Introduction and Overview

My areas of research are computational algebra and algebraic geometry, and I study the existence of sums-of-squares formulas over arbitrary fields.

A sums-of-squares formula can be thought of as a product or composition law $F^r \times F^s \to F^n$ over a field F such that the norm of the product is the product of the norms. More precisely, a sums-of-squares formula of type $[r, s, n]$ over a field F (of characteristic not 2) is an identity of the form

$$(x_1^2 + \cdots + x_r^2)(y_1^2 + \cdots + y_s^2) = z_1^2 + \cdots + z_n^2,$$

where each z_i is a bilinear expression in the x's and y's over F. For example, multiplication of complex numbers comes from a sums-of-squares formula of type $[2, 2, 2]$ over $\mathbb{R}$, with the bilinear expressions for the z_i given by

$$z_1 = x_1y_1 - x_2y_2, \qquad z_2 = x_1y_2 + x_2y_1.$$

Similarly, there are formulas corresponding to multiplication of quaternions and octonions.

My research is primarily focused on two questions:

1. Does existence of a sum-of-squares formula of type $[r, s, n]$ depend on the field F?
2. How can we efficiently find formulas over finite fields and over the integers algorithmically?

In my work, I have found a new way to study these formulas using algebraic geometry. I have defined the scheme of sums-of-squares formulas, and I have used this scheme to show that existence of sums-of-squares formulas over algebraically closed fields is independent of the characteristic p, for large enough p. I have made the bound on p explicit and proven that the existence of a sums-of-squares formula of fixed type over an algebraically closed field is theoretically (though not practically) computable.

By defining an algebraic group action on the scheme of sums-of-squares formulas, I have started to study the structure of this scheme. I have used the group action to improve efficiency in computer searches for sums-of-squares formulas over finite fields. I have incorporated undergraduates into my research by having them investigate the orbits of this group action on sums-of-squares formulas over the integers. Brute force algorithms to find moderately large sums-of-squares formulas over the integers are completely infeasible, and efficient algorithms to produce such formulas have been elusive. I have recently developed constraint propagation algorithms for detecting sums-of-squares formulas over $\mathbb{Z}$ and over $\mathbb{Z}/m\mathbb{Z}$. I am currently working on improving and refining these algorithms using combinatorial observations about sums-of-squares formulas, along with some students.

My future plans are to study sums-of-squares formulas over the p-adics, to generalize some previous results on sums-of-squares formulas over the integers to finite fields, and to study the stucture of the scheme of sums-of-squares formulas through its algebraic group action.

My work with interactive textbooks also provides a future direction for research. I plan to use the data generated by these textbooks to study how students use texts, and how they can be made more effective.

History and Motivation

Sums-of-squares formulas were originally studied in the context of real normed division algebras: existence of a sums-of-squares formula of type $[n, n, n]$ over $\mathbb{R}$ is equivalent to the existence of a real normed division algebra of dimension n. By studying sums-of-squares formulas, Hurwitz was able to settle the question of existence of real normed division algebras in [8], showing the only ones are the real numbers, complex numbers, quaternions, and octonions. Hurtwitz's theorem has been applied to the study of vector fields on spheres and homotopy groups of classical groups, as well as to quantum mechanics through the classification of simple Jordan algebras. In his paper, Hurwitz posed the general question:

> For what r, s, n does a sums-of-squares formula of type $[r, s, n]$ exist over a field F?

Sums-of-squares formulas continue to be of interest for a variety of reasons. They provide immersions of projective space into Euclidean space, they induce Hopf maps, and they yield a system of independent sections of a direct sum of the canonical line bundle over projective space. The immersion problem has long been a central question in differential topology, and Hopf maps are interesting in the context of algebraic topology, as they are maps between spheres which are not null-homotopic. Furthermore, over arbitrary fields, sums-of-squares formulas provide examples of compositions of quadratic forms. The question of existence of sums-of-squares formulas over arbitrary fields is particularly interesting, because formulas over finite fields can be found using computational methods. This then can yield formulas in the classical characteristic zero setting.

Since Hurwitz's paper, sum-of-squares formulas have been studied using linear algebra, algebraic topology, and combinatorics. Most of the results have been limited to the characteristic zero setting, focusing on formulas over the integers and the real and complex numbers. For some special cases of r, s, n, Adem [3] [4] and Yuzvinsky [9] have settled the question of existence of formulas over any field. More recently, Dugger and Isaksen have extended older results using algebraic topology to the case of an arbitrary field [6] [5] [7]. However, apart from these very special cases, little is known about sums-of-squares formulas over arbitrary fields.

Results

In the past, sums-of-squares formulas have been studied as a system of vectors or matrices, or through the maps they induced. I observed that by viewing the coefficients as a solution to a system of polynomials, we can consider the scheme X^F_{rsn} of sums-of-squares formulas of type $[r, s, n]$ over F. This geometric perspective is a new approach, and opens up many new algebro-geometric tools for studying sums-of-squares formulas.

I first showed that existence over an algebraically closed field depends only on the characteristic, so the only fields we need to consider are $\bar{\mathbb{Q}}$ and $\bar{\mathbb{F}}_p$ for $p \neq 2$ prime:

Theorem. *([1], Theorem 3.1) A sums-of-squares formula of type $[r, s, n]$ exists over an algebraically closed field of characteristic 0 if and only if one exists over $\bar{\mathbb{Q}}$.*

A sums-of-squares formula of type $[r, s, n]$ exists over an algebraically closed field of characteristic p if and only if one exists over $\bar{\mathbb{F}}_p$.

Over algebraically closed fields, one can hypothetically determine whether or not the scheme of sums-of-squares formulas is empty by computing a Gröbner basis. Although this is not practical in nontrivial cases, careful analysis of coefficients which appear in Buchberger's algorithm proves the following result.

Theorem. *([1], Theorem 5.10) If a formula of type $[r, s, n]$ exists over any field of characteristic 0, then a formula of that type exists over every algebraically closed field of "large enough" characteristic. If there is no sums-of-squares formula of type $[r, s, n]$ over some algebraically closed field of characteristic 0, then there is no sums-of-squares formula of type $[r, s, n]$ over $\bar{\mathbb{F}}_p$ for "large enough" p.*

In both cases, I have produced an explicit bound for the characteristic of the field.

As a corollary, I showed that if a sums-of-squares formula exists over some field, then a formula of that type necessarily exists over some finite field. This means that all formulas can potentially be found using computer searches involving finite fields. In particular,

Theorem. *([1], Theorem 5.11) The existence of a sums-of-squares formula of type $[r, s, n]$ over an algebraically closed field is computable.*

Studying sums-of-squares formulas from this geometric perspective, I found a group action of a product of orthogonal groups on the scheme of sums-of-squares formulas, X^F_{rsn}. By showing that the action of each of these orthogonal groups is free, I established a lower bound for the dimension of X^F_{rsn} (when it is nonempty), in particular proving the following theorem:

Theorem. *([2], Theorem 6.6.2) If X^F_{rsn} is nonempty, then* $\dim X^F_{rsn} > 0$.

This result means that sums-of-squares could be detected by computing dimension and suggests that they may be detectable using cohomology.

The group action can be used to study how different sums-of-squares formulas relate to each other by studying the orbits. This observation may enable us to lift formulas from characteristic p to characteristic zero.

Current Work

I have recently developed constraint propagation algorithms to produce sums-of-squares formulas over the integers and over $\mathbb{Z}/m\mathbb{Z}$. Over the integers, this algorithm works by searching for consistently signed intercalate matrices:

Definition. A *consistently signed intercalate matrix* of type (r, s, n) is an $r \times s$ matrix M with entries from the set $\{\pm 1, \pm 2, ..., \pm n\}$, such that

1. The entries along each row and column are distinct.
2. If $M_{ij} = \pm M_{i'j'}$, then $M_{i'j} = \pm M_{ij'}$, and the 2×2 submatrix consisting of these entries has an odd number of minus signs.

Consistently signed intercalate matrices correspond precisely to sums-of-squares formulas over the integers. For example, we give the 2×2 consistently signed intercalate matrix corresponding to the sums-of-squares formula giving multiplication of complex numbers.

$$\begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix} \qquad \longleftrightarrow \qquad \begin{aligned} z_1 &= x_1y_1 - x_2y_2 \\ z_2 &= x_1y_2 + x_2y_1 \end{aligned}$$

My algorithm works by tracking and eliminating possible entries in the matrix using the conditions on the rows, columns, and squares of a consistently signed intercalate matrix. The search space is further restricted using combinatorial arguments, and by eliminating matrices which are equivalent through the group action on the set of sums-of-squares formulas.

As a rough measure of the efficiency of this algorithm, a naive brute force search for a formula of type $[10, 10, 16]$ over the integers would involve checking $(2 \cdot 16)^{10 \cdot 10} \approx 3.27 \times 10^{150}$ matrices. Even if we neglect the time to produce the matrices and each check took only a millisecond, such a search would take approximately 1.037×10^{140} years. This is much longer than the age of the universe, which is estimated to be 13.8×10^9 years. In contrast, my algorithm produces a sums-of-squares formula of type $[10, 10, 16]$ in less than 2 seconds, on a standard laptop.[1]

In order to write a similar algorithm for sums-of-squares formulas over $\mathbb{Z}/m\mathbb{Z}$, I've found a way to encode these sums-of-squares formulas as matrices of integers, roughly analogous to consistently signed intercalate matrices. Although the essential idea of this algorithm is the same as the algorithm over the integers, sums-of-squares formulas over $\mathbb{Z}/m\mathbb{Z}$ present additional complications, requiring significant adjustments.

I'm currently working on improving and refining these algorithms, with the goal of determining the existence of sums-of-squares formulas of type $[r, s, n]$ in unknown cases.

[1] Averaged 1.729 seconds per trial over 100 trials, on MacBook Pro with 3.1 GHz Intel Core i7 processor and 16 GB 1867 MHz DDR3.

Future Work

In the longer term, I plan to study sums-of-squares formulas over the p-adics, to generalize some previous results on sums-of-squares formulas over the integers to finite fields, and to study the stucture of the scheme of sums-of-squares formulas through its algebraic group action.

For sums-of-squares formulas over the p-adics, I've recently started working with Sudesh Kalyanswamy, a number theorist at Yale. We've begun to study how sums-of-squares formulas over the p-adic integers and over $\mathbb{Z}/p^t\mathbb{Z}$ relate to each other, and have made some surprising observations. This work is still in a very early stage.

There exists a large body of work on sums-of-squares formulas over the integers, primarily using consistently signed intercalate matrices. I aim to generalize many of these results to sums-of-squares formulas over $\mathbb{Z}/m\mathbb{Z}$, using my new representation of these formulas as matrices of integers.

I also plan to continue to study the structure of the scheme of sums-of-squares formulas. Currently, using the algebraic group action seems like the most promising method. Some of my undergraduate research students have begun to study this group action over the integers; their work is discussed below.

Supervising Undergraduate Research

I have incorporated some advanced high school students into my research on sums-of-squares formulas. These students have completed courses through multivariable calculus and linear algebra, but have no previous background in abstract algebra. My students have been able to approach sums-of-squares formulas through their connection to consistently signed intercalate matrices.

This equivalence is easily accessible to students, and students comfortable with linear algebra can understand the action of orthogonal groups on these matrices. After about three weeks of meeting, my students were already computing orbits (without knowing any of the terminology about group actions). They were thus able to start doing original research almost immediately, and we were able to fill in the knowledge of group actions later. My students have made some exciting preliminary discoveries about the group action on sums-of-squares formulas; they have determined some invariants and are beginning to understand the structure of the orbits.

In a separate project, I recently recruited an additional student, to assist with the combinatorial arguments that I'm using to refine my constraint propagation algorithms.

I plan to continue to work with students to study sums-of-squares formulas over the integers, and eventually over $\mathbb{Z}/m\mathbb{Z}$. Although the problem is simple to understand, it's broad enough to provide work for many different projects.

In addition to original research on sums-of-squares formulas, I have supervised several senior theses and reading projects. The topics have included elliptic curves, options pricing, linear cryptanalysis, secret sharing in video games, applications of math to engineering, knot theory, and algebraic topology.

Interactive Textbooks and Data Mining

My work with interactive textbooks also provides a future direction for research. When students use these textbooks, a huge amount of data on student interactions is recorded, but it has yet to be used. I would like to partner with someone with more experience working with large data sets, and use this data to reach conclusions about how students use texts, how effective they are, and how they could be made more effective.

This could also provide another place to involve students in my research, particularly students who are interested in careers in data science.

References

[1] M. Lynn. *Sums-of-Squares Formulas over Algebraically Closed Fields.* Journal of Algebra, 497 (2018), 393-410

[2] M. Lynn. *Sum-of-Squares Formulas over Arbitrary Fields.* PhD Thesis (2016). Available at escholarship.org/uc/item/9v03g1kh

[3] J. Adem, *On the Hurwitz problem over an arbitrary field I*, Bol. Soc. Mat. Mexicana (2) 25 (1980), no. 1, 29-51

[4] J. Adem, *On the Hurwitz problem over an arbitrary field II*, Bol. Soc. Mat. Mexicana (2) 26 (1981), no. 1, 29-41.

[5] Daniel Dugger and Daniel C. Isaksen. *Algebraic K-Theory and Sums-of-Squares Formulas.* Documenta Mathematica, 10 (2005), 357-366.

[6] Daniel Dugger and Daniel C. Isaksen. *The Hopf Condition for Bilinear Forms over Arbitrary Fields.* Annals of Mathematics, 165 (2007), 943-964.

[7] Daniel Dugger and Daniel C. Isaksen. *Etale Homotopy and Sums-of-Squares Formulas.* Mathematical Proceedings of the Cambridge Philosophical Society, 145 (2008), 1-25.

[8] A. Hurwitz. *Uber die Komposition der Quadratischen Formen.* Math. Ann., 88 (1923), 1-25

[9] S. Yuzvinsky, *Orthogonal pairings of Euclidean spaces*, Michigan Math. J. 28 (1981), 131-145