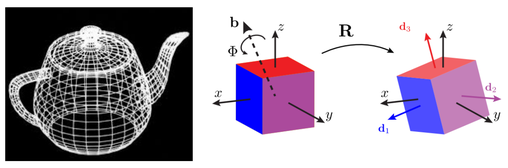
Classifying Symmetric Spaces for SO(3,q)

Jacob Sutter and Hanson Hao

Illinois Mathematics and Science Academy
Mentor: Dr. Ellen Ziliak, Benedictine University
Japan Super Science Fair, November 15, 2018

1. 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.



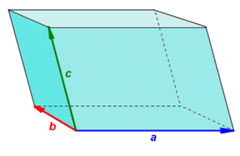
Quantum Physics The Special Orthogonal group is also related to the Special Unitary group, which have a basis formed by the three Pauli matrices. The Pauli matrices are used to represent spin of particles in quantum mechanics.

2. Matrix Operations

Definition 1. *The **Transpose Operator** 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. Modular Arithmetic

Clock Arithmetic On a clock, 5:00 = 17:00 = 29:00 = ..., we call these elements congruent $\mod 12$. But these times are placed together into a class, represented by 5:00.

Generalizing, we define congruence on the integers as follows:

Definition 3. ***Congruence***. *$a \equiv b \mod m$ if and only if m divides $b - a$.*

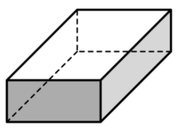
Because congruent elements behave the same algebraically, we put them into a class and pick a single representative in place of enumerating them all.

Definition 4. ***Congruence Class***. *For a given $a \in \mathbb{Z}$ we can define a congruence class, written $[a]$, such that $[a] = \{b \in \mathbb{Z} | a \equiv b \mod m\}$. We call a the representative of $[a]$.*

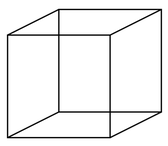
4. Special Orthogonal Group

Definition 5. *A matrix A is **special** if the determinant of A is 1.*

Definition 6. *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 7. *The **Special Orthogonal Group** $SO(n, q)$ is the group of $n \times n$ matrices in a finite field $\mathbb{F}_q$ that are both special and orthogonal. We can think of this as a set of rectangular prisms whose volumes are all congruent to $1 \mod q$.*



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

5. How to Generate $SO(3, q)$

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

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

The Good Way:

1. First find all vectors **v** with $|\mathbf{v}|^2 \equiv 1 \mod q$. This step has complexity $O(q^3)$.
2. Use list of vectors to find all pairs of orthogonal vectors. Complexity $O((q^2)^2) = O(q^4)$.
3. Find a third vector which is pairwise orthogonal to the first two. Complexity $O(q^5)$
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 $O(q^5)$
- 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 $O(q^4)$.
- Instead of being limited to $q = 13$, we have gone as high as $q = 101$

6. Involutions and Symmetric Spaces

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

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

- We can say 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.
- Notice that $(B^T)^T = B$
- Our goal is to define a general version of this symmetric space.
- Lets define another function $\theta(X) = AXA^{-1}$ that maps a matrix to another matrix. We observe that the same property holds, $\theta(\theta(X)) = X$ for all X.
- θ is called an involution, and A the involution matrix.
- In this more general setting the symmetric space $R = \{X \in S(3, q) | \theta(X)^{-1} = X\}$
- Instead of a visual symmetry defined by $B^T = B, \theta(X) = X^{-1}$ is a sort of algebraic symmetry.

Example Elements in $R(3,5)$: $\left\{ \begin{bmatrix} 0 & 0 & 4 \\ 0 & 4 & 0 \\ 4 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 4 \\ 4 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 3 \\ 3 & 4 & 4 \\ 1 & 2 & 1 \end{bmatrix} \right\}$

- One way to create a symmetric matrix in $\mathbb{R}$ is to take any matrix C and multiply by it's transpose. We define a second symmetric space $Q = \{CC^T | C \in \mathbb{R}\}$
- It is important to note that $Q \subset R$
- In our more general notion of symmetry the set $Q = \{X\theta(X)^{-1} | X \in SO(3, q)\}$

Example Elements in $Q(3,5)$: $\left\{ \begin{bmatrix} 4 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 4 \\ 4 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 4 & 4 & 3 \\ 1 & 2 & 1 \\ 3 & 4 & 4 \end{bmatrix} \right\}$

- For the Special Orthogonal Group, we have four different types of maps θ that can be used to define an involution.

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

  For SO(3,q) 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:
  - Class 1: Represented by $(1) = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$
  - Class 2: Represented by $(2) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$
- For Type 3 and 4 there are no involutions.
- For Type 2 we only have preliminary data at this point and have not yet confirmed a count.

7. Results

Theorem 2. *The number of matrices in $O(3, q)$, where $q = p^n$ and p is an odd prime, is twice the number of matrices in $SO(3, q)$:*

$$|O(3, q)| = 2 * |SO(3, q)|.$$

Proof. By previous results, an orthogonal matrix A in a finite field $\mathbb{F}_q$ has determinant ± 1. Consider matrix M which has determinant 1. We know that $-M$ has determinant -1, but $(-M)(-M)^T = MM^T = I$, so $-M$ is an orthogonal matrix. Thus there are the same number of matrices in $O(3, p)$ with determinant 1 as there are with determinant -1. As the matrices with determinant 1 make up $SO(3, p)$, we have that

$$|O(3, p)| = 2 * |SO(3, p)|.$$

□

Conjecture 3. *The number of 3-vectors of length 1 mod p, where p is an odd prime, is:*

$$V(p) = \begin{cases} p^2 + p & p \equiv 1 \mod 4 \\ p^2 - p & p \equiv 3 \mod 4 \end{cases}$$

Conjecture 4. *The number of matrices in $SO(3, p)$, where p is an odd prime, is:*

$$|SO(3, p)| = |V(p)| * M = p^3 - p.$$

where

$$M = \begin{cases} p - 1 & p \equiv 1 \mod 4 \\ p + 1 & p \equiv 3 \mod 4 \end{cases}$$

Theorem 5. *Given the matrix*

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

and fixed a, b, c, d, e, and f such that the vectors (a, b, c) and (d, e, f) each have length 1 and are orthogonal to each other mod p, there is exactly 1 choice for the vector (g, h, i) such that M is both special and orthogonal mod p.

The following conjectures and theorems are for Type 1 Involutions.

Remark 6. *The following tables indicate the patterns we have observed. Those that have been proven are included below.*

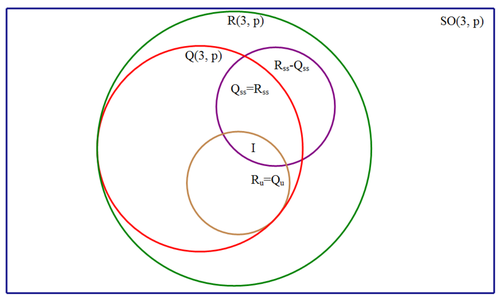
*In summary, for type 1 involutions in the same class as **(1)**:*

	$\lvert R\rvert$	$\lvert Q\rvert$	$\lvert R_u\rvert$	$\lvert Q_u\rvert$	$\lvert R_{ss}\rvert$	$\lvert Q_{ss}\rvert$
$p \equiv 1, 3 \mod 8$	p^2+1	T_p	$2p-1$	$2p-1$	$(p-1)^2+2$	$T_{p-2}+1$
$p \equiv 5, 7 \mod 8$	p^2+1	T_{p-1}	1	1	p^2+1	T_{p-1}

*For type 1 involutions in the same class as **(2)**:*

	$\lvert R\rvert$	$\lvert Q\rvert$	$\lvert R_u\rvert$	$\lvert Q_u\rvert$	$\lvert R_{ss}\rvert$	$\lvert Q_{ss}\rvert$
$p \equiv 1 \mod 4$	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}

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



Theorem 7. *The number of unipotent matrices in the extended symmetric space $R(3, p)$ for involution **(1)**, 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. □

Theorem 8. *The number of unipotent matrices in the extended symmetric space $R(3, p)$ for involution **(2)**, 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. □

Conjecture 9. *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.

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

Theorem 10. *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 11. *There are no Type 3 involutions for any nxn matrices where n is odd.*

Theorem 12. *For all field extensions $\mathbb{F}_q[\sqrt{\alpha}] \cong \mathbb{F}_q[\sqrt{\beta}]$ where α and β are non-square in the finite field $\mathbb{F}_q$, where q is a power of a prime. Therefore $SO(3, q)[\sqrt{\alpha}] \cong SO(3, q)[\sqrt{\beta}]$.*

Proof. Since α is non-square, $\frac{1}{\alpha}$ is also non-square. The product of two non-square values in a finite field must be square (because their Legendre symbols, -1 and -1, multiply to 1), so $\frac{\beta}{\alpha}$ is square. Then let $n \equiv \frac{\sqrt{\beta}}{\sqrt{\alpha}}$ so that $n\sqrt{\alpha} \equiv \sqrt{\beta}$. We can then create a correspondence between $\mathbb{F}_q[\sqrt{\alpha}]$ and $\mathbb{F}_q[\sqrt{\beta}]$ by substituting $n\sqrt{\alpha}$ for $\sqrt{\beta}$ in the latter group. This correspondence is one-to-one as $a + b\sqrt{\beta}$ and $c + d\sqrt{\beta}$ cannot map to the same value unless $a \equiv c$ and $bn \equiv dn \Rightarrow b \equiv d$ (since we are working in a finite field and n is nonzero). Thus, we have $\mathbb{F}_q[\sqrt{\alpha}] \cong \mathbb{F}_q[\sqrt{\beta}]$. Since the two fields are congruent we can conclude that the Special Orthogonal Group over those fields must also be congruent, applying the same map. Thus $SO(3, q)[\sqrt{\alpha}] \cong SO(3, q)[\sqrt{\beta}]$ □

Corollary 13. *Similarly, $R(3, q)[\sqrt{\alpha}] \cong R(3, q)[\sqrt{\beta}]$ and $Q(3, q)[\sqrt{\alpha}] \cong Q(3, q)[\sqrt{\beta}]$.*

8. Future Work

- Prove our remaining conjectures for the sizes of R, R^{ss}, R_u, Q, Q^{ss} and Q_u
- Look at previous classifications of sparse matrices in R and Q
- Use orbits to extend to all of R and Q
- Generalize to higher dimensions.

9. References

- 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.
- Benium, R. W., Dometrus C. E., Helminck, A.G., Wu L. (2014). Isomorphy Classes of Involutions of SO(n, k,) and SP(2n, k) where n ¿ 2. Mathematics Subject Classification.
- [Quaternion Rotation Matrix]. (2014, September 8). Retrieved October 24, 2018, from https://math.stackexchange.com/questions/923293 /rotation-matrix-to-quaternionproper-orientation?rq=1
- [Labeled Parallelepiped]. (n.d.). Retrieved October 24, 2018, from http://www.technologyuk.net /mathematics/geometry/parallelepiped.shtml
- [24 hour analog clock]. (n.d.). Retrieved October 24, 2018, from https://www.abcoffice.com/images/1224-analog-clock.jpg
- [Rectangular Prism Grayscale Clipart]. (n.d.). Retrieved October 24, 2018, from https://www.abcteach.com/documents/clip-art-3d-solids-rectangular-prism-grayscale-i-abcteachcom-19411
- [Symmetrical Butterfly]. (n.d.). Retrieved October 24, 2018, from https://www.ck12.org/book/CK-12-Middle-School-Math-Concepts-Grade-6/section/9.20/