THE DEGREE OF SO(N)

Madeline Brandt
University of Washington, 2018

1. Introduction

This research was done with collaborators Juliette Bruce, Taylor Brysiewicz, Robert Krone, and Elina Robeva. This was inspired by a Fortnight of Apprenticeship orchestrated by Bernd Sturmfels, which had fitness exercises. Determining the degree of SO(n) was one of the exercises.

Definition 1. The group SO(n) is defined as

$$\mathrm{SO}(n) := \mathrm{SO}(n, \mathbb{C}) = \left\{ M \in \mathrm{Mat}_{n,n}(\mathbb{C}) \mid \det M = 1, \quad M^t M = \mathrm{Id} \right\}.$$

Since these conditions are polynomials in the entries of the matrix M, we can view SO(n) as a complex variety. Our main result was to find the *degree* of the projective closure of this complex variety.

Definition 2. If X is an embedded affine variety, then its *projective closure* $\overline{X}$ is the smallest projective variety containing X.

Definition 3. The degree of a complex variety X is the maximum number of intersection points of $\overline{X}$, the projective closure of X, with a linear space L of complementary dimension: $\dim L + \dim X = n^2$. This maximum will be achieved as long as the L is chosen generically.

Why do we care about the degree of SO(n)? The degree is a fundamental piece of data about a variety that one would want to know about it, just like its dimension. Also, it provides the degree of low-rank semidefinite programming and is used to find the number of critical points for certain optimization problems.

Using Gröbner bases, one can compute the degree for small values, but this fails quickly, because the number of variables grows quadratically with n. The Gröbner basis for SO(5) has 344 elements, coming from 26 equations in 25 variables. Further, numerical techniques using monodromy have been developed for computing witness sets for the variety, and these give two more values for the degree of SO(n).

n	Symbolic	Numerical	Formula
2	2	2	2
3	8	8	8
4	40	40	40
5	384	384	384
6	-	4768	4768
7	-	111616	111616
8	-	-	3433600
9	-	-	196968448

Theorem 1. *The degree of* $\mathrm{SO}(n)$ *is given by:*

$$\deg \mathrm{SO}(n) = 2^{n-1} \det \left(\binom{2n-2i-2j}{n-2i} \right)_{1 \le i,j \le \lfloor \frac{n}{2} \rfloor}.$$

This talk will include a proof sketch, a discussion of lattice paths, and application, and some numerical techniques.

2. Proof of Main Result

Our proof of this theorem uses a formula of Kazarnovskij [Kaz87] for the degree of the image of a representation of a connected, reductive, linear algebraic group over an algebraically closed field.

I will now ignore some language from Lie Theory that we used to prove this result. If you know what these things are, that is great; otherwise, the important thing to know is that each of these pieces of data is easily computable for the group $\mathrm{SO}(n)$, and I will immediately say what it is. But this is the main theorem we used to prove our result.

Theorem 2 (Kazarnovskij's Theorem (Prop 4.7.18 [DK02]))**.** *Let G be a connected reductive group of dimension m and rank r over an algebraically closed field. If $\rho : G \to \mathrm{GL}(V)$ is a representation with finite kernel then,*

$$\deg \overline{\rho\,(G)} = \frac{m!}{|W(G)|(e_1! e_2! \cdots e_r!)^2 |\ker(\rho)|} \int_{C_V} (\check{\alpha}_1 \check{\alpha}_2 \cdots \check{\alpha}_l)^2 dv.$$

where $W(G)$ is the Weyl group, e_i are Coxeter exponents, C_V is the convex hull of the weights, and $\check{\alpha}_i$ are the coroots.

The first step is to plug in the data about $\mathrm{SO}(n)$ in to this result, with the standard representation.

Group	Dimension	Rank	Positive Roots	Weights	$\lvert W(G)\rvert$	Coxeter Exponents
SO$(2r)$	$\binom{2r}{2}$	r	$\{e_i \pm e_j\}_{i<j}$	$\{\pm e_i\}$	$r!2^{r-1}$	$1, 3, \ldots, 2r-3, r-1$
SO$(2r+1)$	$\binom{2r+1}{2}$	r	$\{e_i \pm e_j\}_{i<j} \cup \{e_i\}$	$\{\pm e_i\}$	$r!2^r$	$1, 3, 5, \ldots, 2r-1$

I will do this only for the odd case, but the even case follows similarly. Miraculously, they collapse in to one formula.

$$\deg \mathrm{SO}(2r+1) = \frac{\binom{2r+1}{2}!}{r!2^r \prod_{k=1}^{r}(2k-1)!^2} \underbrace{\int_{C_V} \left(\prod_{1 \le i < j \le r} (x_i^2 - x_j^2)^2 \prod_{i=1}^{r} (2x_i)^2 \right) dv}_{I_{odd}}$$

Now we must evaluate the integral, I_{odd}. Here are the main steps:

1. Turn the integrand into monomials. We use the well-known expression for the determinant of the Vandermonde matrix ($m_{i,j} = x_i^j$):

   $$\prod_{1 \le i < j \le r} (y_j - y_i) = \sum_{\sigma \in S_r} \mathrm{sgn}(\sigma) \prod_{\mathrm{i}=1}^{\mathrm{r}} \mathrm{y}_{\mathrm{i}}^{\sigma(\mathrm{i})-1}.$$

   Then we substitute $y_i = x_i^2$ and square the entire expression.

2. Since the integrands are even in all variables, we can simplify the region over which we integrate. Specifically, the integrals over C_V are 2^r times the same integrals over Δ_r, the standard r-simplex.

3. Apply the following proposition.

   Proposition 1 (Lemma 4.23 [Mil14]). *Let $\Delta_r \subset \mathbb{R}^r$ be the standard r-simplex. If $\mathbf{a} = (a_1, \ldots, a_r) \in \mathbb{Z}^r_{>0}$ then*

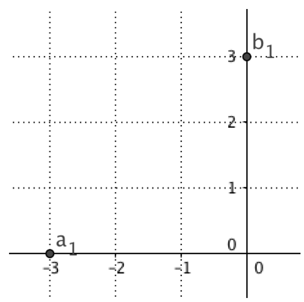
   $$\int_{\Delta_r} x^{\mathbf{a}} d\mathbf{x} = \frac{1}{(\sum a_i + r)!} \prod_{i=1}^{r} a_i!.$$

3. Non-Intersecting Lattice Paths

The formula given in the main theorem can be interpreted as a count of non-intersecting lattice paths via the Gessel-Viennot Lemma [GV85].

Lemma 1 (Gessel-Viennot (Weak Version))**.** *Let $A = \{a_1, \ldots, a_r\}, B = \{b_1, \ldots, b_r\} \subseteq \mathbb{Z}^2$. Let $M_{i,j}$ be the number of North-East lattice paths from a_i to b_j. If the only way that a system of North-East lattice paths from $A \to B$ do not cross each other is by sending $a_i \mapsto b_i$ then the determinant of M is given by the number of such non-intersecting lattice paths.*

Example Here is an example of a point configuration, and we will describe a north-east lattice path and how to count all such paths.



Since the total number of steps taken is 6 and 3 of these must be eastward, we have that the total number of paths is $\binom{6}{3}$. If we add two more points at $(-1, 0)$ and $(1, 0)$, the matrix M in this case is:

$$\begin{bmatrix} \binom{6}{3} & \binom{4}{1} \\ \binom{4}{3} & \binom{2}{1}. \end{bmatrix}$$

Its determinant is 24, which is $\deg(\mathrm{SO}(5))/2^4$.

The determinant appearing in the degree of $\mathrm{SO}(n)$ has a natural interpretation via Gessel-Viennot because binomial coefficients count lattice paths.

Theorem 3.

$$\deg \mathrm{SO}(n) = 2^{n-1}(\#\{\textit{Non-Intersecting Lattice Paths from } A \textit{ to } B\})$$

where the positions of A and B are given by $a_i = (2i - n, 0), b_j = (0, n - 2j)$ where $1 \leq i, j \leq \lfloor \frac{n}{2} \rfloor$.

This suggests a relationship between these non-intersecting lattice paths and the degree of $\mathrm{SO}(n)$, but we currently do not have any meaningful understanding of the nature of this relationship. Such an interpretation could be interesting, and so we pose the following question: Does Theorem 3 have a deeper combinatorial interpretation?

4. Semidefinite Programming

This problem originally arose as an effort to describe the geometry of low rank semidefinite programming. Here, we discuss some background on semidefinite programming in order to explain how knowing the degree of $\mathrm{SO}(n)$ is useful in this context.

We now give the standard formulation of semidefinite programming. Let $C, A_1, \ldots, A_m$ be matrices in $\mathbb{Q}^{n\times n}$. Let $b_1, \ldots, b_m \in \mathbb{Q}^m$. Let $\bullet$ denote the inner product of two matrices: $U \bullet V = \mathrm{trace}(UV)$. Then, we wish to find the positive semidefinite $X \in \mathbb{R}^{n\times n}$ that $C \bullet X$ is minimized, subject to the constraint that $A_i \bullet X = b_i$.

This is solvable in polynomial time in n, the size of the matrix, and m, the number of constraints. However, for many problems n is very large, so this quickly becomes computationally prohibitive. Typically, the rank r of the optimal solution is much smaller than n. Therefore, we can solve more rapidly by replacing X by the low-rank positive semidefinite matrix RR^T, where $R \in \mathbb{R}^{n\times r}$.

This gives new difficulties– the objective function and constraints are no longer linear, but quadratic. Also, the feasible set is non-convex. Burer and Monteiro give a fast algorithm to solve this, and despite there being multiple local minima, the algorithm quickly finds the global minimum.

Theorem 4. *The number of critical points of the low-rank semidefinite programming algorithm is*

$$2\,deg\,\mathrm{SO}(r)\cdot\delta,$$

where δ is a known constant which depends on m, n, and r, called the algebraic degree of semidefinite programming. This is the number of critical points of the original semidefinite programing algorithm.

This motivates the question of trying to find the number of real critical points, or finding how many real points a linear cut on $\mathrm{SO}(n)$ has. We study this problem numerically in the next part of the talk.

5. Computational Methods: Monodromy

We tried several computational methods, but the most efficient and effective proved to be monodromy techniques. The idea is as follows:

1. Choose a random linear space L of complimentary dimension $n^2 - \binom{n}{2}$ containing a favorite matrix I.

2. I is one point (out of $\deg(\mathrm{SO}(n))$ many points) lying inside $L \cap \mathrm{SO}(n)$. Now, move L along a path to a new linear space L'. While this happens, track where

I moves inside of L. Numerical algebraic geometry can do this easily (each step is Newton's method which is linear algebra).

3. Move L' back to L, along a different path, and still keep track of where I is moving. Now, we most likely have an entirely different point $I' \in L \cap \mathrm{SO}(n)$.
4. Repeat this process, hoping to populate all of $L \cap \mathrm{SO}(n)$. (The monodromy group is transitive because the variety is connected and irreducible, meaning there exists a path we could track between any two points)
5. There is a stopping criterion called the trace test. You move the linear cut in a linear fashion, and track the average of the solutions. This should change linearly as well. This turns out to be if and only if.

For SO(7), this terminated in about 12 hours. (Thanks to Anton Leykin for the software, which will probably be released in the next Macaulay2 package.)

We used this method to study real points in linear slices of $\mathrm{SO}(n)$. We choose coefficients needed to produce linear cuts using the *random* function in *Macaulay2*. We determined how many solutions in our linear cuts were real by checking whether each solution was within a 0.001 numerical tolerance of a real point coordinate-wise. One can also certify the results using α-certify. On SO(3), the highest number of real points found was 8, the full degree, On SO(4), it was 30 (out of 40, after 1,000,000 trials), and for SO(5) it was 76 (out of 384, after about half a million trials).

References

[DHJ+16] Timothy Duff, Cvetelina Hill, Anders Jensen, Kisun Lee, Anton Leykin, and Jeff Sommars, *Solving polynomial systems via homotopy continuation and monodromy*, arXiv preprint arXiv:1609.08722 (2016).

[DK02] Harm Derksen and Gregor Kemper, *Computational invariant theory*, Encyclopaedia of Mathematical Sciences, vol. 130, Springer-Verlag, Berlin Heidelberg, 2002.

[GV85] Ira Gessel and Gérard Viennot, *Binomial determinants, paths, and hook length formulae*, Advances in mathematics **58** (1985), no. 3, 300–321.

[HS] Jonathan D. Hauenstein and Frank Sottile, *alphaCertified: Software for certifying numerical solutions to polynomial equations*, Available at http://www.math.tamu.edu/ sottile/research/stories/alphaCertified.

[Kaz87] B Ya Kazarnovskii, *Newton polyhedra and the bezout formula for matrix-valued functions of finite-dimensional representations*, Functional Analysis and its applications **21** (1987), no. 4, 319–321.

[Mil14] James S. Milne, *Algebraic number theory (v3.06)*, 2014, Available at www.jmilne.org/math/, p. 164.