are no Type 3 or 4 involutions for $SO(3, p)$.

Proof.

A Type 3 or 4 involution is $\theta(g) = AgA^{-1}$, where $A^2 \equiv -I$ and A is orthogonal. From orthogonality, A has determinant ± 1 and thus A^2 has determinant 1. However, $-I_3$ has determinant -1, so there are no Type 3 or 4 involutions for 3x3 matrices.

□

Corollary

There are no Type 3 or 4 involutions for any nxn matrices where n is odd.

Unipotent and Semisimple Matrices

We can further divide up the sets R and Q into *unipotent* and *semisimple* matrices.

Definition

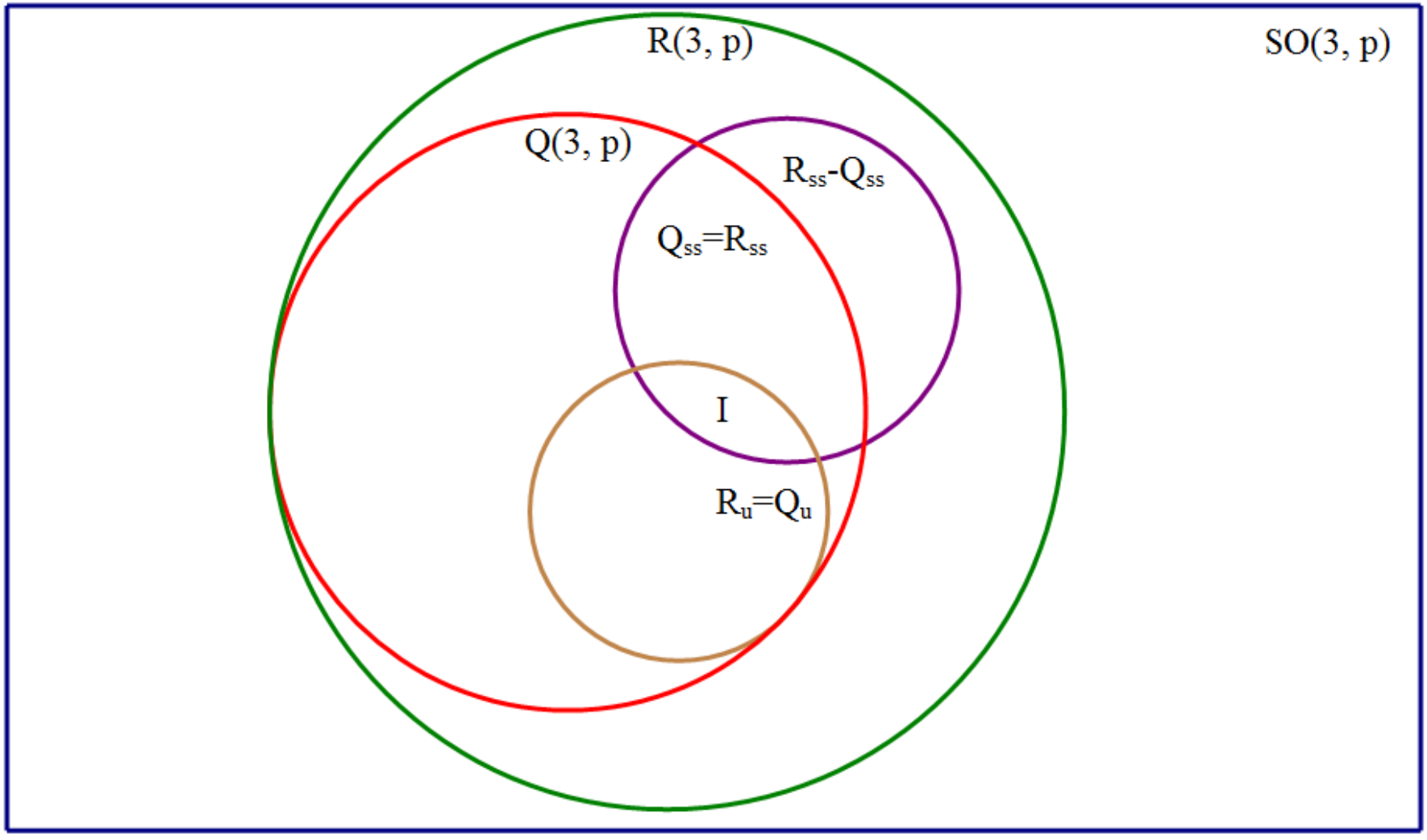
A *unipotent* 3x3 matrix only has an eigenvalue of 1 with algebraic multiplicity 3.

Definition

A *semisimple* 3x3 matrix has a minimal polynomial that splits into distinct linear factors. Most commonly, the matrix has 3 distinct eigenvalues.

Unipotent and Semisimple Matrices

The relationships between the previously described sets:



Unipotent and Semisimple Matrices

Theorem

Every matrix in $SO(3,p)$ *has eigenvalues* 1, λ, $\frac{1}{\lambda}$.

Proof.

It is well known that every orthogonal matrix must have 1 as an eigenvalue. In addition, the product of the three eigenvalues must be 1, the determinant of the matrix. The result follows. $\square$

Unipotent and Semisimple Matrices

Theorem

Every matrix in $SO(3,p)$ has eigenvalues 1, λ, $\frac{1}{\lambda}$.

Proof.

It is well known that every orthogonal matrix must have 1 as an eigenvalue. In addition, the product of the three eigenvalues must be 1, the determinant of the matrix. The result follows. □

Corollary

Every non-identity matrix in R and Q is either unipotent or semisimple.

Proof.

If $\lambda = 1$, the matrix is unipotent; if $\lambda \neq \pm 1$, then the matrix is semisimple. If $\lambda = -1$, then the only orthogonal matrix in R that has eigenvalues $1, -1, -1$ is symmetric and thus semisimple. □

Unipotent and Semisimple Matrices

The following tables indicate the patterns we have observed.
For type 1 involutions in the same class as A_1:

	$\lvert R\rvert$	$\lvert Q\rvert$	$\lvert R_u\rvert$	$\lvert Q_u\rvert$	$\lvert R_{ss}\rvert$	$\lvert Q_{ss}\rvert$
$p \equiv 1 \mod 4$	p^2+1	T_p	$2p-1$	$2p-1$	$(p-1)^2+2$	$T_{p-2}+1$
$p \equiv 3 \mod 4$	p^2+1	T_{p-1}	1	1	p^2+1	T_{p-1}

Unipotent and Semisimple Matrices

The following tables indicate the patterns we have observed.
For type 1 involutions in the same class as A_1:

	$\lvert R\rvert$	$\lvert Q\rvert$	$\lvert R_u\rvert$	$\lvert Q_u\rvert$	$\lvert R_{ss}\rvert$	$\lvert Q_{ss}\rvert$
$p \equiv 1 \mod 4$	p^2+1	T_p	$2p-1$	$2p-1$	$(p-1)^2+2$	$T_{p-2}+1$
$p \equiv 3 \mod 4$	p^2+1	T_{p-1}	1	1	p^2+1	T_{p-1}

For type 1 involutions in the same class as A_2:

	$\lvert R\rvert$	$\lvert Q\rvert$	$\lvert R_u\rvert$	$\lvert Q_u\rvert$	$\lvert R_{ss}\rvert$	$\lvert Q_{ss}\rvert$
$p \equiv 3 \mod 8$	p^2+1	T_p	$2p-1$	$2p-1$	$(p-1)^2+2$	$T_{p-2}+1$
$p \equiv 5 \mod 8$	p^2+1	T_{p-1}	1	1	p^2+1	T_{p-1}

where $T_n = \frac{n(n+1)}{2}$ represents the nth triangular number.

Counting R_u, Type 1, Class 1

Theorem

The number of unipotent matrices in the extended symmetric space $R(3,p)$ for involution A_1, where p is an odd prime, is:

$$|R_u| = \begin{cases} 2p-1 & p \equiv 1 \mod 4 \\ 1 & p \equiv 3 \mod 4 \end{cases}$$

Proof

Consider the 3x3 special, orthogonal, and unipotent matrix

$$M = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}.$$

in the finite field $\mathbb{Z}_p$.

We must have $b \equiv d$, $g \equiv -c$, and $f \equiv -h$ because $AM = M^T A$.

Counting R_u, Type 1, Class 1

$$M = \begin{bmatrix} a & b & c \\ b & e & f \\ -c & -f & i \end{bmatrix}$$

$$char(M) = -\lambda^3 + \lambda^2(a+e+i) + \ldots \Rightarrow i \equiv 3 - a - e$$

$$M = \begin{bmatrix} a & b & c \\ b & e & f \\ -c & -f & 3-a-e \end{bmatrix}.$$

Counting R_u, Type 1, Class 1

$$char(M) = -\lambda^3 + 3\lambda^2$$
$$+\lambda(e^2 - 3a + a^2 - 3e + ea - f^2 + b^2 - c^2) + \ldots$$

so we need

$$e^2 - 3a + a^2 - 3e + ea - f^2 + b^2 - c^2 \equiv -3$$
$$\Rightarrow 2e^2 - 6a + 2a^2 - 6e + 2ea - 2f^2 + 2b^2 - 2c^2 \equiv -6. \quad (1)$$

Subtracting the length-1 orthogonality conditions from equation (1) gives

$$-4c^2 - 4f^2 \equiv 0$$
$$\Rightarrow c^2 + f^2 \equiv 0.$$

Counting R_u, Type 1, Class 1

- If $p \equiv 3 \mod 4$, then -1 is not a quadratic residue, and there is only one solution, the identity matrix.
- If $p \equiv 1 \mod 4$, then -1 is a quadratic residue. First, take $f \equiv \sqrt{-1}c$:

$$M = \begin{bmatrix} a & b & c \\ b & e & \sqrt{-1}c \\ -c & -\sqrt{-1}c & 3-a-e \end{bmatrix}.$$

Counting R_u, Type 1, Class 1

$$-ac - b\sqrt{-1}c + 3c - ac - ec \equiv 0 \tag{2}$$

$$-bc - e\sqrt{-1}c + 3\sqrt{-1}c - a\sqrt{-1}c - e\sqrt{-1}c \equiv 0 \tag{3}$$

Rearranging (2), we have

$$3\sqrt{-1}c - a\sqrt{-1}c - e\sqrt{-1}c \equiv a\sqrt{-1}c - bc.$$

Substituting into equation (3), we have

$$-bc - e\sqrt{-1}c + a\sqrt{-1}c - bc \equiv 0$$

$$\Rightarrow -2b - e\sqrt{-1} + a\sqrt{-1} \equiv 0.$$

Counting R_u, Type 1, Class 1

We also have $(3-a-e)^2 \equiv 1 \Rightarrow 3-a-e \equiv \pm 1$.

- When $3-a-e \equiv 1$, after doing some substitutions, we get

$$M = \begin{bmatrix} \frac{2-c^2}{2} & (\frac{2-c^2}{2})\sqrt{-1} - \sqrt{-1} & c \\ (\frac{2-c^2}{2})\sqrt{-1} - \sqrt{-1} & \frac{c^2+2}{2} & \sqrt{-1}c \\ -c & -\sqrt{-1}c & 1 \end{bmatrix}$$

  This matrix can take on $p-1$ values, depending on the value of $c \not\equiv 0$.

- When $3-a-e \equiv -1$, we get 0 solutions.

Counting R_u, Type 1, Class 1

Instead, if $f \equiv -\sqrt{-1}c$, the only solution(s) are

$$M = \begin{bmatrix} \frac{2-c^2}{2} & \sqrt{-1} - (\frac{2-c^2}{2})\sqrt{-1} & c \\ \sqrt{-1} - (\frac{2-c^2}{2})\sqrt{-1} & \frac{c^2+2}{2} & -c\sqrt{-1} \\ -c & c\sqrt{-1} & 1 \end{bmatrix}$$

where the matrix can take on $p-1$ values, depending on the value of $c \not\equiv 0$.
Adding the cases together along with $c \equiv 0$, equivalent to the $p \equiv 3 \mod 4$ case, there are a total of $2p-1$ matrices in R_u.

□

Counting R_u, Type 1, Class 2

Theorem

The number of unipotent matrices in the extended symmetric space $R(3,p)$ for involution A_2, where p is an odd prime, is:

$$|R_u| = \begin{cases} 2p-1 & p \equiv 3 \mod 8 \\ 1 & p \equiv 5 \mod 8 \end{cases}$$

Counting R_u, Type 1, Class 2

Proof

Similar to the previous proof, but instead with cases:

$$\begin{bmatrix} \frac{x^2+8}{8} & \frac{-x^2\sqrt{-2}+4x}{8} & \frac{x^2+4x\sqrt{-2}}{8} \\ \frac{-x^2\sqrt{-2}-4x}{8} & \frac{4-x^2}{4} & \frac{-x^2\sqrt{-2}+4x}{8} \\ \frac{x^2-4x\sqrt{-2}}{8} & \frac{-x^2\sqrt{-2}-4x}{8} & \frac{x^2+8}{8} \end{bmatrix}$$

with $x \not\equiv 0$ for $p-1$ cases,

$$\begin{bmatrix} \frac{x^2+8}{8} & \frac{x^2\sqrt{-2}+4x}{8} & \frac{x^2-4x\sqrt{-2}}{8} \\ \frac{x^2\sqrt{-2}-4x}{8} & \frac{4-x^2}{4} & \frac{x^2\sqrt{-2}+4x}{8} \\ \frac{x^2+4x\sqrt{-2}}{8} & \frac{x^2\sqrt{-2}-4x}{8} & \frac{x^2+8}{8} \end{bmatrix}$$

with $x \not\equiv 0$ for another $p-1$ cases, and the identity matrix for 1 case and a total count of $2p-1$. □

R_u and Q_u

Conjecture

$$R_u = Q_u$$

for all R and Q in any type 1 involution with given p.

We have verified that this is true for type 1 involutions of class 1:

R_u and Q_u

Proof

The identity matrix I is clearly in Q_u. The other matrices in $R_u(3, p)$ for this case can be represented by

$$M_1 = \begin{bmatrix} \frac{2-x^2}{2} & \frac{2-x^2}{2}\sqrt{-1} - \sqrt{-1} & x \\ \frac{2-x^2}{2}\sqrt{-1} - \sqrt{-1} & \frac{x^2+2}{2} & x\sqrt{-1} \\ -x & -x\sqrt{-1} & 1 \end{bmatrix}.$$

or

$$M_2 = \begin{bmatrix} \frac{2-x^2}{2} & \sqrt{-1} - \frac{2-x^2}{2}\sqrt{-1} & x \\ \sqrt{-1} - \frac{2-x^2}{2}\sqrt{-1} & \frac{x^2+2}{2} & -x\sqrt{-1} \\ -x & x\sqrt{-1} & 1 \end{bmatrix}$$

where x is a nonzero free variable.

R_u and Q_u

Let

$$g_1 = \begin{bmatrix} 1 & c\sqrt{-1} & c \\ \frac{c\sqrt{-1}}{c-1} & \frac{-c^2+c-1}{c-1} & c\sqrt{-1} \\ -\frac{c}{1-c} & -\frac{c}{1-c}\sqrt{-1} & 1 \end{bmatrix}.$$

where $x = 2c$. $g_1 \in SO(3,p)$ and $g_1 a g_1^{-1} a^{-1} = M_1$, so $M_1 \in Q_u$.
Let

$$g_2 = \begin{bmatrix} 1 & -c\sqrt{-1} & c \\ -\frac{c\sqrt{-1}}{c-1} & \frac{-c^2+c-1}{c-1} & -c\sqrt{-1} \\ -\frac{c}{1-c} & \frac{c}{1-c}\sqrt{-1} & 1 \end{bmatrix}.$$

where $x = 2c$. $g_2 \in SO(3,p)$, and $g_2 a g_2^{-1} a^{-1} = M_2$, so $M_2 \in Q_u$.
Since all matrices in R_u are also elements of Q_u, $R_u \subseteq Q_u$, so $R_u = Q_u$. □

Conclusions and Future Work

- Prove the remaining conjectures for the sizes of R and Q and their subsets
- Verify that there are only 2 isomorphism classes for type 1 involutions
- Work on Type 2 involutions as our preliminary results differ from Benim et. al.
- Extend to higher-dimension matrices

Acknowledgments

- We'd like to thank our mentor, Dr. Ellen Ziliak, without whose guidance and support this project would have been impossible.
- We'd also like to thank the Student Inquiry and Research Program at the Illinois Math and Science Academy for making this research opportunity possible.

□

- Grove, L. C. (2002). Classical groups and geometric algebra. Providence, RI: American Mathematical Society.
- Hansen, M., Nordbye, A., & Ziliak, E. (n.d.). Classification of Generalized Symmetric Spaces of the Special Orthogonal Group. College of Science Summer Research Program 2015.
- Benim, R. W., Dometrus C. E., Helminck, A.G., Wu L. (2014). Isomorphy Classes of Involutions of $SO(n, k, \beta)$ and SP$(2n, k)$ where $n > 2$. Mathematics Subject Classification.