Summary

Often in mathematics, a theoretical investigation leads to a system of polynomial equations. Generically, such systems are difficult to solve. In applications, however, the equations come equipped with additional structure that can be exploited. It is crucially important, therefore, to develop techniques for studying structured polynomial systems. Hillar proposes to work on a wide range of problems that arise from other areas of mathematics and from the physical sciences. The intellectual merit of this research is two-fold: on the one hand, Hillar is advancing the theoretical understanding of fundamental mathematical objects; and on the other, he is developing algorithms for performing computations with them. Hillar has collaborated with 13 researchers, many of whom are near the beginning of their careers. In several cases, he has taken a leadership role with these younger people. These interactions broadly impact mathematics by uniting groups in different fields towards common goals as well as by preparing the next generation of mathematicians.

Numerical algorithms from semidefinite programming have become useful in many applications. A guiding open problem is to remove the need for approximations in these methods, while preserving their efficiency. Hillar proposes to solve this problem, building on recent success. A specific application is the Bessis-Moussa-Villani trace conjecture in theoretical physics, where Hägele and Klep-Schweighofer are carrying out a program Hillar has suggested. Hillar will interact further with these researchers on this difficult problem. He also plans to continue his collaboration with the young research group of Sottile on a broad number of questions in the Schubert calculus. This includes designing and maintaining large-scale computational experiments on the secant conjecture.

In chemistry and algebraic statistics, it is important to determine the algebraic relations between experimental measurements. Sturmfels has asked whether, up to symmetry, there are finitely many of them that generate the others. Aschenbrenner and Hillar answered this question for a special case, and Hillar proposes to continue the collaboration to solve this problem more generally. He will also work to provide a theoretical framework for an algorithm that they have been developing. Cyclic resultants count periodic points for systems in topological dynamics and Lagrangian mechanics. Sturmfels and Zworski have a precise conjecture for the number of resultants needed to recover the spectrum of such systems, and Hillar will work on a program to prove this conjecture. He will also continue collaboration with Lauve on binomial factorizations in group algebras.

Inspired by the work of Bayer, de Loera, and Lovász, Hillar and Windfeldt gave an algebraic characterization of uniquely colorable graphs using Gröbner bases. Hillar proposes to continue this commutative algebra approach to graph theory with the team of de Loera, Margulies, and Woo. This involves proving Nullstellensatz complexity bounds for computing chromatic numbers. Gröbner bases also appear in ongoing work with Garcia that is related to a conjecture of Casas-Alvero. In this application, a family of Gröbner bases seem to index partial sums of Catalan numbers, and Hillar will study this combinatorial relationship further.

Finally, Hillar proposes to complete a research program with Levine on word equations. While studying the BMV conjecture, Hillar and Johnson encountered symmetric word equations in positive definite letters. Solutions to such equations are potential counterexamples to the conjecture. This led Hillar to study word equations in uniquely divisible groups and to formulate an Abel theorem in this setting. He proposes to finish the remaining steps of this approach with Levine.

Proposed Research

The following proposal describes several interrelated lines of research in which I will actively participate during the tenure of this proposal. The topics include recent trends in optimization and real algebraic geometry, finiteness questions in commutative algebra, applications of Gröbner bases to graph theory and combinatorics, and progress towards noncommutative Abel theorems. Although these topics are broad, a common theme emerges: exploit structure in novel ways. Moreover, the techniques I have been developing are constructive and use symbolic computation in a fundamental way. I believe this is the new way forward in mathematics, where "algorithm" and "proof" will be as inseparable to mathematicians as "experiment" and "conjecture" have been to scientists.

1. Real Algebraic Geometry and Optimization

1.1. **Rational sums of squares.** In recent years, techniques from semidefinite programming have produced numerical algorithms for expressing positive semidefinite polynomials as sums of squares. These algorithms have many applications in optimization, control theory, quadratic programming, and matrix analysis [61, 62, 63, 64, 65]. Moreover, such representations aid in the computation of the real locus of a polynomial. For a noncommutative application of these techniques to a famous trace conjecture, see the next section, which discusses the papers [13, 30, 34, 46, 51, 74].

One major drawback with these algorithms is that their output is, in general, numerical. For many applications, however, exact polynomial identities are needed. In this regard, Sturmfels has asked the following question.

Question 1.1 (Sturmfels)**.** *If $f \in \mathbb{Q}[x_1, \ldots, x_n]$ is a sum of squares in $\mathbb{R}[x_1, \ldots, x_n]$, then is f also a sum of squares in $\mathbb{Q}[x_1, \ldots, x_n]$?*

This question has a positive answer in the univariate case due to results of Landau [50] and Pourchet [66]. It follows from a famous theorem of Artin [67] that if $f \in \mathbb{Q}[x_1, \ldots, x_n]$ is a sum of squares of rational functions in $\mathbb{R}(x_1, \ldots, x_n)$, then it is a sum of squares in $\mathbb{Q}(x_1, \ldots, x_n)$. Moreover, from the work of Voevodsky on the Milnor conjectures, it is known that 2^{n+2} such squares suffice [49]. However, the transition from rational functions to polynomials is often a very delicate one. For instance, not every polynomial that is a sum of squares of rational functions is a sum of squares of polynomials [67].

More generally, Sturmfels is interested in the algebraic degree [60] of maximizing a linear functional over the space of all sum of squares representations of a given polynomial that is a sum of squares. In the special case of Question 1.1, a positive answer signifies an algebraic degree of 1 for this optimization problem.

General theory reduces Question 1.1 to one involving real algebraic numbers. Recently, I made progress in the multivariate case when the coefficients lie in a totally real number field K. My main theorem in [33] is the following.

Theorem 1.2. *Let K be a totally real number field with Galois closure L and let R be a commutative $\mathbb{Q}$-algebra. If $f \in R$ is a sum of m squares in $R \otimes_{\mathbb{Q}} K$, then f is a sum of $4m \cdot 2^{[L:\mathbb{Q}]}\binom{[L:\mathbb{Q}]+1}{2}$ squares in R.*

My proof of Theorem 1.2 was constructive. It is known [15] that arbitrarily large numbers of squares are necessary to represent any sum of squares over $\mathbb{R}[x_1, \ldots, x_n]$, $n > 1$, making a fixed bound (for a given n) as in the rational function case impossible.

We propose to work on the generalization of this result to any real algebraic extension of $\mathbb{Q}$ in order to give a complete answer to Question 1.1. This work will settle the important question of how much limitation one has in using semidefinite techniques for finding algebraic certificates of nonnegativity.

1.2. **The BMV trace conjecture.** In 1975, while studying partition functions of quantum mechanical systems, Bessis, Moussa, and Villania formulated a conjecture regarding a positivity property of traces of matrices [11]. If this property holds, explicit error bounds in a sequence of Padé approximants follow. Let A and B be $n \times n$ Hermitian matrices with B positive semidefinite, and let

$$\phi^{A,B}(t) = \mathrm{Tr}[\exp{(A - tB)}].$$

The original formulation of the conjecture asserts that $\phi^{A,B}$ is completely monotone.

Since the conjecture was introduced in [11], many partial results and extensive computational experimentation have been given [16, 17, 20, 26, 31, 43, 36, 56, 58], all in favor of the conjecture's validity. However, despite much work, very little is known about the problem, and it has remained unresolved except in very special cases. Recently, Lieb and Seiringer in [53], and as previously communicated to us [43], have reformulated the conjecture of [11] as a question about the traces of certain sums of words in two positive definite matrices.

Conjecture 1.3 (BMV)**.** *The polynomial $p(t) = \mathrm{Tr}\left[(A + tB)^m\right]$ has all nonnegative coefficients whenever A and B are $n \times n$ positive semidefinite matrices.*

The coefficient of t^k in $p(t)$ is the trace of the sum, $S_{m,k}(A, B)$, of all words of length m in A and B, in which k B's appear. In [43], among other things, it was noted that, for $m < 6$, each constituent word in $S_{m,k}(A, B)$ has nonnegative trace. Thus, the above conjecture is valid for $m < 6$ and arbitrary positive integers n. It was also noted in [43] (see also [11]) that the conjecture is valid for arbitrary m and $n < 3$. Thus, the first case in which prior methods did not apply and the conjecture was in doubt, is $m = 6$ and $n = 3$. Even in this case, all coefficients, except $\mathrm{Tr}[S_{6,3}(A, B)]$, were known to be nonnegative (also as shown in [43]). It was only recently [36], using heavy computation, that Johnson and I showed this remaining coefficient to be nonnegative.

Much of the subtlety of Conjecture 1.3 lies in the fact that $S_{m,k}(A, B)$ need not have all nonnegative eigenvalues, and in addition that some terms within the sum defining $S_{m,k}(A, B)$ can have negative trace. This later fact was only proved recently in work with Johnson [43] (with the help of Shaun Fallat), in which we disproved the conjecture [43] that all positive definite words in two letters have positive trace.

In [34], I made progress on the conjecture with the following theorem.

Theorem 1.4. *Suppose that there exist integers m', k' and $n \times n$ positive definite matrices A and B such that $\mathrm{Tr}[S_{m',k'}(A, B)] < 0$. Then, for any $m \geq m'$ and $k \geq k'$ such that $m - k \geq m' - k'$, there exist $n \times n$ positive definite A and B making $\mathrm{Tr}[S_{m,k}(A, B)]$ negative.*

Corollary 1.5. *If the Bessis-Moussa-Villani conjecture is true for some exponent m_0, then it is also true for all $m < m_0$.*

Corollary 1.5 motivates a general program to solve the BMV conjecture, and there is evidence that this approach is more than a theoretical possibility. For instance, Hägele

[30] has used this approach and Corollary 1.5 to prove the conjecture for all $m \leq 7$ (and all n). Inspired by Hägele's ideas, Klep and Schweighofer [74] used semidefinite programming and noncommutative sums of squares techniques to prove the conjecture for all $m \leq 13$. One of their motivations was the Connes' embedding conjecture on von Neumann algebras [47]. It should be noted that these techniques provably fail [30] for the difficult $m = 6$ case, making the appeal to Corollary 1.5 fundamental. Other work along these lines appears in the papers of Burgdorf [13] and Landweber-Speer [51].

Another approach is to use the following theorem found in my paper [34]. It characterizes the BMV conjecture in terms of the eigenvalues of the matrix $S_{m,k}(A,B)$ and resembles the Perron-Frobenius theorem for nonnegative matrices.

Theorem 1.6. *Fix positive integers $m \geq k$ and n. Then, $\mathrm{Tr}[S_{m,k}(A,B)] \geq 0$ for all positive semidefinite A,B if and only if for all positive semidefinite A,B, the matrix $S_{m,k}(A,B)$ either has a positive eigenvalue or is the zero matrix.*

It follows that to prove the BMV conjecture, it is enough to show the positivity of only one of the eigenvalues of $S_{m,k}(A,B)$, rather than the sum of all of them. I propose to continue the study of this conjecture in light of these new methods and approaches.

1.3. **Reality in the Schubert Calculus.** Boris and Michael Shapiro conjectured in 1995 that a zero-dimensional intersection of Schubert varieties given by flags which osculate the real rational normal curve would consist only of real points. Sottile investigated this conjecture both experimentally and theoretically [76], generating significant interest [22, 23, 78]. Utilizing a surprising connection to representation theory, Mukhin, Tarasov, and Varchenko [59] recently settled the Shapiro conjecture. This gives rise to infinite families of polynomial systems which have only real solutions.

Inspired by a generalization of Shapiro to flags called the monotone conjecture [73], Eremenko, et. al [24] formulated another conjecture. The conditions in the Shapiro conjecture are Schubert varieties defined by flags that osculate the rational normal curve γ. A *secant flag* $F_\bullet$ is one where every subspace F_i of $F_\bullet$ is spanned by its points of intersection with γ. Secant flags $F_\bullet^1, \ldots, F_\bullet^s$ are *disjoint* if there exist disjoint intervals $I_1, \ldots, I_s$ of γ such that the subspaces in flag $F_\bullet^i$ meet γ at points of I_i. They conjectured that in a Grassmannian an intersection of Schubert varieties defined by disjoint secant flags has only real points. In the limit as the interval I_i shrinks to a point the secant flag $F_\bullet^i$ becomes an osculating flag, and so this extends the Shapiro conjecture. They proved this secant conjecture for lines in $\mathbb{P}^n$, which implies the monotone conjecture for flags consisting of a point lying on a line in $\mathbb{P}^n$.

I am investigating this secant flag conjecture and a common generalization of both it and the monotone conjecture with Sottile's Schubert calculus group at Texas A&M University. I have been developing the computational framework for storing, maintaining, and running a large-scale experimental exploration of this new conjecture. This project is similar to the one outlined in [73]. This is pat of a long-term program, involving hundreds of gigaHertz-years of computing over many calendar years. We plan to write a paper describing our results about secant flags during this academic year, and we will archive our data on the web, and the next step will be to generalize this work to all flag manifolds. This project also involves mentoring a number of young researchers in both the theoretical and practical aspects of computation.

2. Finiteness questions in rings with infinite Krull dimension

2.1. **Ideals of Algebraic Relations.** In chemistry [55, 71, 72] and algebraic statistics [21], a motivating problem is to determine the algebraic relations between experimental measurements. In this regard, Sturmfels has asked whether, up to symmetry, there are finitely many of them that generate the others. We discuss the mathematics of this problem and an approach by Aschenbrenner and myself for solving it.

Fix a natural number $k \geq 1$. Given a positive integer n, we denote by $\langle n \rangle^k$ the set of all ordered k-element subsets of $\{1, \dots, n\}$. Let K be a field, and for $n \geq k$ consider the polynomial ring $R_n = K\big[\{x_{\boldsymbol{u}}\}_{\boldsymbol{u} \in \langle n \rangle^k}\big]$. We let $\mathfrak{S}_n$ act on $\langle n \rangle^k$ by

$$\sigma(u_1, \dots, u_k) = \big(\sigma(u_1), \dots, \sigma(u_k)\big).$$

This induces an action $(\sigma, x_{\boldsymbol{u}}) \mapsto \sigma x_{\boldsymbol{u}} = x_{\sigma \boldsymbol{u}}$ of $\mathfrak{S}_n$ on the indeterminates $x_{\boldsymbol{u}}$, which we extend to an action of $\mathfrak{S}_n$ on R_n in the natural way. Set $R = \bigcup_{n \geq k} R_n$. Note that $R = K\big[\{x_{\boldsymbol{u}}\}_{\boldsymbol{u} \in \langle \Omega \rangle^k}\big]$, where $\Omega = \{1, 2, 3, \dots\}$ is the set of positive integers, and that the actions of $\mathfrak{S}_n$ on R_n combine uniquely to an action of $\mathfrak{S}_\infty$ on R. Now let $f(y_1, \dots, y_k) \in K[y_1, \dots, y_k]$, let $t_1, t_2, \dots$ be an infinite sequence of pairwise distinct indeterminates over K, and for $n \geq k$ consider the K-algebra homomorphism

$$\phi_n \colon R_n \to K[t_1, \dots, t_n], \qquad x_{(u_1, \dots, u_k)} \mapsto f(t_{u_1}, \dots, t_{u_k}).$$

The ideal $Q_n = \ker \phi_n$ of R_n determined by such a map is the prime ideal of algebraic relations between the quantities $f(t_{u_1}, \dots, t_{u_k})$. An important open problem is to understand the limiting behavior of such relations.

The ideals Q_n form an increasing *chain* $Q_\circ : Q_k \subseteq Q_{k+1} \subseteq \cdots \subseteq Q_n \subseteq \cdots$. Such chains fail to stabilize in the usual sense; however, it is possible for them to stabilize "up to the action of the symmetric group", a concept we make precise below. Notice first that the chains induced by a polynomial f are *invariant* under the action of the symmetric group in the sense that

$$\langle \mathfrak{S}_m Q_n \rangle \subseteq Q_m \ \text{ and } \ R_n \cap Q_m \subseteq Q_n \ \text{ for all } \ n \leq m.$$

Equivalently, the ideal $Q = \bigcup_{n \geq k} Q_n \subseteq R$ is invariant under the action of $\mathfrak{S}_\infty$. The stabilization definition alluded to above is as follows.

Definition 2.1. *A chain $Q_\circ$ stabilizes if there exists a positive integer N such that*

$$\langle \mathfrak{S}_m Q_n \rangle = Q_m \qquad \text{for all } m \geq n > N.$$

To put it another way, accounting for the natural action of the symmetric group, the ideals Q_n are the same for large enough n. In applications, this would imply that there are only a finite number of "test relations" to check whether a series of measurements satisfies a hypothetical underlying model.

When $k = 1$, Aschenbrenner and I have shown that R is Noetherian as an $R[\mathfrak{S}_\infty]$-module [7], which implies that any invariant chain stabilizes. When $k > 1$, however, R is no longer Noetherian, making Sturmfels' question about stability much more subtle. In [7], we were able to prove a special case.

Theorem 2.2. *The sequence of kernels Q_n induced by a square-free monomial $f \in K[y_1, \dots, y_k]$ stabilizes. Moreover, a bound for when stabilization occurs is $N = 4k$.*

The proof of this result used in a special way the toric geometry that underlies this question. This theorem provides evidence for the following conjecture.

Conjecture 2.3. *The sequence of kernels induced by any monomial $f \in K[y_1, \ldots, y_k]$ stabilizes.*

We propose to settle this conjecture. A key step will be to generalize a theorem of Camina and Evans [14]. Namely, we will give a characterization of all the $\mathfrak{S}_\infty$-submodules of $\mathbb{Q}\langle\Omega\rangle^k$. We will then use this description to get precise information on the union Q of toric ideals Q_n. These results will also be of independent interest.

2.2. **Symbolic Computation of Symmetric Gröbner Bases.** In computational algebra, one encounters the following general problem.

Problem 2.4. *Let I be an ideal of a ring R and let $f \in R$. Determine whether $f \in I$.*

When $R = K[x_1, \ldots, x_n]$ is a polynomial ring in n indeterminates over a field K, this problem has a spectacular solution due to Buchberger [10].

Theorem 2.5 (Buchberger)**.** *Let $I = \langle f_1, \ldots, f_m\rangle_R$ be an ideal of $R = K[x_1, \ldots, x_n]$. Then, there is a computable, finite set of polynomials G such that for every polynomial f, we have $f \in I$ if and only if the polynomial reduction of f with G is* 0.

One remarkable feature of this result is that once such a *Gröbner basis* G for I is found, any new instance of the question "Is $f \in I$"? can be solved very quickly. Theorem 2.5 forms the backbone of the field of computational algebraic geometry.

We study a different but related membership problem Let $X = \{x_1, x_2, \ldots\}$ be an infinite collection of indeterminates, indexed by the positive integers, and let $\mathfrak{S}_\infty$ be the group of permutations of X. For a positive integer N, we will also let $\mathfrak{S}_N$ denote the set of permutations of $\{1, \ldots, N\}$. Fix a field K and let $R = K[X]$ be the polynomial ring in the indeterminates X. The group $\mathfrak{S}_\infty$ acts naturally on R: if $\sigma \in \mathfrak{S}_\infty$ and $f \in K[x_1, \ldots, x_n]$,

$$\sigma f(x_1, \ldots, x_n) = f(x_{\sigma 1}, \ldots, x_{\sigma n}) \in R. \tag{2.1}$$

We motivate our discussion with the following concrete problem. Questions of this nature arise in applications to chemistry [55, 71, 72] and algebraic statistics [21].

Problem 2.6. *Let $f_1 = x_1^3 x_3 + x_1^2 x_2^3$ and $f_2 = x_2^2 x_3^2 - x_2^2 x_1 + x_1 x_3^2$ and consider the ideal $I = \langle \mathfrak{S}_\infty f_1, \mathfrak{S}_\infty f_2\rangle_R$ of $R = K[X]$ generated by all permutations of f_1 and f_2. Is the following polynomial involving* 10 *indeterminates in I?*

$$\begin{aligned} f \;=\; & -x_{10}^2x_9^2x_5^6 - 2x_{10}^2x_9x_8^3x_5^5 - x_{10}^2x_8^6x_5^4 + 3x_{10}^2x_8^2 + 3x_{10}^2x_7 + 3x_{10}x_9x_7x_4^3x_3^2x_2^2x_1 \\ & + 3x_{10}x_9x_7x_4^3x_3^2x_1^2 - 3x_{10}x_9x_7x_4^3x_2^2x_1^2 - x_9^2x_8^7x_7x_6x_5^6 - 2x_9x_8^{10}x_7x_6x_5^5 \\ & + x_9x_5^3x_3x_2x_1^3 + x_9x_5^3x_2^4x_1^2 + x_9x_3x_2^3x_1^4 + x_9x_2^6x_1^3 - x_8^13x_7x_6x_5^4 - 3x_8^2x_7 \\ & + x_7^2x_6x_3^3x_2^7 + x_7^2x_6x_3^3x_2^5x_1 - x_7^2x_6x_3x_2^7x_1 + x_5x_4^2 - 3x_5x_3^2 + 2x_5x_1^2 + x_4^2x_3^2 \\ & - 2x_3^2x_1^2 + 5x_3x_1^5 + 5x_2^3x_1^4. \end{aligned}$$

Naively, one could solve this problem using Buchberger's algorithm with truncated polynomial rings $R_n = K[x_1, \ldots, x_n]$. Namely, for each $n \geq 10$, compute a Gröbner basis G_n for the ideal $I_n = \langle \mathfrak{S}_n f_1, \mathfrak{S}_n f_2\rangle_{R_n}$, and reduce f by G_n. There are several problems with this approach. For one, this method requires computation of many Gröbner bases (the bottleneck in any symbolic computation), the number of which depends on the number of indeterminates appearing in f. Additionally, it lacks the ability to solve new membership problems quickly, a powerful feature of Buchberger's technique.

Building on our work in [7], Aschenbrenner and I have been developing an algorithm that solves the general membership problem for symmetric ideals (such as those appearing in Problem 2.6) and has all of the important features of Buchberger's method. It is the first algorithm of its kind that we are aware of. We develop some notation.

Let $R[\mathfrak{S}_\infty]$ denote the (left) group ring of $\mathfrak{S}_\infty$ over R with multiplication given by $f\sigma \cdot g\tau = fg(\sigma\tau)$ for $f, g \in R$ and $\sigma, \tau \in \mathfrak{S}_\infty$, and extended by linearity. The action (2.1) naturally gives R the structure of a (left) module over the ring $R[\mathfrak{S}_\infty]$. An ideal $I \subseteq R$ is called *symmetric* if $\mathfrak{S}_\infty I := \{\sigma f : \sigma \in \mathfrak{S}_\infty,\ f \in I\} \subseteq I$. Symmetric ideals are then simply the $R[\mathfrak{S}_\infty]$-submodules of R.

We will also use the following notation. Let B be a ring and let G be a subset of a B-module M. Then $\langle f : f \in G\rangle_B$ will denote the B-submodule of M generated by the elements of G. For instance, the invariant ideal $I = \langle x_1, x_2, \ldots\rangle_R$, as a module over the group ring $R[\mathfrak{S}_\infty]$, has the compact presentation $I = \langle x_1\rangle_{R[\mathfrak{S}_\infty]}$. The results of [7] generalize this simple example and imply a surprising Noetherianity of the module R.

Theorem 2.7. *Let I be a symmetric ideal of R. Then, I is finitely generated as a module over $R[\mathfrak{S}_\infty]$. Moreover, there is finite set of polynomials G such that for every polynomial f, we have $f \in I$ if and only if the polynomial reduction of f with G is 0.*

The polynomial reduction appearing in Theorem 2.7 is a symmetric modification of the reduction in the context of normal (finite dimensional) polynomial rings.

Example 2.8. *The ideal $I = \langle x_1^3x_3 + x_1^2x_2^3, x_2^2x_3^2 - x_2^2x_1 + x_1x_3^2\rangle_{R[\mathfrak{S}_\infty]}$ from Problem 2.6 has a symmetric Gröbner basis given by:*

$$G = \mathfrak{S}_3 \cdot \{x_3x_2x_1^2, x_3^2x_1 + x_2^4x_1 - x_2^2x_1, x_3x_1^3, x_2x_1^4, x_2^2x_1^2\}.$$

Once G is found, testing whether a polynomial f is in I is computationally fast; for instance, one finds that $f \in I$ for the polynomial encountered in Problem 2.6. □

My work with Aschenbrenner has focused on developing a theoretical framework for an algorithm we discovered that finds the set G in Theorem 2.7. This involves a new and important partial order on monomials that respects the action of the symmetric group. We aim to make our techniques computationally effective, and we will apply them to the important finite dimensional situation. Many researchers in this field have been interested in incorporating our methods for computing Gröbner bases with symmetry because traditional techniques remove such structure. We also aim to generalize our results to other group actions and rings.

3. Questions Related to Cyclic Resultants

3.1. **The Chez Panisse Conjecture.** Given a polynomial $f(x) = c\prod_{i=1}^d (x - \lambda_i) \in \mathbb{C}[x]$, the m-th *cyclic resultant* of f is

$$r_m = \operatorname{Res}(f, x^m - 1) = c^m \prod_{i=1}^{d} (\lambda_i^m - 1). \tag{3.1}$$

One motivation for the study of cyclic resultants comes from topological dynamics. Sequences of the form (3.1) count periodic points for toral endomorphisms A. Cyclic resultants were also studied by Pierce and Lehmer [25] in the hope of using them to produce large primes. Further motivation comes from knot theory [77], Lagrangian mechanics [29, 42], and, more recently, in the study of amoebas of varieties [69], complexity theory [70], and quantum computing [45].

The problem of recovering a polynomial from its sequence of cyclic resultants arises naturally in many applications. Commonly, an explicit bound $N = N(d)$ is desired in terms of the degree d of f so that the first N resultants $r_1, \ldots, r_N$ determine f [42, 45]. For instance, given a toral endomorphism, one would like to use a minimal amount of period data to recover the spectrum of A. Building on my work in [39], Levine and I Proved the following in [39].

Theorem 3.1. *A generic monic polynomial $f(x) \in \mathbb{C}[x]$ of degree d is determined by its first 2^{d+1} cyclic resultants $r_1, \ldots, r_{2^{d+1}}$. A generic monic reciprocal polynomial of even degree d is determined by its first $2 \cdot 3^{d/2}$ cyclic resultants.*

Theorem 3.1 is far from tight. A conjecture of Sturmfels and Zworski addresses the special case of a *reciprocal* polynomial f, that is, one satisfying $f(1/x) = x^d f(x)$.

Conjecture 3.2 (Chez Panisse I)**.** *A reciprocal monic polynomial $f(x) \in \mathbb{C}[x]$ of even degree d is determined by its first $d/2 + 1$ cyclic resultants.*

The name of the conjecture comes from the fact that Sturmfels and Zworski have offered a free dinner to the solver at the world-class Chez Panisse restaurant in Berkeley. Recently, there has been some progress on this conjecture for a special class of reciprocal polynomials. Kedlaya [45] has shown that for a certain reciprocal polynomial f of degree d arising from the numerator $P(t)$ of a zeta function of a curve over a finite field $\mathbb{F}_q$, the first d resultants are sufficient to recover f. He uses this result to give a quantum algorithm that computes $P(t)$ in time polynomial in the degree of the curve and $\log q$. A proof of Conjecture 3.2 would further reduce the running time for Kedlaya's algorithm. Levine and I made the following related conjecture [39].

Conjecture 3.3 (Chez Panisse II)**.** *A generic monic polynomial $f(x) \in \mathbb{C}[x]$ of degree d is determined by its first $d + 1$ cyclic resultants.*

In [39], Levine and I were able to offer a result in the direction of these conjectures. We say that a sequence $\{a_n\}_{n\geq 1}$, $a_n \in K$ obeys a *polynomial recurrence of length ℓ* if there is a polynomial $P \in K[x_1, \ldots, x_\ell]$ such that $P(a_n, \ldots, a_{n+\ell-1}) = 0$ for all $n \geq 1$.

Theorem 3.4. *Let $f \in \mathbb{C}[x]$ be a monic polynomial of degree d. The sequence $\{r_n\}_{n\geq 1}$ of cyclic resultants of f obeys a polynomial recurrence of length $d + 1$. Moreover if f is reciprocal of even degree d, then $\{r_n\}$ obeys a polynomial recurrence of length $d/2 + 1$.*

For example, the monic quadratic polynomial $f(x) = x^2 + ax + b$ gives rise to the length-3 polynomial recurrence,

$$\begin{aligned}
&(a+b+1)\left[(a-2)r_{n+2} + a(a-b-1)r_{n+1} + (a-2b)br_n - (a-b-1)(a+b+1)\right] \\
&= -r_{n+2}^2 - (a-2b)r_{n+1}r_{n+2} + abr_nr_{n+2} + (a-b-1)br_{n+1}^2 \\
&\quad - (a-2)b^2r_nr_{n+1} - b^3r_n^2.
\end{aligned}$$

I have two approaches to settling the Chez Panisse conjectures. The first idea is to use Theorem 3.4 to find polynomial recurrences for cyclic resultants and set up a system of equations for the unknown polynomial f. Kauers and Zimmermann have developed tools for this purpose [44]. These polynomial recurrences exist because of an algebraic relation in a certain semigroup ring. Given enough cyclic resultant data, we can produce enough equations in the coefficients of f to determine the unique solution in terms of the coefficients. Moreover, these equations are nice because they are all supported on the same monomials in the coefficients of f.

There is another approach that I believe it has a high chance of settling the Chez Panisse conjectures. Equations 3.1 are sparse polynomials in the roots of f. There is a well-developed theory of sparse systems of equations with supports given by the integer points in polytopes. This involves an interplay of polyhedral subdivisions and toric geometry. I propose to use this machinery in this highly structured special case. The analysis is delicate, however, since the coefficients of these sparse systems are far from generic. I implemented this program successfully for the case $d = 2$ and $d = 3$, and I aim to generalize these arguments.

3.2. **Binomial Factorizations in Group Algebras.** Let G be a group and let $\mathbb{Z}[G]$ be the group algebra over $\mathbb{Z}$. We study the question of when two binomial factorizations in $\mathbb{Z}[G]$ are equal. This problem arises naturally from the study of cyclic resultants [27, 35, 39]. Given a polynomial $f(x) \in \mathbb{C}[x]$, let r_m be the m-th cyclic resultant of f, given by (3.1). Let S denote the ring of sequences over $\mathbb{C}$ under pointwise sum and product, and for $\mu \in \mathbb{C}$, let $e(\mu)$ denote the exponential sequence $e(\mu)_n = \mu^n$. With this identification, the infinite sequence $r = (r_m)$ (3.1) of cyclic resultants can be represented succinctly by

$$r = e(c)\prod_{i=1}^{d}(e(\lambda_i) - e(1)) \in S.$$

When $G = \mathbb{C}^*$, the map $e : \mathbb{Z}[G] \to S$ sending $\mu \mapsto e(\mu)$ (and extended by linearity) is an embedding of $\mathbb{Z}$-algebras [39]. It follows that determining when two polynomials have equal sets of cyclic resultants is equivalent to solving a problem in binomial factorization.

Extending earlier work of Fried [27], I used this approach in [35] to completely characterize when two polynomials have equal sets of cyclic resultants. Lauve and I are generalizing the underlying factorization result used to prove the main theorem of [35] to the case of noncommtative groups G. The following definition explains what we shall mean by unique factorization of binomials.

Definition 3.5. *A subset S of a group G has the unique binomial factorization property if the existence of a factorization*

$$a\prod_{i=1}^{m}(g_i - h_i) = b\prod_{i=1}^{n}(u_i - v_i), \quad a, b \in \mathbb{Z},\ g_i^{-1}h_i, u_i^{-1}v_i \in S$$

in $\mathbb{Z}[G]$ implies that $a = \pm b$, $m = n$, and that up to permutation, for each i, there are elements $c_i \in G$ such that $(g_i - h_i)$ is conjugate to $\pm c_i(u_i - v_i)$.

The factorization result in [35] can be rephrased as saying that set of the torsion-free elements of an Abelian group G have unique binomial factorization. We do not know if this statement holds for any group G. However, we have made some progress for groups with some additional structure that generalizes the abelian case.

Definition 3.6. *Let G be a finitely generated group and let $S \subset G$. The set S is called* nonderogatory *if for any $g_1, \ldots, g_n \in S$, there is an additive group homomorphism $\phi : G \to \mathbb{R}$ such that $\phi(g_i) \neq 0$ for all i.*

A large class of nonderogatory subsets can be obtained from the following [35].

Proposition 3.7. *The torsion-free elements of an Abelian group are nonderogatory.*

An important noncommutative example is the case $G = GL_n(\mathbb{C})$. Here, there is a natural homomorphism $\phi : G \to \mathbb{R}$ given by $\phi(A) = \log|\det A|$, and the set of elements of G with determinants outside the unit circle is nonderogatory.

Lauve and I are working on a program to prove a sufficient condition for unique factorizations of binomials in a group algebra.

Conjecture 3.8. *Nonderogatory subsets of a group G have the unique binomial factorization property.*

In the case of abelian G, this generalizes the known result [35], but it also would have direct consequences for many other groups, such as $GL_n(\mathbb{C})$.

There are several steps in our program to prove Conjecture 3.8. Using the nonderogatory property of the set S, we embed a supposed factorization into the (generalized) Laurent polynomial ring $\mathbb{Z}[G][t, t^{-1}]$ by way of the map $g \mapsto gt^{\phi(g)}$. This allows us to equate the group algebra coefficients of powers of t separately. The argument then deals with the explosion of combinatorial possibilities that results, and this requires a subtle study of finitely presented groups. We have carried out this study successfully for small numbers of binomials and also for special cases in the free group F_2. This project involves a pleasing blend of combinatorics, group theory, and symbolic computation

4. Gröbner Basis and Combinatorics

4.1. **Graphs and Commutative Algebra.** In recent years, it has been fruitful to study questions on graphs using commutative algebra. Let G be a simple, undirected graph with vertex set $V = \{1, \ldots, n\}$ and edge set E. Fix a positive integer $k < n$, and let $C_k = \{c_1, \ldots, c_k\}$ be a k-element set. Each element of C_k is called a *color*. A (vertex) *k-coloring* of G is a map $\nu : V \to C_k$. We say that a k-coloring ν is *proper* if adjacent vertices receive different colors; otherwise ν is called *improper*. The graph G is said to be *k-colorable* if there exists a proper k-coloring of G. Let $R = \mathbb{C}[x_1, \ldots, x_n]$, and consider the following ideals of R:

$$I_{n,k} = \langle x_i^k - 1 : i \in V \rangle,$$
$$I_{G,k} = I_{n,k} + \langle x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_i x_j^{k-2} + x_j^{k-1} : \{i, j\} \in E \rangle.$$

The zeroes of $I_{n,k}$ and $I_{G,k}$ represent k-colorings and proper k-colorings of the graph G, respectively. The idea of using roots of unity and ideal theory to study graph coloring problems seems to originate in Bayer's thesis [9], although it has appeared in many other places, including the work of de Loera [18] and Lovász [54]. These ideals are important because they allow for an algebraic formulation of k-colorability. Versions of the following theorem appeared in [4, 9, 18, 54, 57].

Theorem 4.1. *The following statements are equivalent:*

(1) *The graph G is not k-colorable.*
(2) $\dim_{\mathbb{C}} R/I_{G,k} = 0$.
(3) *The constant polynomial* 1 *belongs to the ideal* $I_{G,k}$.
(4) *The graph polynomial* f_G *belongs to the ideal* $I_{n,k}$.

This theorem gives rise to algorithms [41] for determining k-colorability of a graph that are different from the traditional ones that use deletion and contraction. In [41], Windfeldt and I refined Theorem 4.1 and gave an algebraic characterization of uniquely colorable graphs. This provided us with algorithms to verify a counterexample of Akbari, Mirrokni, and Sadjad [3] to Xu's conjecture [79].

Independently, de Loera et al [19] have been studying complexity questions related to Gröbner bases and combinatorial optimization problems, such as graph colorings. The condition that $1 \in I_{G,k}$ can be checked by a Gröbner basis calculation, but the speed of this calculation is intimately related to the sizes of the degrees in a Nullstellensatz certificate. General theory says that this complexity is doubly exponential in the number of vertices n. However, for the special situation encountered here, there is much evidence to suggest that the complexity is only singly exponential. This would explain our experimental findings in [41]. Moreover, a careful implementation would allow for the computation of the chromatic numbers of large graphs, a significant advance.

I have begun working on this complexity problem with the team of de Loera, Margulies, and Woo. Our first approach will be to step through the papers of Sombra [75] and Kollár [48] for our special class of ideals. The hope is that some of the estimates in these works can be improved when the ideals come from graphs. We will also perform a similar inspection of the recent algorithmic advances on Castelnuovo-Mumford regularity [32], which is an important invariant measuring the complexity of an ideal. This theoretical work will be accompanied by a series of large-scale computations, which we will use to test our conjectures. In the process, we will develop a suite of tools that will be made available for other researchers working on symbolic computation and graph theory.

4.2. **Gröbner Bases and Partial Sums of Catalan Numbers.** The Casas-Alvero conjecture says that the following are equivalent for a degree d monic polynomial $f \in \mathbb{C}[x]$:

(1) $f(x) = (x-b)^d$ for some $b \in \mathbb{C}$.
(2) $\gcd(f, \frac{d^i f}{dx^i}) \neq 1$ for all $k = 1, \dots, d-1$.

For certain classes of degrees (for instance, prime powers), this result is known to be true [12]. Garcia and I have been studying this conjecture from the perspective of commutative algebra and Gröbner bases. Clearly (1) $\Rightarrow$ (2), and so the conjecture is (2) $\Rightarrow$ (1). Fix d and let $r_1, \dots, r_d$ be indeterminates. Also, set $f_d(x) = (x-r_1)\cdots(x-r_d)$. Consider the polynomials in $\mathbb{Z}[r_1, \dots, r_d]$,

$$s_k = \mathrm{Res}(f_d, f_d^{(k)}), \quad k = 1, \dots, d-1,$$

in which $f_d^{(k)}$ is the kth derivative of f_d with respect to x. The conjecture may be reformulated in terms of the ideal $I_d = \langle s_k : k = 1, \dots, d-1 \rangle$ and its variety:

Conjecture 4.2. *For the ideals I_d, we have $V(I_d) = \{(r, r, \dots, r) \in \mathbb{C}^d : r \in \mathbb{C}\}$.*

Unfortunately, this ideal is very complicated [12], and so Garcia and I made a relaxation. Let J_d be the ideals generated by the following polynomials:

$$t_k = \mathrm{Res}(x - r_1, f_d^{(k)}), \quad k = 1, \ldots, d-1.$$

In this case, it is readily verified that an analog of Conjecture 4.2 holds. We have some ideas for using the information gained from studying the ideals J_d. For instance, we hope to induct on the integer l in a relaxation that replaces $(x - r_1)$ with $(x - r_1) \cdots (x - r_l)$ in the definition of t_k. The ideals J_d then form the base case in this approach.

It turns out that the collection of J_d are very interesting combinatorially. For instance, choosing the lexicographic ordering on monomials in $r_1, \ldots, r_d$ and computing the reduced Gröbner basis G_d for each J_d, one finds that it consists of homogenous polynomials and that $|G_d|$ is identical (up to $d = 12$) to an interesting combinatorial sequence of numbers $\{1, 2, 4, 9, 23, 65, 197, 626, \ldots\}$, the partial sums of the Catalan numbers. Let $C_d = \frac{1}{d+1}\binom{2d}{d}$ denote the dth Catalan number. Then, we conjecture the following.

Conjecture 4.3. *For the Gröbner bases G_d, we have $|G_d| = \sum_{i=0}^{d-1} C_d$.*

We have much evidence for this conjecture. For instance, we have determined an algorithm that (conjecturally) generates the leading monomials in G_d. We also found a way to index the monomials generated by this algorithm, and we have proved that they are in combinatorial bijection with partial sums of Catalan numbers. The next step in our approach is to match the steps in this algorithm with the sequence of S-polynomial reductions that occur in a Gröbner basis calculation of the ideals J_d.

The phenomenon found in Conjecture 4.3 appears to be new, although Aval-Bergeron-Bergeron have also recently discovered an ideal having similar combinatorial structure that occurs naturally when computing the dimension of a quotient ring of quasisymmetric functions [8]. As in our case, they sought a bijection between the combinatorial objects they were studying and steps in a Gröbner basis calculation. Garcia and I also plan to investigate if there is a quotient ring of dimension $|G_d|$ hiding in our work.

5. An Abel Theorem for Word Equations

The Lieb and Seiringer formulation of the BMV trace conjecture says that the trace of $S_{m,k}(A, B)$, the sum of all words of length m in A and B with k Bs, is nonnegative for all positive semidefinite matrices A and B. In the case of 2×2 matrices, every word in two positive semidefinite letters has nonnegative trace, thereby verifying the BMV conjecture for this case. It was unknown whether this fact held in general until Johnson and I [43] (with the help of Shaun Fallat) found that the word $W = BABAAB$ has negative trace with the matrices:

$$A_1 = \begin{bmatrix} 1 & 20 & 210 \\ 20 & 402 & 4240 \\ 210 & 4240 & 44903 \end{bmatrix} \quad \text{and} \quad B_1 = \begin{bmatrix} 36501 & -3820 & 190 \\ -3820 & 401 & -20 \\ 190 & -20 & 1 \end{bmatrix}.$$

Finding such examples is surprisingly difficult as the methods in [43] show, and randomly generating millions of matrices will fail to produce them [43]. Nonetheless, we believe that most words can have negative trace, and we made the following conjecture in [43].

Conjecture 5.1. *A word in two letters A and B has positive trace for every pair of real positive definite A and B if and only if the word is a palindrome or a product (juxtaposition) of 2 palindromes.*

Evidence for the conjecture can be found in [38], where we essentially proved it in the complex Hermitian case. Positive definite matrices which give a word a negative trace are potential counterexamples to the BMV conjecture, and it is useful to be able to generate many of these matrices. As remarked above, this is a difficult task since random sampling methods do not work.

We were led to constructing these matrices by solving positive definite word equations. Let W be a palindrome in the letters A and B. If the equation $W(A_1, X) = B_1$ may be solved for a positive definite X given A_1 and B_1, then the word $WAWAAW$ can have negative trace. This would allow us to construct many potential counterexamples to the BMV conjecture. In this regard, we were able to show the surprising result that every palindromic word equation $W(A, X) = B$ has a positive definite solution X for any pair of positive definite A and B [37]. The proof of this result uses fixed point methods, although for special cases, one may express X explicitly in terms of A, B, and their fractional powers. For instance, the Riccati equation $XAX = B$ has solution

$$X = A^{-1/2}\left(A^{1/2}BA^{1/2}\right)^{1/2}A^{-1/2}. \tag{5.1}$$

Even though solutions always exist, it is usually very difficult to solve word equations [5]. Solutions of the form (5.1), however, can be computed efficiently, and it is natural to try and determine those equations which can be solved similarly. The correct setting for this question is the category of *uniquely divisible groups* (also called *universal*). These are groups G for which every $g \in G$ has a unique nth root for each positive integer n. Such groups have appeared recently in Aguiar's work on combinatorial Hopf algebras [1, 2]. Equation (5.1) is the unique solution to $XAX = B$ in any uniquely divisible group.

I have investigated this problem and formulated a conjecture that gives a complete description of those word equations that have solutions in terms of radicals.

Definition 5.2. *A word is called totally decomposable if it can be expressed as a composition of maps of the following forms applied to the letter X.*

- $\pi_{m,k}(W) = (WA^k)^m W$, *$m$ a positive integer, k a nonnegative integer*
- $r(W) = WA$
- $l(W) = AW$

It is not hard to prove that a decomposable word equation has solutions in terms of radicals. The following converse can be viewed as an Abel theorem for word equations.

Conjecture 5.3. *A word equation $W(X, A) = B$ is solvable in terms of radicals only if W is a totally decomposable word.*

I have developed a program to prove this conjecture. The idea involves gluing together an infinite sequence of specially constructed finite groups. It uses a pleasing blend of number theory (Dirichlet's theorem on arithmetic progressions and the Weil conjectures for curves) and combinatorics (a new word polynomial which characterizes total decomposability in terms of its factorability). With Levine, we can show that this program settles Conjecture 5.3 for words of length less than 20. I will continue to collaborate with Levine on this problem and carry out the remaining details of the program.

References

[1] M. Aguiar, N. Bergeron, F. Sottile, *Combinatorial Hopf algebras and generalized Dehn-Sommerville equations*, Compositio Mathematica **142** (2006) 1–30.

[2] M. Aguiar, *Factorization of characters on graded connected Hopf algebras*, preprint.

[3] S. Akbari, V. S. Mirrokni, B. S. Sadjad, *K_r-Free uniquely vertex colorable graphs with minimum possible edges*. Journal of Combinatorial Theory, Series B **82** (2001), 316–318.

[4] N. Alon, M. Tarsi, *Colorings and orientations of graphs*. Combinatorica **12** (1992), 125–134.

[5] S. Armstrong and C. Hillar, *Solvability of symmetric word equations in positive definite letters*, J. London Math. Soc., **76** (2007), no. 3, 777–796.

[6] M. Aschenbrenner and C. Hillar, *An algorithm for computing symmetric Gröbner bases in infinite dimensional polynomial rings*, in preparation.

[7] M. Aschenbrenner and C. Hillar, *Finite generation of symmetric ideals*, Trans. Amer. Math. Soc., **359** (2007), 5171–5192.

[8] J.C. Aval, F. Bergeron, N. Bergeron, *Ideals of quasi-symmetric functions and super-covariant polynomials for S_n*, Adv. Math., **181** (2004), 353–367.

[9] D. Bayer, *The division algorithm and the Hilbert scheme*. Ph.D. Thesis, Harvard University, 1982.

[10] B. Buchberger, *An algorithmic criterion for the solvability of algebraic systems of equations*, Aequat. Math. **4** (1970), 374–383.

[11] D. Bessis, P. Moussa, M. Villani, *Monotonic converging variational approximations to the functional integrals in quantum statistical mechanics*, J. Math. Phys. **16** (1975), 2318–2325.

[12] H. von Bothmer, O. Labs, J. Schicho, C. van de Woestijne, *The Casas-Alvero conjecture for infinitely many degrees*, preprint.

[13] S. Burgdorf, *Notes on $S_{m,4}(X{\cdot}Y^2)$*, preprint.

[14] A. R. Camina, D. M. Evans, *Some infinite permutation modules*, Quart. J. Math. Oxford Ser. (2) **42** (1991), no. 165, 15–26.

[15] M. D. Choi, Z. D. Dai, T. Y. Lam, B. Reznick, *The Pythagoras number of some affine algebras and local algebras*. J. Reine Angew. Math. **336** (1982), 45–82.

[16] K. J. Le Couteur, *Representation of the function* $\mathrm{Tr}(\exp(A - \lambda B))$ *as a Laplace transform with positive weight and some matrix inequalities*, J. Phys. A: Math. Gen. **13** (1980), 3147–3159.

[17] K. J. Le Couteur, *Some problems of statistical mechanics and exponential operators*, pp 209–235 in Proceedings of the International Conference and Winter School of Frontiers of Theoretical Physics, eds. F. C. Auluck, L.S. Kothari, V.S. Nanda, Indian National Academy, New Dehli, 1977, Published by the Mac Millan Company of India, 1978.

[18] J. A. de Loera, *Gröbner bases and graph colorings*, Beitrage zur Algebra und Geometrie **36** (1995), 89–96.

[19] J. A. de Loera, J. Lee, S. Margulies, S. Onn, *Expressing combinatorial optimization problems by systems of polynomial equations and the Nullstellensatz*, preprint.

[20] M. Drmota, W. Schachermayer and J. Teichmann, *A hyper-geometric approach to the BMV-conjecture*, Monatshefte fur Mathematik **146** (2005), 179–201.

[21] M. Drton, B. Sturmfels, S. Sullivant, *Algebraic factor analysis: Tetrads, pentads and beyond*, Probability Theory and Related Fields, to appear.

[22] A. Eremenko and A. Gabrielov, *Degrees of real Wronski maps*, Discrete Comput. Geom. **28** (2002), 331–347.

[23] A. Eremenko and A. Gabrielov, *Rational functions with real critical points and the B. and M. Shapiro conjecture in real enumerative geometry*, Ann. of Math. **155** (2002), 105–129.

[24] A. Eremenko, A. Gabrielov, M. Shapiro, A. Vainshtein, *Rational functions and real Schubert calculus*, Proc. Amer. Math. Soc. **134** (2006), 949–957

[25] G. Everest and T. Ward. Heights of Polynomials and Entropy in Algebraic Dynamics. Springer-Verlag London Ltd., London, 1999.

[26] M. Fannes and D. Petz, *Perturbation of Wigner matrices and a conjecture*, Proc. Amer. Math. Soc. **131** (2003), 1981–1988.

[27] D. Fried, *Cyclic resultants of reciprocal polynomials*, in Holomorphic Dynamics (Mexico 1986), Lecture Notes in Math. 1345, Springer Verlag, 1988, 124-128.

[28] D. Gondard, P. Ribenboim, *Le 17e problme de Hilbert pour les matrices*, Bull. Sci. Math., **98** (1974) 49–56.
[29] V. Guillemin, *Wave trace invariants*, Duke Math. J. **83** (1996), 287-352.
[30] D. Hägele, *Proof of the cases $p \leq 7$ of the Lieb-Seiringer formulation of the Bessis-Moussa-Villani conjecture*, J. Stat. Phys., **127** (2007), 1167–1171.
[31] F. Hansen, *Trace functions as Laplace transforms*, J. Math. Phys., **47** 043504 (2006).
[32] A. Hashemi, *Computation of Castelnuovo-Mumford regularity and satiety*, ISSAC 2007, preprint.
[33] C. Hillar, *Sums of polynomial squares over totally real fields are rational sums of squares*, Proc. Amer. Math. Soc., **137** (2009), 921–930.
[34] C. Hillar, *Advances on the Bessis-Moussa-Villani Trace Conjecture*, Lin. Alg. Appl., **426** (2007), 130–142.
[35] C. Hillar, *Cyclic resultants*, J. Symb. Comp. **39** (2005), 653–669; erratum, ibid. **40** (2005), 1126-1127.
[36] C. Hillar and C. R. Johnson, *On the positivity of the coefficients of a certain polynomial defined by two positive definite matrices*, J. Stat. Phys., **118** (2005), 781–789.
[37] C. Hillar and C. R. Johnson, *Symmetric word equations in two positive definite letters*, Proc. Amer. Math. Soc., **132** (2004), 945–953.
[38] C. Hillar and C R. Johnson, *Positive eigenvalues of generalized words in two Hermitian positive definite matrices*, in: Novel Approaches to Hard Discrete Optimization (P. Pardalos and H. Wolkowicz, eds.), Fields Institute Communications **37** (2003), 111–122.
[39] C. Hillar and L. Levine, *Polynomial recurrences and cyclic resultants*, Proc. Amer. Math. Soc., **135** (2007), 1607–1618.
[40] C. Hillar, J. Nie, *An elementary and constructive solution to Hilbert's 17th problem for matrices*, Proc. Amer. Math. Soc., **136** (2008), 73–76.
[41] C. Hillar and T. Windfeldt, *Algebraic characterization of uniquely colorable graphs*, J. Comb. Th. Ser. B, **98** (2008), 400–414.
[42] A. Iantchenko, J. Sjöstrand, and M. Zworski, *Birkhoff normal forms in semi-classical inverse problems*, Math. Res. Lett. 9 (2002), 337-362.
[43] C. R. Johnson and C. Hillar, *Eigenvalues of words in two positive definite letters*, SIAM J. Matrix Anal. Appl., **23** (2002), 916–928.
[44] M. Kauers and B. Zimmermann, *Computing the Algebraic Relations of C-finite Sequences and Multisequences*, Technical Report 2006-24, SFB F013, Johannes Kepler Universität Linz, Austria.
[45] K. Kedlaya, *Quantum computation of zeta functions of curves*, Computational Complexity **15** (2006), 1–19.
[46] I. Klep and M. Schweighofer, *Sums of Hermitian squares and the BMV conjecture*, J. Stat. Phys., **133** (2008), 739–760.
[47] I. Klep and M. Schweighofer, *Connes' embedding conjecture and sums of hermitian squares*, Adv. Math., **217** (2008), 1816–1837.
[48] J. Kollár, *Sharp effective Nullstellensatz.* J. Amer. Math. Soc. **1** (1988), 963–975.
[49] T. Y. Lam, *Introduction To Quadratic Forms Over Fields*, American Mathematical Society, 2004.
[50] E. Landau, *Uber die Darstellung definiter Funktionen durch Quadrate*, Math Ann., **62** (1906), 272–285.
[51] P. Landweber and E. Speer, *On D. Hägeles approach to the Bessis-Moussa-Villani conjecture*, Lin. Alg. Appl., **431** (2009) 1317–1324.
[52] J. Lawson and Y. Lim, *Solving symmetric matrix word equations via symmetric space machinery*, Lin. Alg. Appl., **414** (2006), 560–569.
[53] E. H. Lieb and R. Seiringer, *Equivalent forms of the Bessis-Moussa-Villani conjecture*, J. Stat. Phys., **115** (2004), 185-190.
[54] L. Lovász, *Stable sets and polynomials.* Discrete Mathematics **124** (1994), 137–153.
[55] A. Mead, E. Ruch, A. Schönhofer, *Theory of chirality functions, generalized for molecules with chiral ligands.* Theor. Chim. Acta **29** (1973), 269–304.
[56] N. Miller, 3×3 *cases of the Bessis-Moussa-Villani conjecture*, Princeton University Senior Thesis, 2004.

[57] M. Mnuk, *On an algebraic description of colorability of planar graphs.* In Koji Nakagawa, editor, *Logic, Mathematics and Computer Science: Interactions. Proceedings of the Symposium in Honor of Bruno Buchberger's 60th Birthday.* RISC, Linz, Austria, October 20-22 (2002), 177–186.

[58] P. Moussa, *On the representation of* $\mathrm{Tr}\left(e^{A-\lambda B}\right)$ *as a Laplace transform*, Rev. Math. Phys. **12**, 621–655 (2000).

[59] E. Mukhin, V. Tarasov, A. Varchenko, *The B. and M. Shapiro conjecture in real algebraic geometry and the Bethe ansatz*, preprint.

[60] J. Nie, K. Ranestad, B. Sturmfels, *The algebraic degree of semidefinite programming*, math.CO/0611562.

[61] S. Prajna, A. Papachristodoulou, P. A. Parrilo, *Introducing SOSTOOLS: A General Purpose Sum of Squares Programming Solver.* Proceedings of the IEEE Conference on Decision and Control (CDC), Las Vegas, NV. 2002.

[62] S. Prajna, A. Papachristodoulou, P. A. Parrilo, *New Developments in Sum of Squares Optimization and SOSTOOLS.* Proceedings of the American Control Conference (ACC), Boston, MA. 2004.

[63] P. Parrilo, *Semidefinite programming relaxations for semialgebraic problems.* Math. Program., Ser. B **96** (2003), 293–320.

[64] P. Parrilo, *Exploiting algebraic structure in sum of squares programs*, Positive polynomials in Control, Lecture Notes in Control and Information Sciences, Vol. 312, pp. 181–194, Springer, 2005.

[65] P. Parrilo, B. Sturmfels, *Minimizing polynomial functions*, Algorithmic and quantitative real algebraic geometry, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Vol. 60, pp. 83–99, AMS.

[66] Y. Pourchet, *Sur la représentation en somme de carrés des polynômes á une indéterminée sur un corps de nombres algébriques*, Acta Arith. **19** (1971), 89–104.

[67] A. Prestel, C. N. Delzell, *Positive Polynomials: From Hilbert's 17th Problem to Real Algebra*, Springer, 2001.

[68] C. Procesi, M. Schacher, *A Non-Commutative Real Nullstellensatz and Hilbert's 17th Problem*, Ann. of Math., **104** (1976) 395–406.

[69] K. Purbhoo, *A Nullstellensatz For Amoebas*, preprint.

[70] M. Rojas, *Efficiently detecting subtori and torsion points*, proceedings of MAGIC 2005 (Midwest Algebra, Geometry, and their Interactions Conference, Oct. 7-11, 2005, Notre Dame University, Indiana), edited by A. Corso, J. Migliore, and C. Polini), pp. 213-233, Contemporary Mathematics, vol. 44x, AMS Press, to appear.

[71] E. Ruch, A. Schönhofer, *Theorie der Chiralitätsfunktionen*, Theor. Chim. Acta **19** (1970), 225–287.

[72] E. Ruch, A. Schönhofer, I. Ugi, *Die Vandermondesche Determinante als Näherungsansatz für eine Chiralitätsbeobachtung, ihre Verwendung in der Stereochemie und zur Berechnung der optischen Aktivität*, Theor. Chim. Acta **7** (1967), 420–432.

[73] J. Ruffo, Y. Sivan, F. Sottile, E. Soprunova, emphExperimentation and conjectures in the real Schubert calculus for flag manifolds, Exper. Math., **15**, tt(2006), 199–221.

[74] M. Schweighofer, *Algorithmische Beweise für Nichtnegativ- und Positivstellensätze*, Diplomarbeit an der Universität Passau, 1999.

[75] M. Sombra, *Bounds for the Hilbert function of polynomial ideals and for the degrees in the Nullstellensatz.* J. Pure Appl. Algebra **117** & **118** (1997) 565–599.

[76] F. Sottile, *Real Schubert calculus: polynomial systems and a conjecture of Shapiro and Shapiro*, Experiment. Math. **9** (2000), 161–182.

[77] W. H. Stevens, *Recursion formulas for some abelian knot invariants*, Journal of Knot Theory and Its Ramifications, Vol. 9, No. 3 (2000) 413-422.

[78] J. Verschelde, *Numerical evidence of a conjecture in real algebraic geometry*, Exper. Math. **9** (2000), 183–196.

[79] S. Xu, *The size of uniquely colorable graphs*, Journal of Combinatorial Theory Series B **50** (1990), 319–320.