My area of research is algebraic geometry and number theory. Specifically, I study the existence of sums-of-squares formulas over arbitrary fields.

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 \(F\). Over the real numbers, a sums-of-squares formula of type \([r, s, n]\) is equivalent to a bilinear map \(f : \mathbb{R}^r \times \mathbb{R}^s \to \mathbb{R}^n\) such that \(\|f(x, y)\| = \|x\| \cdot \|y\|\). A sums-of-squares formula can be thought of as a product or composition law \(F^r \times F^s \to F^n\) such that the norm of the product is the product of the norms. For an example, multiplication of complex numbers comes from a sums-of-squares formula of type \([2, 2, 2]\) over \(\mathbb{R}\):

\[
\begin{align*}
z_1 &= x_1y_1 - x_2y_2 \\
z_2 &= x_1y_2 + x_2y_1
\end{align*}
\]

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

Sums-of-squares formulas have been studied for their relationship with real normed division algebras, which have applications in quantum mechanics. These formulas continue to be of interest because of their connection to important problems in geometry and topology.

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 using computer searches?

In my work, I have found a new way to study these formulas by defining the algebraic variety of sums-of-squares formulas. This new perspective has enabled me to apply tools from algebraic geometry to sums-of-squares formulas.

By studying this variety, I have shown that, for large enough \(p\), existence of sums-of-squares formulas over algebraically closed fields is independent of the characteristic. 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 a group action on the variety of sums-of-squares formulas, I have started to study the structure of this variety. I have used the group action to improve efficiency in computer searches for sum-of-squares formulas over finite fields. I have incorporated undergraduates into my research by having them investigate the orbits of the this group action on sums-of-squares formulas over the integers.

For sums-of-squares formulas over the integers or finite fields, the search space is finite, so a brute force search can (theoretically) determine the existence of a formula. However, for even moderately large formulas, the search space is huge, making a brute force search completely impractical. Fortunately, using the group action and other observations, it’s possible to significantly refine this search.

I am currently working with Sudesh Kalyanswamy (Yale) on studying sums-of-squares formulas over the \(p\)-adics and developing efficient algorithms for finding formulas.
Background 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 [2], 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 \(F\)?

An example of a sums-of-squares formula of a more general type is given by:

\[
\begin{align*}
    z_1 &= x_1y_1 + x_2y_2 - x_3y_3 \\
    z_2 &= x_2y_1 - x_1y_2 + x_3y_4 \\
    z_3 &= x_1y_3 + x_3y_1 - x_2y_4 \\
    z_4 &= x_1y_4 + x_2y_3 + x_3y_2 \\
    z_5 &= x_1y_5 \\
    z_6 &= x_2y_5 \\
    z_7 &= x_3y_5
\end{align*}
\]

This is a formula of type \([3, 5, 7]\). There are also examples of sums-of-squares formulas over finite fields that do not come from a formula over \(\mathbb{Z}\).

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 [5] 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] [7] [8]. Fixing \(r\) and \(s\), their results establish lower bounds on \(n\) for which formulas of type \([r, s, n]\) exist. They showed that these lower bounds are valid over any field \(F\).

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 variety $X_{rsn}^F$ of sums-of-squares formulas of type $[r, s, n]$ over $F$. This geometric perspective is a new approach, and opens up many new algerbro-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 $\mathbb{Q}$ and $\bar{\mathbb{F}}_p$ for $p \neq 2$ prime:

**Theorem.** 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 $\mathbb{Q}$.

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 variety 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.** 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.

**Corollary.** If a sums-of-squares formula of type $[r, s, n]$ exists over some field $F$, then there is a sums-of-squares formula of type $[r, s, n]$ over some finite field $\mathbb{F}_p^m$.

This means that all formulas can potentially be found using computer searches involving finite fields.

The above results are proved in [1].

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

**Theorem.** If $X_{rsn}^F$ is nonempty, then $\dim X_{rsn}^F > 0$.

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

In addition, using the group action, I’m able to limit my computer searches to sums-of-squares formulas that have specific forms, making my algorithm significantly more efficient. For example, one can assume that certain coefficients are 0 or 1. The difficulty in these reductions arises from working with the quadratic form

$$(x_1, \ldots, x_m) \cdot (y_1, \ldots, y_m) = x_1 y_1 + \cdots + x_m y_m$$

(the dot product), which does not behave well in finite characteristic.

Improving efficiency of these searches is crucial to finding formulas computationally. The brute force algorithm for finding sums-of-squares formulas of a fixed type over a field of size $p$ has time complexity $p^{rsn}$. Thus, even small refinements on searches have a large impact on computability.
The group action can also 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 0.

**Undergraduate Research**

I’ve 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. Sums-of-squares formulas over the integers are equivalent to 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 are distinct.
2. The entries along each column are distinct.
3. If $M_{ij} = \pm M_{i'j'}$, then $M_{i'j'} = \pm M_{ij}$, and the $2 \times 2$ submatrix consisting of these entries has an odd number of minus signs.

The correspondence between sums-of-squares formulas and consistently signed intercalate matrices is given by:

$$M_{ij} = \pm k \text{ if and only if } x_iy_j \text{ occurs in } z_k \text{ with the given sign.}$$

For example, we give the $2 \times 2$ consistently signed intercalate matrix corresponding to the sums-of-squares formula giving multiplication of complex numbers.

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

This equivalence is easily accessible to students, and students comfortable with linear algebra can easily 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.

I plan to continue to recruit students to work on computing orbits of sums-of-squares formulas over the integers and over finite fields. Although the problem is simple to understand, it’s broad enough to provide work for many different projects. In addition, I hope that students will be able to use their computations to make new conjectures about the structure of the group action on the variety of sums-of-squares formulas.

In addition to original research on sums-of-squares formulas, I have supervised several senior projects 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.
References


