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

Jacob Sutter and Hason Hao

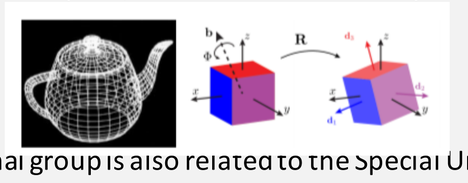
1 IMSA Illinois Mathematics and Science Academy

ABSTRACT

In this paper, we look at the Special Orthogonal group of 3x3 matrices over a finite field, denoted SO(3,p). In particular, we focus on classifying the generalized symmetric spaces, which are defined by an involution $f: SO(3,p) \to SO(3,p)$ such that $f(f(M)) = M$, for these matrices. We begin by explaining what types of involutions exist for our group, and once those involutions are established, we classify two important spaces: the Extended Symmetric Space **R** and the General Symmetric Space **Q**. We describe these spaces for the two isomorphy classes of involutions (building off of Benim & Wu) through counting arguments, in which we split **R** and **Q** into unipotent and semisimple cases. Some counting arguments are established for the size of $\mathbf{R_u}$, $\mathbf{Q_u}$, and $\mathbf{R_{ss}}$ (unipotent matrices in **R**, unipotent matrices in **Q**, and semisimple matrices in **R**, respectively). Further progress can be made on verifying our other conjectures and generalizing our results to field extensions. Applications of our research can be seen in physics, where the SO(3,p) matrices are particularly effective at describing the effects of rotation and spin.

MOTIVATIONS

Computer Graphics: Rotational Matrices are also Special Orthogonal. Because special orthogonal matrices preserve size and shape, they are used to rotate objects in 3D space, and thus can be used by computers to animate objects in a 3D scene.



Quantum Physics The Special Orthogonal group is also related to the Special Unitary group, which have a basis formed by the three Pauli matrices. The Pauli matrices are used to represent spin of particles in quantum mechanics.

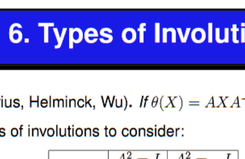
DEFINITIONS

2. Matrix Operations

Definition 1. *The **transpose** takes a matrix A and flips it about its diagonal to form another matrix, denoted A^T.*

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

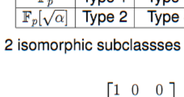
Definition 2. *The **determinant** of a square matrix A is a notion of the area/volume/hyper-volume enclosed within the region formed by the parallelpiped with sides being the row or column vectors of the matrix.*



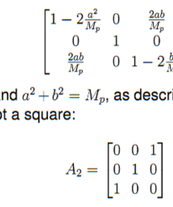
3. Special Orthogonal Group

Definition 3. *A matrix A is **special** if the determinant of A is 1.*

Definition 4. *A matrix is **orthogonal** if all of its row (or column) vectors are pairwise orthogonal. Equivalently, a matrix A is orthogonal if $AA^T = A^TA = I$.*



Definition 5. *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 special 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 $SO(3,5)$: $\left\{ \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 2 \\ 1 & 2 & 1 \\ 2 & 1 & 1 \end{bmatrix} \right\}$

4. How to Generate $SO(3,p)$

The Bad Way: We can iterate over all members of $M(3,p)$, but this gives us an algorithm with complexity $O(p^9)$.

- Works okay for small $p <= 13$, where we test $13^9 = 10,604,499,373$ matrices.
- To generalize our results, we were required to look at $p > 13$.

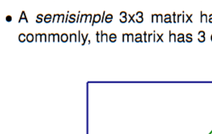
The Good Way:

1. First find all vectors **v** with $|\mathbf{v}|^2 \equiv 1 \mod q$. This step has complexity $O(p^3)$.
2. Use list of vectors to find all pairs of orthogonal vectors. Complexity $O((p^2)^2) = O(p^4)$.
3. Find a third vector which is pairwise orthogonal to the first two. Complexity $O(p^5)$
4. Check that the matrix formed by the 3 vectors is special. Complexity $O(1)$

- The complexity is equal to the slowest step, thus this algorithm has complexity of $O(p^5)$
- We later combined the last two steps into one with complexity of $O(1)$ due to us finding an expression for the last vector, thus our algorithm has complexity $O(p^4)$.
- Instead of being limited to $p = 13$, we have gone as high as $p = 101$

5. Involutions and Symmetric Spaces

- Our goal is to study symmetric spaces. First we must describe symmetry.



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

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

- In $\mathbb{R}$ the set of all symmetric matrices $R = \{B \in \mathbb{R} | B = B^T\}$ 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*.
- 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.
- For the Special Orthogonal Group, we have four different types of maps θ that can be used to define an involution.

CLASSIFYING SYMMETRIC SPACES

6. Types of Involutions

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

For SO(3,p) we have 4 types of involutions to consider:

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

- 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.
  - Class 2: Represented by

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

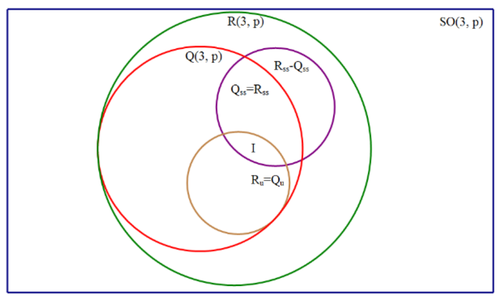
  where M_p is nonsquare in $\mathbb{F}_p$ and $a^2 + b^2 = M_p$, as described by Benim et al. This is an example of the below form when 2 is not a square:

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

  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 3 and 4 there are no involutions.
- For Type 2 Benim et al. claims no involutions exist, however we found matrices that satisfy this definition.

7. Unipotent and Semisimple

- We can further divide up the sets R and Q into *unipotent* and *semisimple* matrices.
- A *unipotent* 3x3 matrix only has an eigenvalue of 1 with algebraic multiplicity 3.
- A *semisimple* 3x3 matrix has a minimal polynomial that splits into distinct linear factors. Most commonly, the matrix has 3 distinct eigenvalues.



Theorem 2. *Every matrix in $SO(3,p)$ has eigenvalues $1, \lambda, \frac{1}{\lambda}$.*

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 3. *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. □

RESULTS

8. Results

The following conjectures and theorems are for Type 1 Involutions.

Remark 4. *The following tables indicate the patterns we have observed. Those that have been proven are included below.*

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.

Theorem 5. *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. For $p \equiv 1 \mod 4$, where -1 is a quadratic residue, take:

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

where c ranges from 1 to $p-1$ for $p-1$ cases,

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

where c ranges from 1 to $p-1$ for another $p-1$ cases, and the identity matrix for 1 case and a total count of $2(p-1)+1 = 2p-1$.

For $p \equiv 3 \mod 4$, where -1 is *not* a quadratic residue, take the identity matrix for a total count of 1. □

Theorem 6. *The number of unipotent matrices in the extended symmetric space $R(3,p)$ for involution A_2, where p is an odd prime, is:*

$$|R_u| = \begin{cases} 2p-1 & p \equiv 1,3 \mod 8 \\ 1 & p \equiv 5,7 \mod 8 \end{cases}$$

Proof. For $p \equiv 1,3 \mod 8$, where -2 is a quadratic residue, take:

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

where x ranges from 1 to $p-1$ for $p-1$ cases,

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

where x ranges from 1 to $p-1$ for another $p-1$ cases, and the identity matrix for 1 case and a total count of $2(p-1)+1 = 2p-1$.

For $p \equiv 5,7 \mod 8$, where -2 is *not* a quadratic residue, take the identity matrix for a total count of 1. □

Conjecture 7. *For all odd primes p, the number of unipotent matrices in the extended symmetric space $R(3,p)$ for any type 1 involution and the number of unipotent matrices in the general symmetric space $Q(3,p)$ for any type 1 involution are equal.*

$$R_u = Q_u$$

for all R and Q with given p.

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

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.
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 $R_u = Q_u$. □

The following theorems and corollaries are for the other types of Involutions.

Theorem 8. *There are no Type 3 involutions for 3x3 matrices.*

Proof. A Type 3 involution is $\theta(g) = AgA^{-1}$, where $A^2 \equiv -I$ and A is orthogonal. Thus, A has determinant ± 1 and A^2 has determinant $1 \mod p$. However,

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

has determinant -1. There is no odd p such that $1 \equiv -1 \mod p$, so there is no such A such that $A^2 \equiv -I$, and thus there are no Type 3 involutions for 3x3 matrices. □

Corollary 9. *There are no Type 3 involutions for any nxn matrices where n is odd.*

FUTURE WORK

- Continue classifying the symmetric groups for semisimple elements.
- Classify type 3 involutions
- Generalize from 3x3 to NxN matrices

REFERENCES

- Grove, L. C. (2002). Classical groups and geometric algebra.Providence, RI: American Mathematical Society.
- Hansen, M., Nordbye, A., & Ziliak, E. (n.d.). Classification ofGeneralized Symmetric Spaces of the Special OrthogonalGroup. College of Science Summer Research Program 2015.
- Benim, R. W., Dometrus C. E., Helminck, A.G., Wu L.(2014). Isomorphy Classes of Involutions ofSO(n,k,β)andSP(2n,k)wheren >2. Mathematics Subject Classification.