Complexity of Membership Problems of Different Types of Polynomial Ideals

Ernst W. Mayr and Stefan Toman

Abstract We survey degree bounds and complexity classes of the word problem for polynomial ideals and related problems. The word problem for general polynomial ideals is known to be exponential space-complete, but there are several interesting subclasses of polynomial ideals that allow for better bounds. We review complexity results for polynomial ideals with low degree, toric ideals, binomial ideals, and radical ideals. Previously known results as well as recent findings in our project "Degree Bounds for Gröbner Bases of Important Classes of Polynomial Ideals and Efficient Algorithms" are presented.

Keywords Polynomial ideal • Binomial ideal • Gröbner basis • Degree bound • Radical • Thue system • Cellular decomposition • Computational complexity

Subject Classifications 13P10, 14Q20, 03D40, 08A50, 03D03, 06B10

1 Introduction

Solving systems of polynomial equations is one of the most common problems in mathematics. Objects are modelled as polynomial equations and the solutions of these equations themselves or properties of them need to be found. These problems turn out to be inherently hard and it is a common technique to first deduce bases with certain properties that make solving the problems easier. The goal of our project "Degree Bounds for Gröbner Bases of Important Classes of Polynomial Ideals and Efficient Algorithms" in the priority program SPP 1489 "Algorithmic

E.W. Mayr • S. Toman (✉)
Institut für Informatik, TU München, München, Germany
e-mail: mayr@in.tum.de; toman@tum.de

G. Böckle et al. (eds.), *Algorithmic and Experimental Methods in Algebra, Geometry, and Number Theory*,
https://doi.org/10.1007/978-3-319-70566-8_20

and Experimental Methods in Algebra, Geometry, and Number Theory" of Deutsche Forschungsgemeinschaft (DFG) was to find upper and lower complexity bounds for solving different subclasses of polynomial equations. In this paper we report on results that were previously known and the ones found during this project.

The special case of linear equations is well-understood. These systems can be transformed to row-echelon form in polynomial time using the Gaussian algorithm. Several problems like finding solutions of the system or the word problem can be solved easily once the system is in row-echelon form. The corresponding problems for non-linear systems of equations are inherently much harder. According to the Abel-Ruffini theorem solutions of these systems cannot even be expressed in general using simple formulas involving roots only [1]. Nevertheless, there is also a normal form of these systems called Gröbner bases that allows for easier computations of many problems.

2 General Polynomial Ideals

Gröbner bases were introduced in 1965 by Buchberger in his PhD thesis [4]. They can be employed to solve many problems in computer algebra, the most immediate being the word problem for polynomial ideals. This problem is given a list of multivariate polynomial equations to decide whether another polynomial equation is contained in the ideal they span, i.e. whether the latter is already implied by these equations. The word problem can be solved using Gröbner bases and Buchberger also presented an algorithm for this problem using the so-called Buchberger criterion.

At first, it was only known that Buchberger's algorithm runs in finite time without having better space or runtime bounds. In 1982 Mayr and Meyer proved a lower bound on the worst-case space usage of each algorithm solving the word problem for polynomial ideals that is exponential in the number of variables appearing in the equations [18].

Theorem 2.1 ([18]) *There is a constant $\epsilon \in \mathbb{Q}$ with $\epsilon > 0$ such that any algorithm which is able to decide the word problem for polynomial ideals contained in $\mathbb{Q}[x_1, \ldots, x_n]$ for some $n \in \mathbb{N}_{>0}$ requires space exceeding $2^{\epsilon n}$ on infinitely many instances of this problem with different sizes.*

Their result was slightly improved in 1991 by Yap who changed the constant in the exponent [27].

The time and space requirements of algorithms computing Gröbner bases heavily depend on the number of indeterminates of the polynomial ring. For this reason it is important to have degree bounds, for instance the ones by Hermann [10] and Dubé [6]. They found degree bounds double-exponential in the number of indeterminates.

Theorem 2.2 ([6]) *Let $f_1, \ldots, f_s \in R[x_1, \ldots, x_n]$ be polynomials with $\deg(f_i) \leq d$ for all $i \in \{1, \ldots, s\}$ over a ring R for some $d, s \in \mathbb{N}_{>0}$. Every reduced Gröbner basis of $\langle f_1, \ldots, f_s \rangle$ consists of polynomials $g_1, \ldots, g_r \in R[x_1, \ldots, x_n]$ for some $r \in \mathbb{N}_{>0}$ with*

$$\deg(g_i) \leq 2\left(\frac{d^2}{2} + d\right)^{2^{n-1}}$$

for all $i \in \{1, \ldots, r\}$.

Using those bounds, Kühnle and Mayr showed in 1996 that Gröbner bases can indeed be computed using exponential space in the number of indeterminates [15]. Thus, the lower and upper bounds for the word problem for polynomial ideals coincided and the problem was proven to be **EXPSPACE**-complete in the number of indeterminates. There are several surveys on further complexity results for the computation of Gröbner bases, for instance the one presented by Mayr [17].

Since the computation of Gröbner bases is that important and hard it is a natural question to ask whether there are special subclasses of polynomial ideals that allow for faster computations of them.

3 Polynomial Ideals with Low Dimension

One class of polynomial ideals that allows easier computations of their Gröbner bases is the set of zero-dimensional polynomial ideals. The dimension of a polynomial ideal is the maximum size of a set of indeterminates such that no leading monomial of a polynomial contained in this ideal consists of these indeterminates only. Equivalently, the dimension of a polynomial ideal is the size of the biggest set of indeterminates that is unrelated modulo the ideal. This means that zero-dimensional ideals have many relations between their indeterminates and there is even a relation for each indeterminate alone. This additional structure may be used to find improved degree bounds.

In 1983 Faugère et al. presented an algorithm that is much faster in practice for zero-dimensional polynomial ideals than Bucherberger's algorithm [8]. It was also proven that there is a single-exponential bound on the degree of Gröbner basis elements for zero-dimensional polynomial ideals by Dickenstein et al. which enables better algorithms [5].

Theorem 3.1 ([5]) *Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ be polynomials with $\deg(f_i) \leq d$ for all $i \in \{1, \ldots, s\}$ over a field k for $d, n, s \in \mathbb{N}_{>0}$ such that $\langle f_1, \ldots, f_s \rangle$ has dimension 0 and let $g \in \langle f_1, \ldots, f_s \rangle$ be a polynomial. There are polynomials*

$$g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$$

such that $g = \sum_{i=1}^{s} f_i g_i$ *and*

$$\deg(f_i g_i) \leq n d^{2n} + d^n + d + \deg(f)$$

for all $i \in \{1, \ldots, s\}$.

Since the special case of zero-dimensional polynomial ideals is much easier than the general problem one could expect polynomial ideals with low dimension to have better algorithms, too.

All degree bounds given above are dependent on the number of indeterminates as this turned out to be a very significant parameter of polynomial ideals to describe their inherent complexity. The following bound does not use the number of indeterminates as a parameter but the degree of the polynomial ideal which may result in better bounds for special subsets of polynomial ideals.

Using a new degree bound by Kratzer [14], Mayr and Ritscher were able to find an algorithm to compute Gröbner bases whose space is bounded exponentially in the dimension of the polynomial ideal [19].

Theorem 3.2 ([19]) *Let* $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ *be polynomials with* $\deg(f_i) \leq d$ *for all* $i \in \{1, \ldots, s\}$ *over an infinite field* k *for* $d, n, s \in \mathbb{N}_{>0}$. *Let* $m \in \mathbb{N}_0$ *be the dimension of* $\langle f_1, \ldots, f_s \rangle$. *Every reduced Gröbner basis of* $\langle f_1, \ldots, f_s \rangle$ *with respect to an admissible monomial ordering consists of polynomials* $g_1, \ldots, g_r \in R[x_1, \ldots, x_n]$ *for some* $r \in \mathbb{N}_{>0}$ *with*

$$\deg(g_i) \leq 2\left(\frac{1}{2}\left(d^{2(n-m)^2} + d\right)\right)^{2^m}$$

for all $i \in \{1, \ldots, r\}$.

This theorem is proven using an algorithm based on a cone decomposition of the space of polynomials. The construction of this decomposition is based on a similar decomposition presented by Dubé [6].

They also presented an incremental version of their algorithm that does not use degree bounds. The space bound of this algorithm uses the degree of the actual problem instance instead of a worst-case instance. Therefore, the algorithm does not require the knowledge of any a-priori degree bounds.

Both findings improved the known space bounds for polynomial ideals with low degree in comparison to the general bounds. Later, they also proved a matching lower bound [20] which finished the complexity analysis of computing Gröbner bases depending on the degree of the polynomial ideal.

4 Binomial Ideals

Another interesting subclass are binomial ideals and pure binomial ideals which are polynomial ideals that can be generated by binomials respectively pure binomials only. Binomials are polynomials with at most two terms while pure binomials

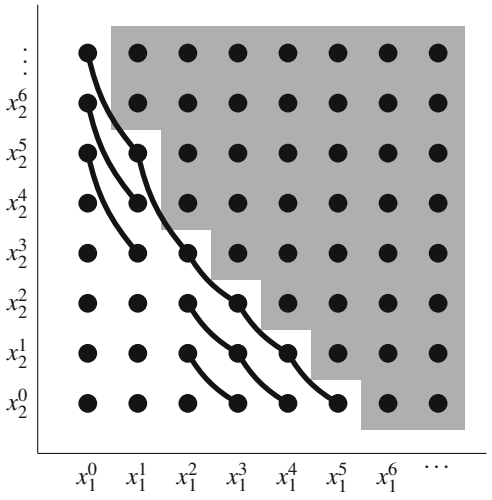

Fig. 1 The equivalence classes of monomials modulo $I = \langle x_1^3 - x_1^2 x_2, x_1 x_2^3 - x_2^5 \rangle$. Monomials are represented by points. Two of them are in the same equivalence class if they are connected by a line or both are in an area with gray background color

are polynomials with exactly two terms and coefficients 1 and -1, respectively. Pure binomial ideals can be thought of a partition of the set of monomials into equivalence classes. Two monomials are in the same equivalence class if and only if a pure binomial in the ideal uses those monomials as terms. This means that each of the monomials can be replaced by the other one modulo the ideal. A visualization of these equivalence classes for an example is shown in Fig. 1.

The example Mayr and Meyer presented to prove the exponential space lower bound on the word problem for general polynomial ideals consists of pure binomial ideals only, which implies that the word problem for pure binomial ideals is as hard as the word problem for general polynomial ideals.

Theorem 4.1 ([18]) *The word problem for pure binomial ideals is* **EXPSPACE***-complete.*

It is an interesting finding that binomial ideals do already contain the full complexity of the general case whereas the word problem for monomial ideals is solvable in polynomial time. An overview of the complexity of the word problem for different classes of polynomial ideals is listed in Table 1.

An application from theoretical computer science where pure binomial ideals occur are commutative Thue systems. These systems are term replacement systems with the additional properties that the order of the characters may be changed at every time and all replacements can also be executed backwards [23, 24].

Definition 4.2 ([23, 24]) A commutative Thue system consists of a finite set of congruences $\mathcal{P} = \{\alpha_i \equiv \beta_i \mid i \in \{1, \ldots, s\}\}$ for some $s \in \mathbb{N}_{>0}$ between words over a finite alphabet Σ. Two words $\gamma, \delta \in \Sigma^*$ are equivalent modulo the commutative Thue system $\mathcal{P}$ if and only if there are $\lambda_1, \ldots, \lambda_r \in \Sigma^*$ for some $r \in \mathbb{N}_{>0}$ with $\gamma = \lambda_1$, $\delta = \lambda_r$ and λ_j can be transformed to λ_{j+1} for all $j \in \{1, \ldots, r-1\}$ by

Table 1 Complexity classes known for the (radical) word problem of several classes of polynomial ideals

Type of ideals	Word problem	Radical word problem
Polynomial ideals	**EXPSPACE**-complete [18]	**PSPACE** [3, 11]
Binomial ideals	**EXPSPACE**-complete [18]	**coNP**-complete [25]
Pure binomial ideals	**EXPSPACE**-complete [18]	**coNP**-complete [25]
Toric ideals	**L** [22]	**L** [22]
Monomial ideals	**P**	**P**

reordering letters or applying a congruence $\alpha_i \equiv \beta_i$ for some $i \in \{1, \ldots, s\}$, i.e. replacing the subword α_i by the subword β_i or vice versa.

It turns out that there is a bijection from the set of pure binomial ideals to the set of commutative Thue systems preserving the structure of these objects.

Definition 4.3 Let $\Sigma = \{\sigma_1, \ldots, \sigma_n\}$ be a finite set with $n \in \mathbb{N}_0$ and let

$$\mathcal{P} = \left\{\alpha_i \equiv \beta_i | i \in \{1, \ldots, s\}\right\}$$

be a commutative Thue system for $s \in \mathbb{N}_{>0}$ and $\alpha_i, \beta_i \in \Sigma^*$ for $i \in \{1, \ldots, s\}$. Let $\Phi : \Sigma^* \to \mathbb{N}_0^n$ be the Parikh mapping, i.e. the i-th entry of $\Phi(\gamma)$ is the number of occurrences of σ_i in γ for all $\gamma \in \Sigma^*$ and $i \in \{1, \ldots, n\}$. For each ring R we define the polynomial ideal

$$\mathcal{I}_R(\mathcal{P}) := \left\langle \underline{x}^{\Phi(\alpha_i)} - \underline{x}^{\Phi(\beta_i)} | i \in \{1, \ldots, s\} \right\rangle \trianglelefteq R[x_1, \ldots, x_n]$$

Each instance of the equivalence problem for commutative Thue systems can be mapped to an instance of the word problem for pure binomial ideals and vice versa.

Theorem 4.4 ([18]) *For all commutative Thue Systems $\mathcal{P}$ we have*

$$\underline{x}^{\Phi(\gamma)} - \underline{x}^{\Phi(\delta)} \in \mathcal{I}_{\mathbb{Z}}(\mathcal{P}) \Leftrightarrow \underline{x}^{\Phi(\gamma)} - \underline{x}^{\Phi(\delta)} \in \mathcal{I}_{\mathbb{Q}}(\mathcal{P}) \Leftrightarrow \gamma \equiv \delta(\mathcal{P})$$

for all $\gamma, \delta \in \Sigma^*$.

The lower bound by Mayr and Meyer [18] was proven by giving a reduction of the **EXPSPACE**-complete problem to decide whether three-counter machines terminate with a computation bounded double-exponentially by the input size to the equivalence problem of commutative Thue systems.

5 Toric Ideals

Toric ideals are another important special case of polynomial ideals that often occur in practice. They appear in particular as the kernel of maps from polynomial rings to rings of Laurent polynomials. Toric ideals are the same as saturated pure binomial ideals or the extension of pure binomial ideals into the ring of Laurent polynomials [25]. Over algebraically closed coefficient fields toric ideals are the same as binomial prime ideals [7].

There is a polynomial time algorithm to solve the word problem for toric ideals and binomials by using Gaussian elimination on the Macaulay matrix of the toric ideal. This means that the inherent complexity of toric ideals is much lower than the one of binomial ideals.

Theorem 5.1 *Let $f_1, \ldots, f_s \in R[x_1, \ldots, x_n]$ be pure binomials over a ring R with $n, s \in \mathbb{N}_{>0}$ such that $\langle f_1, \ldots, f_s \rangle$ is a toric ideal. Let ϕ be a map from the set of pure binomials contained in $R[x_1, \ldots, x_n]$ to the $\mathbb{Z}$-vector space $\mathbb{Z}^n$ defined by $\phi(\underline{x}^\alpha - \underline{x}^\beta) := \alpha - \beta$ for all $\alpha, \beta \in \mathbb{N}_0^n$. Then we have*

$$g \in \langle f_1, \ldots, f_s \rangle \trianglelefteq R[x_1, \ldots, x_n] \Leftrightarrow \phi(g) \in \operatorname{span}\{\phi(f_1), \ldots, \phi(f_s)\} \subseteq \mathbb{Z}^n$$

for all pure binomials $g \in R[x_1, \ldots, x_n]$.

Using this approach and a memory-efficient algorithm for solving linear systems of equations Ritscher proved an upper space bound for the membership problem for toric ideals [22]. He was also able to extend the algorithm to test for the membership of general polynomials instead of pure binomials in toric ideals.

Theorem 5.2 ([22]) *Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ be pure binomials over a well-endowed field k with $n, s \in \mathbb{N}_{>0}$ such that $\langle f_1, \ldots, f_s \rangle$ is a toric ideal and let $g \in k[x_1, \ldots, x_n]$ be a polynomial with $t \in \mathbb{N}_{>0}$ terms. Let $q \in \mathbb{N}_{>0}$ be an upper bound on the bitsize of all coefficients and exponents of g and $f_1, \ldots, f_s$. The word problem to check whether $g \in \langle f_1, \ldots, f_s \rangle$ can be decided in space $\mathcal{O}\left(\log^2((n+s+t)q)\right)$.*

The word problem for toric ideals is therefore known to be contained in **L**, the complexity class of all problems solvable in logarithmic space. **L** is known to be contained in **P**, the class of all problems solvable in polynomial time, but it is unknown whether both classes are actually the same.

6 Radical Ideals

The radical of a polynomial ideal is constructed by adding all polynomials to the ideal such that a power of them is included in the original polynomial ideal. Thus, the radical is a superset of the original polynomial ideal. Growing the polynomial ideal in the described way does not change its variety, i.e. the set of

common solutions of all polynomials contained in the polynomial ideal, but just the multiplicities of the roots. The radical therefore contains all geometric information about a polynomial ideal. In contrast to pure binomial ideals, the degree bounds for radical ideals are better than the ones for the general case, although there are much less results for radical ideals. Containing the full geometric information but having better degree bounds makes radical ideals interesting objects to study.

Brownawell proved a single-exponential bound for the degrees of the coefficients of a polynomial's representation contained in radical ideals [3]. Kollár improved this bound 1 year later [11].

Theorem 6.1 ([11]) *Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ be polynomials with $\deg(f_i) \leq d$, $\deg(f_i) \neq 2$ for all $i \in \{1, \ldots, s\}$ over a field k for some $d, n, s \in \mathbb{N}_{>0}$ and let $g \in \sqrt{\langle f_1, \ldots, f_s \rangle}$. There are $r \in \mathbb{N}_{>0}$ and $g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$ such that*

$$g^r = \sum_{i=1}^{s} f_i g_i$$

with $s \leq d^n$ and $\deg(f_i g_i) \leq (1 + \deg(g))d^n$ for all $i \in \{1, \ldots, s\}$.

Using those degree bounds the word problem for radical ideals can be solved in polynomial space and exponential time by enumerating all possible $g_1, \ldots, g_s$. There are also several algorithms that compute the actual radical of a polynomial ideal, for instance the one presented by Laplagne in 2006 [16], but all known algorithms that compute radicals of all polynomial ideals need at least exponential space and double-exponential time which are the same bounds as for Gröbner basis computations and the word problem for general polynomial ideals.

7 Radical Binomial Ideals

The radical word problem is given a polynomial ideal and a polynomial to solve the word problem for the radical of this ideal and the polynomial. This problem is a generalization of the word problem for radical ideals. Algorithms solving the radical word problem might be more efficient than **EXPSPACE** which is needed to compute the radical since they do not need to actually compute a basis of the radical ideal. This problem is interesting because the result of the radical word problem is true if and only if the given polynomial holds for all solutions of the polynomial ideal, which means that using this problem one can deduce information about the solutions of a system of equations without actually computing the full solution.

Radicals of (pure) binomial ideals and toric ideals have even more structure as proven by Gilmer in 1984 [9] and Eisenbud and Sturmfels in 1996 [7].

Theorem 7.1 ([7, 9]) *Let k be a field and $n \in \mathbb{N}_{>0}$. The radical of each binomial ideal contained in $k[x_1, \ldots, x_n]$ is a binomial ideal again. Similarly, the radical of each pure binomial ideal contained in $k[x_1, \ldots, x_n]$ is a pure binomial ideal again.*

Theorem 7.2 ([7]) *Let k be an algebraically closed field with* $\mathrm{char}(k) = 0$ *and* $n \in \mathbb{N}_{>0}$ *and let* $I \trianglelefteq k[x_1, \ldots, x_n]$ *be a toric ideal. I is a radical ideal.*

This means the radical operation is closed under binomial ideals and pure binomial ideals. For toric ideals computing the radical does not change the ideal at all. It is therefore a common technique to reduce computations of radicals to toric ideals which are already radical.

In the case of binomial ideals over fields with characteristic 0 there is a special tool available to compute radicals doing this. In 1996 Eisenbud and Sturmfels introduced the cellular decomposition of binomial ideals [7]. They suggested to partition the variety of the binomial ideal into cells where points are in the same cell if they have the same components being non-zero. The intersection of the ideals corresponding to each cell is the radical of the original ideal.

Theorem 7.3 ([7]) *Let k be a field with* $\mathrm{char}(k) = 0$, $n \in \mathbb{N}_0$ *and* $I \trianglelefteq k[x_1, \ldots, x_n]$ *be a binomial ideal. Then*

$$\sqrt{I} = \bigcap_{\Delta \subseteq \{x_1, \ldots, x_n\}} I_\Delta : \left(\prod_{x_i \in \Delta} x_i \right)^\infty + \langle \{x_i \mid x_i \notin \Delta\} \rangle$$

where I_Δ is the image of I under the ring endomorphism on $k[x_1, \ldots, x_n]$ defined by

$$1 \mapsto 1, x_i \mapsto \begin{cases} x_i & \text{if } x_i \in \Delta \\ 0 & \text{else} \end{cases}$$

for all $i \in \{1, \ldots, n\}$ and $\Delta \subseteq \{x_1, \ldots, x_n\}$.

Even though the radical of a binomial ideal over a field with characteristic 0 is binomial again, the intermediate results do not have to be binomial since the intersection of two binomial ideals is not binomial in general. Nevertheless, in 1997 Becker, Grobe, and Niermann proved that the intersections of the cellular decomposition can be executed in an order such that all intermediate results are binomial [2]. This result implies that all intermediate results of the cellular decomposition of pure binomial ideals can be interpreted as commutative Thue systems, too.

Mayr and Toman presented an algorithm to solve the radical word problem for pure binomial ideals in **coNP** [21]. They used the cellular decomposition of binomial ideals and the polynomial time algorithm to solve the word problem for toric ideals. They also showed how to encode the coefficients of binomials to solve the radical word problem for non-pure binomial ideals in the same complexity class. Additionally, they proved a matching lower bound for the radical word problem of pure binomial ideals by giving a reduction from the **TAUTOLOGY** problem. This showed that the radical word problem for binomial ideals is **coNP**-complete.

It is interesting to note that this complexity class is characterized by the time needed for running the machine instead of its space consumption. All other complexity classes listed in Table 1 for general polynomial ideals or subclasses

mentioned in this report use space bounds for the machines. It is known that **coNP** is contained in **PSPACE**, which is the complexity of the radical word problem for general polynomial ideals, but it is still unknown whether there are problems contained in **PSPACE** but not in **coNP**.

We have seen that the bijection between pure binomial ideals and commutative Thue systems provides versatile tools for systems of pure binomial ideals. Operations on pure binomial ideals like the sum, product, intersection, quotient, and saturation each can be equivalently defined in terms of commutative Thue systems. As opposed to this, it is not possible to directly define radicals of commutative Thue systems since this definition involves powers of pure binomials which are no pure binomials anymore and therefore have no corresponding objects in terms of commutative Thue systems. In his PhD thesis Toman suggests a definition of radicals of commutative Thue systems not involving polynomial ideals [26].

To do this one needs a way to represent powers of binomials as binomials again. Squares of binomials for instance can be split up to two different binomials.

Theorem 7.4 ([26]) *Let $I \trianglelefteq k[x_1, \ldots, x_n]$ be a pure binomial ideal over a field k with $\mathrm{char}(k) = 0$ for some $n \in \mathbb{N}_{>0}$. Let $u, v \in \mathbb{N}_{>0}^n$. We have*

$$(\underline{x}^u - \underline{x}^v)^2 \in I \Leftrightarrow \underline{x}^{2u} - \underline{x}^{u+v} \in I, \underline{x}^{u+v} - \underline{x}^{2v} \in I$$

For a binomial g this theorem implies that g^2 is contained in the pure binomial ideal I if and only if all monomials of g^2 are equivalent modulo I. The latter property can be easily expressed using commutative Thue systems whereas the former involves polynomials that are no pure binomials and can therefore not be expressed in terms of commutative Thue systems. A similar theorem is true for higher powers of the binomial.

Theorem 7.5 ([26]) *Let $f_1, \ldots, f_s \in R[x_1, \ldots, x_n]$ be pure binomials over a ring R for some $d, n, s \in \mathbb{N}_{>0}$. Let*

$$g \in \sqrt{\langle f_1, \ldots, f_s \rangle} \trianglelefteq R[x_1, \ldots, x_n]$$

be a pure binomial. There is an $r \in \mathbb{N}_{>0}$ such that all terms of g^r are equivalent modulo $\langle f_1, \ldots, f_s \rangle$.

We were also able to find a degree bound on the exponent r that makes all terms of g^r equivalent that is only slightly bigger than all known degree bounds on the exponent t such that $g^t \in \langle f_1, \ldots, f_s \rangle$.

Theorem 7.6 ([26]) *In the setting of Theorem 7.5 with the additional property that $2 < \deg(f_i) \leq d$ for all $i \in \{1, \ldots, s\}$ we can choose*

$$r := 2d^n \Big(\log 2d^n + \log\log 2d^n \Big) + 1 \in \mathbb{N}_{>0}$$

All terms of a polynomial contained in a pure binomial ideal can be partitioned into equivalence classes modulo the ideal where the sum of the coefficients in each

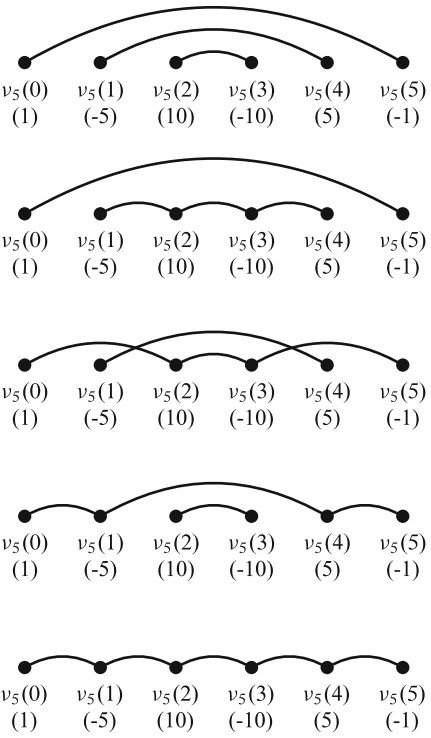

Fig. 2 All possible equivalence classes of terms of a fifth power of a pure binomial $(\underline{x}^u - \underline{x}^v)^5 \in I$ modulo a pure binomial ideal I. We use the notation $\nu_i(j) = \underline{x}^{ju+(i-j)v}$ and the coefficients of the terms are given in brackets

equivalence class is to 0. All possible configurations of those equivalence classes of the fifth power of a pure binomial are visualized in Fig. 2.

The theorems above imply that for powers of pure binomials we additionally only get one equivalence class for exponents of the given size. Those theorems allow the following definition of a radical of commutative Thue systems by translating them form pure binomial ideals to commutative Thue systems since they only contain statements on pure binomials only.

Theorem 7.7 ([26]) *Let Σ be a finite alphabet and let $\mathcal{P}$ be a commutative Thue system over Σ^*. We iteratively define $\mathcal{P}_0 := \mathcal{P}$ and $\mathcal{P}_i$ to be the commutative Thue system over Σ^* generated by all equivalences $\alpha \equiv_{\mathcal{P}_i} \beta$ with $\alpha, \beta \in \Sigma^*$ and*

$$\alpha\alpha \equiv_{\mathcal{P}_{i-1}} \alpha\beta \text{ as well as } \alpha\beta \equiv_{\mathcal{P}_{i-1}} \beta\beta$$

for $i \in \mathbb{N}_{>0}$. There is an $s \in \mathbb{N}_{>0}$ with $\mathcal{P}_s = \mathcal{P}_i$ for all $i \in \mathbb{N}_{>0}$, $i \geq s$ and

$$\mathcal{I}_{\mathbb{Q}}(\mathcal{P}_s) = \sqrt{\mathcal{I}_{\mathbb{Q}}(\mathcal{P})}$$

Using this approach one can compute the radical of a commutative Thue system in **EXPSPACE**. This is similar to numerous other problems on commutative Thue

systems which have a complexity of **EXPSPACE** like the coverability, the subword, the containment, and the equivalence problems [12, 13].

$\mathcal{P}_s$ is a radical of $\mathcal{P}$ defined purely in terms of commutative Thue systems. This construction provides another tool for finding better degree bounds for radical ideals.

8 Future Research

There are numerous open questions related to degree bounds of polynomial ideals that can be answered in future research. The known upper and lower bounds for the degree of the generators of a Gröbner bases of the radical of a given polynomial ideal do not match.

Likewise, the algorithms presented above for the radical word problem of binomial ideals do not compute an actual basis of the radical ideal. It is an open question whether the complexity for computing the basis of the radical of a binomial ideal is different to the general case.

Some of the results presented above only work for the rationals as base field of the polynomial ring. Similar bounds for positive characteristics of the base field are often unknown.

Acknowledgements This work was partially supported by Deutsche Forschungsgemeinschaft (DFG) through priority program SPP 1489 "Algorithmic and Experimental Methods in Algebra, Geometry, and Number Theory" in the project "Degree Bounds for Gröbner Bases of Important Classes of Polynomial Ideals and Efficient Algorithms", TUM Graduate School, and TopMath, a graduate program of the Elite Network of Bavaria. We are grateful for their support.

References

1. N.H. Abel, Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrieme degré. J. Reine Angew. Math. **1**, 65–96 (1826)
2. E. Becker, R. Grobe, M. Niermann, Radicals of binomial ideals. J. Pure Appl. Algebra **117–118**, 41–79 (1997)
3. W.D. Brownawell, Bounds for the degrees in the nullstellensatz. Ann. Math. **126**(3), 577 (1987)
4. B. Buchberger, Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal (An algorithm for finding the basis elements in the residue class ring modulo a zero dimensional polynomial ideal). Ph.D. Thesis, Mathematical Institute, University of Innsbruck (1965)
5. A. Dickenstein, N. Fitchas, M. Giusti, C. Sessa, The membership problem for unmixed polynomial ideals is solvable in single exponential time. Discret. Appl. Math. **33**(1), 73–94 (1991)
6. T.W. Dubé, The structure of polynomial ideals and Gröbner bases. SIAM J. Comput. **19**(4), 750–773 (1990)
7. D. Eisenbud, B. Sturmfels, Binomial ideals. Duke Math. J. **84**(1), 1–45 (1996)

8. J.C. Faugère, P. Gianni, D. Lazard, T. Mora, Efficient computation of zero-dimensional gröbner bases by change of ordering. J. Symb. Comput. **16**(4), 329–344 (1993)
9. R. Gilmer, *Commutative Semigroup Rings*. Chicago Lectures in Mathematics (University of Chicago Press, Chicago, 1984)
10. G. Hermann, Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. Math. Ann. **95**(1), 736–788 (1926)
11. J. Kollár, Sharp effective Nullstellensatz. J. Am. Math. Soc. **1**(4), 963 (1988)
12. U. Koppenhagen, E.W. Mayr, Optimal algorithms for the coverability, the subword, the containment, and the equivalence problems for commutative semigroups. Inf. Comput. **158**(2), 98–124 (2000)
13. U. Koppenhagen, E.W. Mayr, An optimal algorithm for constructing the reduced Gröbner basis of binomial ideals, and applications to commutative semigroups. J. Symb. Comput. **31**(1–2), 259–276 (2001)
14. M. Kratzer, Computing the dimension of a polynomial ideal and membership in low-dimensional ideals. Master's Thesis, TU München (2008)
15. K. Kühnle, E.W. Mayr, Exponential space computation of Gröbner bases. In: *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation - ISSAC '96* (ACM, New York, 1996), pp. 63–71
16. S. Laplagne, An algorithm for the computation of the radical of an ideal. In: *Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation - ISSAC '06* (ACM, New York, 2006), p. 191
17. E.W. Mayr, Some complexity results for polynomial ideals. J. Complexity **13**(3), 303–325 (1997)
18. E.W. Mayr, A.R. Meyer, The complexity of the word problems for commutative semigroups and polynomial ideals. Adv. Math. **46**(3), 305–329 (1982)
19. E.W. Mayr, S. Ritscher, Space-efficient Gröbner basis computation without degree bounds. In: *Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation* (ISSAC '11) (ACM, New York, 2011), pp. 257–264
20. E.W. Mayr, S. Ritscher, Dimension-dependent bounds for Gröbner bases of polynomial ideals. J. Symb. Comput. **49**, 78–94 (2013). The International Symposium on Symbolic and Algebraic Computation
21. E.W. Mayr, S. Toman, The complexity of the membership problem for radical binomial ideals, in *International Conference Polynomial Computer Algebra '2015*, ed. by N.N. Vassiliev (Euler International Mathematical Institute/VVM Publishing, Saint Petersburg, 2015), pp. 61–64
22. S. Ritscher, Degree bounds and complexity of Gröbner bases of important classes of polynomial ideals. Ph.D. Thesis, TU München (2012)
23. A. Thue, Die Lösung eines Spezialfalles eines generellen logischen Problems. Skrifter udg. af Videnskabs-Selskabet i Christiania. I, Math. Naturv. Klasse **8** (1910)
24. A. Thue, Problem über Veränderungen von Zeichenreihen nach gegebenen Regeln. Skrifter udg. af Videnskabs-Selskabet i Christiania. I, Math. Naturv. Klasse **10** (1914)
25. S. Toman, The radical word problem for binomial ideals. Master's Thesis, TU München (2015)
26. S. Toman, Radicals of binomial ideals and commutative Thue systems. Ph.D. Thesis, TU München (2017)
27. C.K. Yap, A new lower bound construction for commutative Thue systems with applications. J. Symb. Comput. **12**(1), 1–27 (1991)