The H-Orbit Decomposition of the Special Orthogonal Group

Andrew Katson, Ellen Ziliak

September 15, 2024

1 Abstract

In this paper, we characterize the General and Extended Symmetric Spaces of the Special Orthogonal Group of 3×3 matrices over a finite field. Specifically, we use the fixed point group H to partition the sets of matrices that are unipotent, semisimple, or both in the General and Extended Symmeteric Spaces of SO(3, $\mathbb{F}_q$).

2 Introduction

The symmetric spaces were first studied nearly 100 years ago as a special class of homogeneous Riemannian manifolds by Cartan [7], with a focus on symmetric matrices over the real numbers. Symmetric matrices are those where $A^T = A$. They were later generalized to include other fields by Berger [3], and then the natural extension to symmetric k varieties were first introduced by Helmnick in [8]. In this setting, we can consider symmetric spaces over groups G_k. Symmetric spaces have found applications in differential geometry, general relativity, representation theory, and harmonic analysis.

The symmetric space is defined as the space $Q \cong G/H$ with H the fixed-point group of an automorphism θ of order n. Automorphisms of order 2 are called involutions and behave much like matrix transposition. By definition, this means that applying an involution or transposition twice yields the same output as the input, $\phi*(\phi(A)) = A$ for all involutions ϕ. In this project we will be focusing on the special orthogonal group of 3×3 matrices. The Special Orthogonal Group $SO(n, \mathbb{F}_p)$ is the group of orthogonal matrices of determinant one with dimension n over field $\mathbb{F}_p$. In [2], R Benim classified the involutions for $SO(n, \mathbb{F}_p)$ for odd characteristics. There are 4 types of involutions for the Special Orthogonal Group, depending on whether $A^2 = \pm I$, where I is the identity matrix, and whether A is from a field extension. In Corollary 2.4.3, Benim shows that $SO(3, \mathbb{F}_p)$ has only one type of involution, in which $A^2 = I$ and A is an inner involution. This fact implies that there are only two isomorphy classes, which are described in the following theorem.

Theorem 2.1 (Corollary 2.5.3 and Corollary 2.4.3[2]). *Let θ_i is an involution of $SO(3, \mathbb{F}_q)$ where $q = p^h$ and $p > 2$, then θ is isomorphic to Inn_{A_i} where $A_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ and $A_2 = \begin{pmatrix} 1 - \frac{2a^2}{M_q} & 0 & \frac{2ab}{M_q} \\ 0 & 1 & 0 \\ \frac{2ab}{M_q} & 0 & 1 - \frac{2b^2}{M_q} \end{pmatrix}$, where M_q is a non-trivial non-square element in $\mathbb{F}_q$ and $a^2 + b^2 = M_q$, for $a, b \in \mathbb{F}_q$. Equivalently, A_2 can also be written as $A_2 = \begin{bmatrix} u & 0 & v \\ 0 & 1 & 0 \\ v & 0 & -u \end{bmatrix}$, where $u = 1 - \frac{2a^2}{M_q}$ and $v = \frac{2ab}{M_q}$.*

Once the involutions are classified, there are two spaces of particular interest: the extended symmetric space $R = \{g \in G | \theta(G) = g^{-1}\}$ and the generalized symmetric space $Q = \{g\theta(g)^{-1} | g \in G\}$. In [1], Aliakeseyeu, Oliven, Thieme, and Ziliak went on to classify and characterize the generalized and extended symmetric spaces for $SO(3, \mathbb{F}_q)$. The next natural step is to consider orbit decomposition.

Theorem 2.2. *The sets R_i are extended symmetric spaces $R_1 = \left\{ G = \begin{bmatrix} a & b & c \\ b & e & f \\ -c & -f & i \end{bmatrix} \mid G \in SO(3, \mathbb{F}_p) \right\}$, $R_2 = \left\{ G = \begin{bmatrix} a & b & c \\ bu + hv & e & bv - hu \\ g & h & i \end{bmatrix} \mid G \in SO(3, \mathbb{F}_p), cu + iv = av - gu, u^2 + v^2 = 1 \right\}$ for θ_1 and θ_2 respectively.*

Orbit decomposition has been studied for both H-orbits and parabolic orbits for other groups previously. Reductive algebraic groups defined over algebraically closed fields and real numbers orbits of various subgroups have been well-studied (see Springer [12], Brion and Helminck [4, 5], Matsuki [10], Helminck and Wang [9], and Rossmann [11]). More recently Buell et al. [6] characterized the orbit decomposition for unipotent elements of the special linear group for 3×3 and 4×4 matrices.

The orbit decomposition of a set is the collection of disjoint subsets whose union is that set. Mathematically, if $A_1, A_2, ..., A_n$ are disjoint subsets of A and

$$A = \bigcup_{i=1}^{n} A_i,$$

then $A_1, A_2, ..., A_n$ are the orbits of A. Furthermore, we will find that the eigenvalues of a matrix impact the orbit decomposition. An eigenvalue is defined as a scalar λ such that $\lambda x = Ax$ for any nonzero vector x. A matrix is unipotent if all eigenvalues are 1, and semisimple if all of the eigenvalues are distinct. Another important concept is the trace of a matrix, defined as the sum of its diagonal entries.

In this paper, we investigate the orbit characteristics of the unipotent and semisimple subsets of the extended and generalized symmetric spaces of the special orthogonal group, over the modular

ring with a prime modulus p in dimension 3, so that $G = SO(3, \mathbb{F}_p)$.

3 Results

Lemma 3.1. *For any matrix A, it is true that* $det(A-\lambda I) = -\lambda^3+Trace(A)\lambda^2-(Cofactors of A)\lambda+det(A) = 0$*, where I is the identity matrix.*

Theorem 3.2. *A matrix* $G \in R_i$ *is unipotent if* $Trace(G) \equiv 3$ *(mod p) and semisimple if* $Trace(G) - 1 \not\equiv \pm 2$ *(mod p).*

Proof. To compute the eigenvalues of a matrix $G \in R_i$, we solve $det(G - \lambda I) = 0$ for λ. Using Lemma 3.1, the fact that $G \in SO(n, \mathbb{F}_q) \implies det(G) = 1$, and that $Trace(G) = a + e + i$,

$$-\lambda^3 + (a + e + i)\lambda^2 - (a + e + i)\lambda + 1 = 0.$$

If we substitute $\lambda = 1$, we see that $\lambda = 1$ is a valid solution to $det(G - \lambda I) = 0$. We may therefore divide $-\lambda^3 + (a + e + i)\lambda^2 - (a + e + i)\lambda + 1$ by $(\lambda - 1)$, which yields

$$-\lambda^2 + (a + e + i - 1)\lambda - 1 = 0.$$

Applying the quadratic equation, we find that

$$\lambda = \frac{-(a + e + i - 1) \pm \sqrt{(a + e + i - 1)^2 - 4}}{-2}.$$

The two remaining eigenvalues are the same when the determinant $(a+e+i-1)^2-4$ is zero, which implies $a + e + i = 3$ or $a + e + i = -1$. Thus, we have proved it is necessary that $Trace(G) = 3$ or $Trace(G) = -1$ for unipotency. For sufficiency, we see that

$$\lambda = \frac{-(a + e + i - 1) \pm \sqrt{(a + e + i - 1)^2 - 4}}{-2}.$$

only has one solution with $\lambda = 1$ when $a + e + i = 3$, removing the $Trace(G) = -1$ case. Thus, Trace(G)= 3 $\iff$ G is unipotent.

□

Lemma 3.3 (Cofactor Condition)**.** *Let* a_{ij} *be the ith row, jth column entry for any matrix* $A \in SO(3, \mathbb{F}_q)$*. Then,* $a_{ij} = (-1)^{i+j} det(M_{ij})$*, where* M_{ij} *is the minor matrix of A with the ith row and jth column removed.*

Proof. It is known that the adjoint matrix of A $adj(A)$, which is the transpose of the cofactor matrix of A, is given by $adj(A) = det(A)A^{-1}$. Since $det(A) = 1$, $adj(A) = A^{-1}$. In $SO(3, \mathbb{F}_q)$, $A^{-1} = A^T$ by orthogonality. Transposing both sides, we find that $adj(A)^T = CofactorMatrix(A) = (A^{-1})^T = A$. Thus, A equals the cofactor matrix of A and $a_{ij} = (-1)^{i+j} det(M_{ij})$. □

Lemma 3.4 (Length One Condition)**.** *Let* $A \in SO(3, \mathbb{F}_q)$*, with ij-th entry* a_{ij}*. Then* $\sum_i (a_{ij})^2 = \sum_j (a_{ij})^2 = 1$ *(mod p). In other words, the row and column vectors in A are length 1.*

Theorem 3.5. *Let R^u be the set of unipotent elements in the Extended Symmetric Space of $SO(3, \mathbb{F}_q)$ under θ_1. Then*

$$|R^u| = \begin{cases} 2q-1 & \text{if } -1 \text{ is a square in } \mathbb{F}_q \\ 1 & \text{if } -1 \text{ is not a square in } \mathbb{F}_q \end{cases}$$

Proof. We first simplify this matrix by solving for all the values in terms of f and c. Note that i=3-a-e because of the unipotency condition in Theorem 3.2. To solve for A, we sum the two length 1 conditions on the two rows that do not contain a:

$$b^2 + e^2 + f^2 + c^2 + f^2 + (3-a-e)^2 = 2$$

Then, we add a^2 to both sides and simplify via the first length 1 condition. Simplifying, we get

$$2e^2 + 2f^2 + 2ae - 6a - 6e = -8$$

The cofactor condition on a is

$$a = 3e - ae - e^2 + f^2$$

Adding 2a to both sides,

$$2e^2 + 2f^2 + 2ae - 6a - 6e + 2(3e - ae - e^2 + f^2) = -8 + 2a$$

$$a = 1 + \frac{f^2}{2}$$

Applying the same method on e, one will see that

$$e = 1 + \frac{c^2}{2}$$

Next, we remove b from the matrix. Applying the cofactor conditions on c and f,

$$c = -bf + ce, f = af - bc$$

$$c = \frac{b^2 c}{(a-1)(e-1)}$$

$\implies c = 0$ or $b^2 = (a-1)(e-1)$ For now, we focus on the latter case. Substituting the formulas for a and e,

$$b = \pm\frac{cf}{2}$$

Thus, our original matrix becomes $R_1 = \left\{ G = \begin{bmatrix} 1+\frac{f^2}{2} & \pm\frac{cf}{2} & c \\ \pm\frac{cf}{2} & 1+\frac{c^2}{2} & f \\ -c & -f & (1-\frac{c^2}{2}-\frac{f^2}{2}) \end{bmatrix} \mid G \in SO(3, \mathbb{F}_p) \right\}$.

Since $G \in SO(3, \mathbb{F}_q)$, the (3, 3) entry of $G * G^T - I_3 = 0$, which implies

$$\implies f = \pm\sqrt{-1} \cdot c.$$

Thus, we have 5 cases:

(1) c=0. This is just the identity matrix.

(2) $b = +\frac{cf}{2}, c = +\sqrt{-1}f$. Looking at $G * G^T - I_3 = 0$, we see that f must be zero. This implies the only valid matrix is I_3.

(3) $b = -\frac{cf}{2}, c = +\sqrt{-1}f$. All matricies take the form $R_1 = \begin{bmatrix} 1+\frac{f^2}{2} & -\frac{\sqrt{-1}*f^2}{2} & \sqrt{-1}f \\ -\frac{\sqrt{-1}f^2}{2} & 1-\frac{f^2}{2} & f \\ -\sqrt{-1}f & -f & 1 \end{bmatrix}$.

(4) $b = +\frac{cf}{2}, c = -\sqrt{-1}f$. Looking at $G * G^T - I_3 = 0$, we see that f must be zero. This implies the only valid matrix is I_3.

(5) $b = -\frac{cf}{2}, c = -\sqrt{-1}f$. All matricies take the form $R_1 = \begin{bmatrix} 1+\frac{f^2}{2} & \frac{\sqrt{-1}*f^2}{2} & -\sqrt{-1}f \\ \frac{\sqrt{-1}f^2}{2} & 1-\frac{f^2}{2} & f \\ \sqrt{-1}f & -f & 1 \end{bmatrix}$.

Note that when $\sqrt{-1}$ does not exist in $\mathbb{F}_p$, R^u consists of only the identity matrix because f=0 is the only matrix of cases 3 and 5. Moreover, there are q-1 unique elements in cases 3 and 5 when $\sqrt{-1}$ exists. When f=0 in cases 3 and 5, we get the identity matrix as in cases 1, 2, and 4. Thus, there are $2(q-1)+1 = 2q-1$ elements in R^u when -1 is square in $\mathbb{F}_q$. □

Corollary 3.6. *Let Q^u be the set of unipotent elements in the General Symmetric Space of $SO(3, \mathbb{F}_q)$. Then $|Q^u| = 1$ when $\sqrt{-1}$ does not exist in $\mathbb{F}_q$.*

Proof. This follows from $Q^u \subseteq R^u$. □

4 Conclusion

So far, we have determined the size of the set of unipotent elements in R_1 and determined a condition for unipotency in the Extended Symmetric Space under both involutions in $SO(3, \mathbb{F}_q)$. We have attained data in GAP for the orbits of the extended and general symmetric groups of $SO(3, \mathbb{F}_q)$ and have made several conjectures on their size, which remain to be proven or disproven.

References

[1] R. Aliakseyeu, N. Oliven, E. Thieme, and E. Ziliak (2023). The Combinatorics of the Generalized and Extended Symmetric Spaces of SO(3, $\mathbb{F}_p$.) To be published in Involve.

[2] R. Benim (2014). Isomorphy Classes of Involutions of SO(n, k, β) and SP(2n, k) where n > 2 Ph. D thesis, North Carolina State University.

[3] M. Berger. (1957). Les espaces symetriques noncompacts. Annales Scientifiques De L'E.N.S. *74: 85–177.*

[4] M. Brion and A. Helminck. (2000). On orbit closures of symmetric subgroups in flag varieties. Canad. J. Math, *52(2):265–292.*

[5] *A. Helminck. (2004). Combinatorics related to orbit closures of symmetric subgroups in flag varieties. In H. E. Alexander, E. Campbell, and D. L. Wehlau, editors* Invariant theory in all characteristics*, pages 71–90. American Mathematics Society.*

[6] *Buell, C., Helminck, A., Klima, V., Schaefer, J., Wright, C., and Ziliak, E. (2023). Fixed-point group conjugacy classes of unipotent elements in low-dimensional symmetric spaces of special linear groups over a finite field.* Journal of Algebra and Its Applications. *https://doi.org/10.1142/S0219498824501421*

[7] *E. Cartan. (1929). Groupes simples clos et ouvert et geometrie Riemannienne* J. Math. Pure Appl. *8: 1-33.*

[8] *A. G. Helminck. (1993). Symmetric k-varieties* Proc. Smpos. Pure Math. *56: 233–279.*

[9] *A. G. Helminck and S. P. Wang. (1993). On rationality properties of involutions of reductive groups.* Adv. Math, *99(no. 1):26–96.*

[10] *T. Matsuki. (1979). The orbits of affine symmetric spaces under the action of minimal parabolic subgroups.* J. Math. Soc, Japan, *31(no 2):331–357.*

[11] *W. Rossmann. (1979). The structure of semisimple symmetric spaces.* Canad. J. Math, *31:157–180.*

[12] *T. A. Springer. (1985). Some results on algebraic groups with involutions.* Algebraic groups and related topics (kyoto/nagoya, 1983)*, pages 525–543.*