Ideal Membership Problem and a Majority Polymorphism over the Ternary Domain

Arpitha P. Bharathi
IDSIA, Lugano, Switzerland
arpitha@idsia.ch

Monaldo Mastrolilli
IDSIA, Lugano, Switzerland
monaldo@idsia.ch

Abstract

The Ideal Membership Problem (IMP) asks if an input polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ with coefficients from a field $\mathbb{F}$ belongs to an input ideal $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$. It is a well-known fundamental problem with many important applications, though notoriously intractable in the general case. In this paper we consider the IMP for polynomial ideals encoding combinatorial problems and where the input polynomial f has degree at most $d = O(1)$ (we call this problem IMP_d). Our main interest is in understanding when the inherent combinatorial structure of the ideals makes the IMP_d "hard" (NP-hard) or "easy" (polynomial time) to solve.

Such a dichotomy result between "hard" and "easy" IMPs was recently achieved for Constraint Satisfaction Problems over finite domains [5, 24] (this is equivalent to IMP_0) and IMP_d for the Boolean domain [16], both based on the classification of the IMP through functions called polymorphisms. For the latter result, each polymorphism determined the complexity of the computation of a suitable Gröbner basis.

In this paper we consider a 3-element domain and a majority polymorphism (constraints under this polymorphism are a generalisation of the 2-SAT problem). By using properties of the majority polymorphism and assuming graded lexicographic ordering of monomials, we show that the reduced Gröbner basis of ideals whose varieties are closed under the majority polymorphism can be computed in polynomial time. This proves polynomial time solvability of the IMP_d for these constrained problems. We conjecture that this result can be extended to a general finite domain of size $k = O(1)$. This is a first step towards the long term and challenging goal of generalizing the dichotomy results of solvability of the IMP_d for a finite domain.

2012 ACM Subject Classification Mathematics of computing → Gröbner bases and other special bases; Mathematics of computing → Combinatoric problems

Keywords and phrases Polynomial ideal membership, Polymorphisms, Gröbner basis theory, Constraint satisfaction problems

Digital Object Identifier 10.4230/LIPIcs.MFCS.2020.13

Funding This research was supported by the Swiss National Science Foundation project 200020-169022 "Lift and Project Methods for Machine Scheduling Through Theory and Experiments".

1 Introduction

A polynomial ideal is a subset of the polynomial ring $\mathbb{F}[x_1, \ldots, x_n]$ with two properties: for any two polynomials f, g in the ideal, $f + g$ also belongs to the ideal and so does hf for any polynomial h in $\mathbb{F}[x_1, \ldots, x_n]$. The Hilbert Basis Theorem [10] states that every ideal I is finitely generated by a set $F = \{f_1, \ldots, f_m\} \subset I$, i.e., any polynomial in I is a polynomial combination of elements from F. The polynomial Ideal Membership Problem (IMP) is to find out if a polynomial f belongs to an ideal I or not, given a set of generators of the ideal. This fundamental algebraic complexity problem was first pioneered by David Hilbert [11] and

has important applications in solving polynomial systems and polynomial identity testing [8, 23]. The IMP is, in general, EXPSPACE-complete and Mayr and Meyer show examples that prove the double exponential growth of degree bounds [17, 18, 19].

The *vanishing ideal* of a set $S \subseteq \mathbb{F}^n$ is the set of all polynomials in $\mathbb{F}[x_1, \ldots, x_n]$ that vanish at every point of S. This set of polynomials forms an ideal. In this paper we consider vanishing ideals of the sets S of feasible solutions that arise from combinatorial problems. The vanishing ideal of the solution space S is defined as its *combinatorial ideal*. We consider the IMP for polynomial ideals over the field of rationals (i.e., $\mathbb{F} = \mathbb{Q}$) that encode combinatorial problems. We call such problems where the input polynomial has degree at most $d = O(1)$ as IMP_d. The polynomial ideals that arise from combinatorial problems frequently have special properties: these ideals are finite domain and therefore zero-dimensional and radical. It is important to identify restrictions (combinatorial problems) for which IMP_d is tractable, since this has applications to Sum-of-Squares (SoS) proof systems (or Lasserre relaxations) and theta bodies [9].

The SoS proof system is an increasingly popular tool to solve combinatorial optimization problems. Especially over the last few decades, SoS has had several applications in continuous and discrete optimization (see, e.g., [14]). It has often been claimed in recent papers that one can compute a degree d SoS proof (if one exists) via the Ellipsoid algorithm in $n^{O(d)}$ time. In a recent work, O'Donnell [20] observed that this often repeated claim is far from true. O'Donnell gave an example of a polynomial system and a polynomial which had degree two proofs of non-negativity with coefficients requiring an exponential number of bits, causing the Ellipsoid algorithm to take exponential time. O'Donnell [20] raised the open problem to establish useful conditions under which "small" SoS proof can be guaranteed automatically. Raghavendra and Weitz [21] provided a sufficient condition on a polynomial system that implies bounded coefficients in SoS proofs. In particular, the work of Raghavendra and Weitz [21] shows that the IMP_d tractability for combinatorial ideals implies polynomially bounded coefficients in SoS proofs. Therefore, the IMP_d tractability yields to degree d SoS proof (if one exists) computation via the Ellipsoid algorithm in $n^{O(d)}$ time. Moreover an efficient computation of the IMP_d leads to the efficient construction of theta bodies SDP relaxations for the considered problems [9, 15]. There are only very few examples of efficiently constructible theta bodies relaxations.

Hence the following question poses itself: which *restrictions* on combinatorial problems can guarantee an efficient computation of the IMP_d? In this paper we make restrictions on the constraint language (see Section 1.1), where each constraint language Γ produces a particular polynomial ideal membership problem denoted $\text{IMP}_d(\Gamma)$ (see A.2.1 of [16] for details on Ideal-CSP correspondence). The ultimate objective is to describe the complexity of the $\text{IMP}_d(\Gamma)$ for all constraint languages Γ. By placing restrictions on constraint languages, examinations regarding the computational complexity of the decision version of the Constraint Satisfaction Problem (CSP) over a language Γ on a finite domain (denoted by $\text{CSP}(\Gamma)$), has yielded successful results. The complexity classification of $\text{CSP}(\Gamma)$ started with the classic dichotomy result of Schaefer [22] for CSPs over the Boolean domain. Nearly thirty years after [22], the renowned dichotomy result for ternary domains was proven by Bulatov [4]. It took another decade to generalize the latter to any finite domain (see Bulatov [5] and Zhuk [24]), settling the long-standing Feder-Vardi dichotomy conjecture for finite domain CSPs. We refer to [6] for an excellent survey. Note that $\text{CSP}(\Gamma)$ corresponds to the very special case of the $\text{IMP}_d(\Gamma)$ with $d = 0$, i.e. where we are only interested in testing if the constant polynomial "1" belongs to the combinatorial ideal (see A.2.1 of [16] for more details). In this paper we are interested in the problem with $d \geq 1$.

By following the constraint language approach, Mastrolilli [16] recently showed that the question of ideal membership tractability for the Boolean setting admits a very clean answer. He presented a dichotomy result on when $\mathrm{IMP}_d(\Gamma)$ is decidable in polynomial time and when it is NP-complete. Mastrolilli's approach is based on the celebrated dichotomy result of Schaefer [22], the modern view of Constraint Satisfaction Problems and Gröbner basis theory introduced by Buchberger [3]. The modern approach of satisfiability of CSP is through functions called polymorphisms [1, 12]. Solvability of CSP in the Boolean domain has a nice dichotomy result: it is solvable in polynomial time if all constraints are closed under one of six polymorphisms (majority, minority, MIN, MAX, constant 0 and constant 1), else it is NP-complete. Mastrolilli [16] proved that the IMP_d generalization of the CSP for the Boolean domain also has a nice dichotomy result: it is solvable in polynomial time if all constraints are closed under one of four polymorphisms (majority, minority, MIN, MAX), else it is NP-complete.

In this paper, we attempt to begin the generalization of $\mathrm{CSP}(\Gamma)$ (viz. $\mathrm{IMP}_0(\Gamma)$) by working on the corresponding $\mathrm{IMP}_d(\Gamma)$ for any $d = O(1)$ in the ternary domain, which expands the known set of tractable IMP_d cases by providing a suitable class of combinatorial problems. The contribution of the paper can be viewed as the first step towards a long term and challenging goal: to extend the dichotomy results of $\mathrm{IMP}_0(\Gamma)$ for finite domain to $\mathrm{IMP}_d(\Gamma)$ for any constant $d \geq 1$. This would imply a very clean classification on the applicability of the approach in [21] for SoS and it would imply a dichotomy result on the complexity of theta bodies for any finite domain constraint language. However, this challenging goal is fraught with several difficulties, as partially underlined by the present paper. To some extent, this is not a surprise and reflects the fact that even the generalization from $\mathrm{CSP}(\Gamma)$ over the Boolean domain to the more general finite domain took about forty years to complete. We refer to Section 5 for a discussion.

Throughout this paper we assume that the reader has some basic knowledge of both, CSPs over a constraint language and algebraic geometry, more specifically Gröbner basis. We use notations and basic properties as in standard textbooks and literature [6, 7, 8]. However, in order to make this article accessible to non-expert readers, the appendix in [16] provides the essential context needed with the adopted notation. We recommend the non-expert reader to start with that section or refer to [6, 8]. We start with some basic definitions in Section 1.1. In Section 1.2 we formally state our results and how they are obtained. Therein we provide an overview of the proofs whose more detailed explanations are to be found in the remaining parts of the paper. Due to space limitations, omitted proofs can be found in the full version of this paper.

1.1 Preliminaries

Let D denote a finite set (*domain*). By a k-ary ***relation*** R on a domain D we mean a subset of the k-th cartesian power D^k; k is said to be the *arity* of the relation. We often use relations and (affine) varieties interchangeably since both essentially represent a set of solutions. A ***constraint language*** Γ over D is a set of relations over D. A constraint language is ***finite*** if it contains finitely many relations, and is *Boolean* if it is over the two-element domain $\{0, 1\}$. In this paper, D is the ternary domain $\{0, 1, 2\}$.

A ***constraint*** over a constraint language Γ is an expression of the form $R(x_1, \ldots, x_k)$ where R is a relation of arity k contained in Γ, and the x_i are variables. A constraint is satisfied by a mapping ϕ defined on the x_i if $(\phi(x_1), \ldots, \phi(x_k)) \in R$.

▶ **Definition 1.** *The* (nonuniform) Constraint Satisfaction Problem (CSP) *associated with language* Γ *over* D *is the problem* $CSP(\Gamma)$ *in which: an instance is a triple* $\mathcal{C} = (X, D, C)$ *where* $X = \{x_1, \ldots, x_n\}$ *is a set of* n *variables and* C *is a set of constraints over* Γ *with variables from* X*. The goal is to decide whether or not there exists a solution, i.e. a mapping* $\phi : X \to D$ *satisfying all of the constraints. We will use* $Sol(\mathcal{C})$ *to denote the set of solutions of* $\mathcal{C}$*.*

Moreover, we follow the algebraic approach to Schaefer's dichotomy result [22] formulated by Jeavons [12] where each class of CSP(Γ) that is polynomial time solvable is associated with a polymorphism of Γ.

▶ **Definition 2.** *An operation* $f : D^m \to D$ *is a* ***polymorphism*** *of a relation* $R \subseteq D^k$ *if for any choice of* m *tuples from* R *(allowing repetitions), it holds that the tuple obtained from these* m *tuples by applying* f *coordinate-wise is in* R*. If this is the case we also say that* f preserves R*, or that* R *is* invariant *or* closed *with respect to* f*. A polymorphism of a constraint language* Γ *is an operation that is a polymorphism of every* $R \in \Gamma$*.*

In this paper we deal with a *majority polymorphism*[13, 2]: for a finite domain D, a ternary operation f is called a majority polymorphism if $f(a, a, b) = f(a, b, a) = f(b, a, a) = a$ for all $a, b \in D$. There is only one majority polymorphism for the Boolean domain, but this is not the case for larger domains. We focus on one of the majority polymorphisms in particular:

▶ **Definition 3.** *The dual discriminator, denoted by* ∇*, is a majority polymorphism such that* $\nabla(a, b, c) = a$ *for pairwise distinct* $a, b, c \in D$*.*

We chose this particular majority polymorphism as there is a general consensus that the dual discriminator is often used as a starting point in many CSP-related classifications [2].

▶ **Example 4.** Consider relations $R_1 = \{(0, 1, 1), (2, 0, 2), (2, 2, 1), (2, 0, 1), (2, 1, 1)\}$ and $R_2 = \{(1, 1), (2, 1)\}$. Observe that both R_1 and R_2 are ∇-closed. Consider an instance $\mathcal{C}$ over $\Gamma = \{R_1, R_2\}$ with constraints $C_1 = R_1(x, y, z)$ and $C_2 = R_2(x, z)$. The assignment ϕ where $\phi(x) = 2, \phi(y) = 0, \phi(z) = 1$ satisfies all constraints.

The well-known Boolean 2-SAT problem is another example of CSP closed under the majority polymorphism.

For a given instance $\mathcal{C}$ of CSP(Γ), the ***combinatorial ideal*** $\mathtt{I}_{\mathcal{C}}$ is defined as the vanishing ideal of the set $Sol(\mathcal{C})$, i.e. $\mathtt{I}_{\mathcal{C}} = \mathbf{I}(Sol(\mathcal{C}))$.We call polynomials of the form $x_i(x_i - 1)(x_i - 2)$ ***domain polynomials***, denoted by $dom(x_i)$, and it is easy to see that they belong to $I_{\mathcal{C}}$ for every $i \in [n]$ as they describe the fact that $Sol(\mathcal{C}) \subseteq D^n$. For a more detailed Ideal-CSP correspondence we refer to A.2.1 of [16].

▶ **Definition 5.** *The* Ideal Membership Problem *associated with language* Γ *is the problem* $IMP(\Gamma)$ *in which the input consists of a polynomial* $f \in \mathbb{F}[X]$ *and a* $CSP(\Gamma)$ *instance* $\mathcal{C} = (X, D, C)$*. The goal is to decide whether* f *lies in the combinatorial ideal* $\mathtt{I}_{\mathcal{C}}$*. We use* $IMP_d(\Gamma)$ *to denote* $IMP(\Gamma)$ *when the input polynomial* f *has degree at most* d*.*

1.2 Our contributions

In this paper we focus on instances $\mathcal{C} = (X = \{x_1, \ldots, x_n\}, D = \{0, 1, 2\}, C)$ of CSP(Γ) where Γ is a language that is closed under the dual discriminator. We identify certain structural properties of the dual discriminator and exploit them in order to characterize varieties as ∇-closed or not. We claim that the reduced Gröbner basis of the combinatorial ideal $I_{\mathcal{C}}$, is a

subset of a "well structured" set $\mathcal{G}$ (see Definition 17) that only depends on the number of variables n, and is of size $O(n^3)$. We prove this by first showing that $I_{\mathcal{C}}$ has a generating set that is a subset of $\mathcal{G}$. It is known that the Buchberger's algorithm [3, 8] is one way to form a Gröbner basis of the ideal from a generating set by computing S-polynomials for every pair of polynomials in the generating set. We then show that polynomials in $\mathcal{G}$ have the property that for any $f, g \in \mathcal{G}$, there is a polynomial in $\mathcal{G}$ that divides $S(f, g)$ and belongs to $I_{\mathcal{C}}$. Since $|\mathcal{G}| = O(n^3)$, we have the following main results:

▶ **Theorem 6.** *The reduced Gröbner basis of a combinatorial ideal, whose variety is over the domain $\{0, 1, 2\}$ and is closed under the dual discriminator polymorphism, is a subset of $\mathcal{G}$ and can be computed in polynomial time assuming the graded lexicographic ordering of monomials.*

This gives us proof of the following:

▶ **Corollary 7.** *$IMP_d(\Gamma)$ can be solved in polynomial time for $d = O(1)$ if the dual discriminator is a polymorphism of Γ.*

Overview of the proof structure of this paper: A high level description of the proof structure is as follows. We first begin by observing in Section 2 that every ∇-closed variety V of arity n can be written as the intersection of varieties $\cap V_{i,j}$ where each $V_{i,j}$ is the projection of V onto its i-th and j-th coordinates. This implies that we can represent the vanishing ideal of V as a sum of vanishing ideals of each of the projections as $\mathbf{I}(V) = \sum \mathbf{I}(V_{i,j})$ [8]. This prompts us to examine varieties of arity two that are ∇-closed. In Section 3, we find a structural property of such varieties: where we say varieties of arity two are ∇-closed iff they are L-closed (see Definition 10). This allows an easy examination of the (2^9 many) possible varieties of arity two, based on the number of elements in the subset. In each case, we produce a set of polynomials and prove that this is the reduced Gröbner basis of the vanishing ideal of the variety. These polynomials partially make up the set $\mathcal{G}$ (recall that we claim that the reduced Gröbner basis of $I_{\mathcal{C}}$ can only come from $\mathcal{G}$). We claim the remaining polynomials in $\mathcal{G}$ can be obtained by the reduced Gröbner basis of the vanishing ideals of certain varieties of arity three, as explained in Section 4.1.

Thus far we have that the reduced Gröbner basis of each $\mathbf{I}(V_{i,j})$ is a subset of $\mathcal{G}$. In Section 4.2 we prove that the reduced Gröbner basis of $I_{\mathcal{C}} = \mathbf{I}(V) = \sum \mathbf{I}(V_{i,j})$ is also a subset of $\mathcal{G}$. Theorem 18 and Lemma 19 prove that the reduced Gröbner basis of $\mathbf{I}(V_{i,j}) + \mathbf{I}(V_{k,l})$ is a subset of $\mathcal{G}$ for any $i, j, k, l \in [n]$. Since we prove that the reduced Gröbner basis of $\sum \mathbf{I}(V_{i,j})$ is a subset of $\mathcal{G}$, and $|\mathcal{G}| = O(n^3)$, proof of Theorem 6 follows.

2 Structure of ∇-closed varieties

In this section we explain a certain geometric structure of majority closed varieties.

▶ **Definition 8.** *Let V be a variety of arity n. Let the n-arity variety $V_{i,j}$ $(1 \leq i < j \leq n)$ be the projection of V along its (i, j)th coordinates such that the variety along the rest of the coordinates is D^{n-2}.*

For example, let $V = \{(0, 1, 2), (1, 1, 2)\}$. Then $V_{1,2} = \{(0, 1, 0), (0, 1, 1), (0, 1, 2), (1, 1, 0), (1, 1, 1), (1, 1, 2)\}$, $V_{1,3} = \{(0, 0, 2), (0, 1, 2), (0, 2, 2), (1, 0, 2), (1, 1, 2), (1, 2, 2)\}$ and $V_{2,3} = \{(0, 1, 2), (1, 1, 2), (2, 1, 2)\}$.

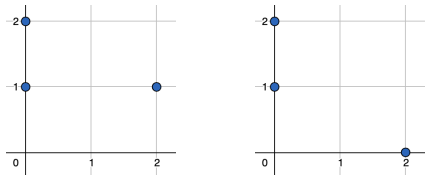
We now state a result proved in [13] which is a structural property of any majority polymorphism.

▶ **Lemma 9** (Proposition 5.4 [13]). *If a variety V of arity $n \geq 2$ is closed under any majority polymorphism then $V = \bigcap_{i<j} V_{i,j}$.*

Any variety $V_{i,j}$ can be represented by using a two dimensional grid with $|D|$ rows and columns, where every point (a, b) in the grid corresponds to the tuples in $V_{i,j}$ whose ith and jth coordinates are (a, b). Note that the other coordinates take all possible values from D. For example, Figure 1 shows two varieties $\{(0,1),(0,2),(2,1)\}$ and $\{(0,1),(0,2),(2,0)\}$. This allows us to introduce the following important geometric view of ∇-closed varieties.

▶ **Definition 10.** *Consider D^2 as a two dimensional grid with $|D|$ rows and columns. Let V be a variety arity 2 with at least three elements such that two of its elements have the same row (/column) and the third is in a different row and in a column different from the first two. We say V is L-closed if for any such three elements, V contains the element that shares the same row (/column) as the first two and the same column (/row) as the third. Varieties containing less than three elements are trivially L-closed.*

See Figure 1 for examples.



(a) L-closed **(b)** Not L-closed

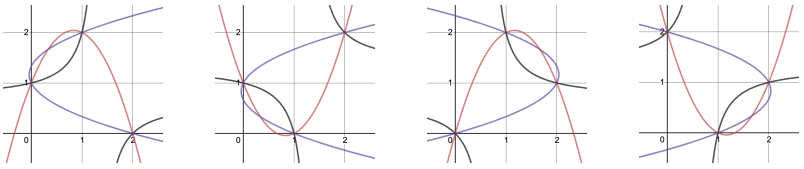
Figure 1 L-closedness.

▶ **Lemma 11.** *A variety V of arity 2 is ∇-closed iff it is L-closed.*

Proof. If V is not L-closed, then without loss of generality it contains three elements of the form $(a,0),(a,1),(d,2)$ where $a, d \in D$, $a \neq d$ and $(a,2) \notin V$. Then $\nabla((d,2),(a,1),(a,0)) = (a,2) \notin V$ (see Definition 3). Hence V is not ∇-closed. Suppose V is not ∇-closed, then it contains three elements whose majority is not in V. If the first coordinates are all distinct and so are the second, then the majority of the three elements is one of the three, a contradiction, hence there are at least two elements which agree on one coordinate. Without loss of generality, we can assume that at least two elements agree on the first coordinate. Let the three elements be $(a,b),(a,c)$ and (d,e) where $a,b,c,d,e \in D$ and $b \neq c$. $d \neq a$ else the majority of the three elements is one of them. The first coordinate of the majority is a considering any order of the three elements. $e \neq b$, else the majority is (a,b), which is in V, a contradiction. Similarly, $e \neq c$, so b, c, e are distinct. Then $\nabla((d,e),(a,b),(a,c)) = (a,e) \notin V$ and hence V is not L-closed. ◀

3 Polynomials that describe ∇-closed varieties of arity two

Suppose V is a ∇-closed variety of arity two. This section provides the reduced Gröbner basis for every possibility of $\mathbf{I}(V)$ based on the number of tuples the variety can contain. Let the first coordinate of each tuple correspond to the variable x, the second to y with $x > y$ and we assume graded lexicographic ordering. We provide a set of generators $G = \{f_1, f_2, \ldots, f_s\}$ such that it is easy to see that $\mathbf{V}(\langle G \rangle) = V$ implies $\langle G \rangle \subseteq \mathbf{I}(V)$. We then prove that *(i)* $\langle G \rangle = \mathbf{I}(V)$ (i.e., $\langle G \rangle$ is a radical ideal) and *(ii)* G is a Gröbner basis of $\mathbf{I}(V)$.



(a) P_1 **(b)** P_2 **(c)** P_3 **(d)** P_4

Figure 2 Polynomials describing non-linear varieties with three tuples with no shared coordinates.

We prove this by showing that for all $f \in \mathbf{I}(V)$, we have $f|_G = 0$. We use $f|_G$ to denote the normal form of f, i.e. the remainder of the division of f by polynomials of G (in any order) such that no polynomial in G can further divide the remainder. Clearly $\forall f \in \mathbf{I}(V)$ if we have $f|_G = 0$ then *(i)* holds because we can express $f = \sum_{i=1}^{s} h_i f_i$ where we obtain h_i by dividing f by the ordered tuple in G. *(ii)* also holds because $f|_G$ generalises $S(f_i, f_j)|_G$ (see Buchberger's criterion in [8] for more details). We let $f|_G = p(x, y)$ in the following cases. We observe that in the set G, no leading monomial of f_i should divide any term of p. Since $p \in \mathbf{I}(V)$, we use the fact that $p(a, b) = 0\, \forall (a, b) \in V$ to prove that p is the zero polynomial. Once proved that $p = 0$, the reader can see that G is actually a reduced Gröbner basis as no leading monomial of f_i will divide any monomial of f_j $(i \neq j)$. In what follows below, let Case i represent the case where the variety V contains i tuples.

Case 1: Suppose $V = \{(\alpha, \beta)\}$, $\alpha, \beta \in D$. We propose $G = \{x-\alpha, y-\beta\}$. Clearly, $p(x, y) = 0$ here.

Case 2: Suppose $V = \{(\alpha_1, \beta_1), (\alpha_2, \beta_2)\}$, where $\alpha_1, \beta_1, \alpha_2, \beta_2 \in D$. If $\beta_1 = \beta_2$ then we propose $G = \{y - \beta_1, (x - \alpha_1)(x - \alpha_2)\}$. The leading monomials of polynomials in G are y and x^2, therefore p has to be linear in x. As $p(x) = ax + b = 0\, \forall x \in \{\alpha_1, \alpha_2\}$, we have $p = 0$. If $\beta_1 \neq \beta_2$ we simply take the line passing through the points of V, i.e, $G = \{x - \alpha_2 - (y - \beta_2)(\alpha_1 - \alpha_2)/(\beta_1 - \beta_2), (y - \beta_1)(y - \beta_2)\}$. The reasoning for the Gröbner basis remains the same, except that p has to be linear in y.

Case 3: If the three tuples are points that are collinear, then they can be described by one of the following lines: $x - \alpha$, $y - \beta$, $x - y$, $x + y - 2$, where $\alpha, \beta \in D$. They form the reduced Gröbner basis of the vanishing ideal along with the domain polynomial in y (except for $y - \beta$ in which case we need the domain polynomial in x): suppose the variety in question is described by a line with x as the leading monomial. Then p must not contain x and y^3. This implies that p is a polynomial in y with degree at most 2. But since the line passes through three points, $p(y) = ay^2 + by + c = 0\, \forall y \in D$ implies $p = 0$.

Suppose the three points are non-collinear in such a way that no two points share neither the first nor the second coordinates. Then there are 4 possibilities of such an arrangement and all are ∇-closed (see intersection points of the polynomials in Figure 2): $V_1 = \{(0, 1), (1, 2), (2, 0)\}$, $V_2 = \{(0, 1), (1, 0), (2, 2)\}$, $V_3 = \{(0, 0), (1, 2), (2, 1)\}$ and $V_4 = \{(0, 2), (1, 0), (2, 1)\}$.

The reduced Gröbner basis of the vanishing ideal of V_i is $\{P_i(x, y)\}$ where

$$
\begin{aligned}
P_1(x, y) &:= x^2 - \tfrac{5}{3}x + \tfrac{2}{3}y - \tfrac{2}{3},\ \ xy - \tfrac{2}{3}x - \tfrac{4}{3}y + \tfrac{4}{3},\ \ y^2 - \tfrac{2}{3}x - \tfrac{7}{3}y + \tfrac{4}{3} \\
P_2(x, y) &:= x^2 - \tfrac{5}{3}x - \tfrac{2}{3}y + \tfrac{2}{3},\ \ xy - \tfrac{4}{3}x - \tfrac{4}{3}y + \tfrac{4}{3},\ \ y^2 - \tfrac{2}{3}x - \tfrac{5}{3}y + \tfrac{2}{3} \\
P_3(x, y) &:= x^2 - \tfrac{7}{3}x + \tfrac{2}{3}y,\ \ xy - \tfrac{2}{3}x - \tfrac{2}{3}y,\ \ y^2 + \tfrac{2}{3}x - \tfrac{7}{3}y \\
P_4(x, y) &:= P_1(y, x)
\end{aligned}
$$

In each case, the polynomial with leading monomial x^2, xy, y^2 is denoted by the curve in red, black and purple respectively. It is easy to see that these are the reduced Gröbner

basis, because p cannot contain the leading monomials x^2, xy, y^2, hence can only be linear in x, y. But the fact that p is a line that has 3 non-linear solutions would imply $p(x, y) = 0$.

The only case that is left to consider which is L-closed is if the three points are non-collinear but of the form $V = \{(\alpha_1, \beta_1), (\alpha_1, \beta_2), (\alpha_2, \beta_2)\}$ where $\alpha_1, \beta_1, \alpha_2, \beta_2 \in D$. In this case, $G = \{(x - \alpha_1)(x - \alpha_2), (y - \beta_1)(y - \beta_2), (x - \alpha_1)(y - \beta_2)\}$. The reasoning behind why G is the reduced Gröbner basis is the same as the one above. This concludes Case 3.

In the following cases, we need to consider specifically the arrangement of points which are ∇-closed. Let C_i ($/R_i$), be the set of points of the variety whose x ($/y$) coordinate is i, where $i \in D$. Suppose $\alpha_1, \alpha_2, \alpha_3 \in D$ and are all distinct.

Case 4: We claim that such a variety can be described by the following polynomials: $(x - \alpha)(x - \beta)$, $(x - \alpha)(y - \beta)$, $(y - \alpha)(y - \beta)$.

1. $|C_{\alpha_1}| = 3, |C_{\alpha_2}| = 1$. Then $G = \{(x - \alpha_1)(x - \alpha_2), (x - \alpha_1)(y - \beta), dom(y)\}$ where the point in C_{α_2} has $y-$coordinate β. Now p can be written as $p(x, y) = yp_1(y) + p_2(x)$ where $deg(p_1), deg(p_2) \leq 1$. We have $p(x, y) = 0\ \forall (x, y) \in V$. Since $(\alpha_1, 0) \in V$, $p_2(\alpha_1) = 0$. Since all points of C_{α_1} are in V and $yp_1(y)$ is at most quadratic in y, we now have $yp_1(y) = 0\ \forall y \in D \iff p_1 = 0$. Now $p(x, y) = p_2(x)$, but both α_1, α_2 satisfy p_2 and p_2 is linear, which implies $p_2 = 0$ and hence $p(x, y) = 0$.
2. $|C_{\alpha_1}| = 2, |C_{\alpha_2}| = 2$. This case is L-closed only if the elements in C_{α_1} and C_{α_2} lie on the same rows, say β_1 and β_2. Then, $G = \{(x - \alpha_1)(x - \alpha_2), (y - \beta_1)(y - \beta_2)\}$. Now p can be written as $p(x, y) = xp_1(y) + p_2(y)$ where $deg(p_1), deg(p_2) \leq 1$ and $p(x, y) = 0\ \forall (x, y) \in V$. Since $(\alpha_1, \beta_1), (\alpha_1, \beta_2) \in V$, $p_2(\beta_i) = -\alpha_1 p_1(\beta_i)$ for $i = 1, 2$. Since $(\alpha_2, \beta_1), (\alpha_2, \beta_2) \in V$, $p_2(\beta_i) = -\alpha_2 p_1(\beta_i)$ for $i = 1, 2$. Hence we have $(\alpha_1 - \alpha_2)p_1(\beta_i) = 0$ implies $p_1(\beta_i) = 0$ for $i = 1, 2$ because $\alpha_1 \neq \alpha_2$. Since p_1 is linear, this implies $p_1 = 0$. Now $p(x, y) = p_2(y)$, but both β_1, β_2 satisfy p_2 and p_2 is linear, which implies $p_2 = 0$ and hence $p(x, y) = 0$.
3. $|C_{\alpha_1}| = 2, |C_{\alpha_2}| = |C_{\alpha_3}| = 1$. In keeping with L-closedness, three of the points must lie in the same row, and is hence similar to the first point.

In the following cases, since it is easy to prove, we simply state the polynomials that form the reduced Gröbner basis for the only possible ∇-closed varieties.

Case 5: The ∇-closed varieties are specifically those whose points lie on one horizontal and one vertical line, hence $G = \{(x - \alpha)(y - \beta), dom(x), dom(y)\}$.

Case 6: The ∇-closed varieties are specifically those whose points lie on two vertical or two horizontal lines, hence G is either $\{(x - \alpha)(x - \beta), dom(y)\}$ or $\{(y - \alpha)(y - \beta), dom(x)\}$ for distinct α, β.

Cases 7 and 8 can similarly be examined to see that there are no arrangements that are ∇-closed. Case 9 implies $\mathbf{I}(V) = \langle dom(x), dom(y)\rangle$. This proves the following lemma:

▶ **Lemma 12.** *The vanishing ideal of a ∇-closed variety of arity 2 has reduced Gröbner basis which is polynomial in size. Specifically, the polynomials from the basis are of the form $x_i - \alpha$, $x_i - \alpha_2 - (x_j - \beta_2)(\alpha_1 - \alpha_2)/(\beta_1 - \beta_2)$ where $\alpha_1 \neq \alpha_2$ and $\beta_1 \neq \beta_2$, $(x_i - \alpha)(x_i - \beta)$, $(x_i - \alpha)(x_j - \beta)$, $x_i(x_i - 1)(x_i - 2)$ or belong to $P_a(x_i, x_j)$ where $\alpha, \alpha_1, \alpha_2, \beta, \beta_1, \beta_2 \in D$ and $a \in [4]$ assuming $x_i > x_j$.*

We can also deduce the following corollary:

▶ **Corollary 13.** *Any polynomial p in up to two variables (say x_i and x_j, $i \neq j$ and $x_i > x_j$) from the polynomials listed in the above lemma belongs to the reduced Gröbner basis of the ideal $\langle p, dom(x_i), dom(x_j)\rangle$.*

The proof follows from the fact that $\langle p, dom(x_i), dom(x_j)\rangle$ has variety that is one of the cases[1] already considered in Lemma 12.

4 Closedness

4.1 Defining the set $\mathcal{G}$

For a ∇-closed variety of arity 2, the reduced Gröbner basis of its vanishing ideal comes from polynomials listed in Lemma 12. These polynomials define a part of the set $\mathcal{G}$ from Theorem 6. Although polynomials from Lemma 12 can generate $\mathbf{I}(V)$ for an arbitrary ∇-closed variety V of arity greater than 2, they need not form the reduced Gröbner basis of $\mathbf{I}(V)$. However, we only need two more polynomials to complete the definition of $\mathcal{G}$. These two polynomials come from two particular ∇-closed varieties of arity 3. It is easy to see from our previous proof strategy that the following holds:

▶ **Lemma 14.** *Consider the ∇-closed varieties $V_1 = \{(0,1,2), (1,2,0), (2,0,1)\}$ and $V_2 = \{(0,2,1), (1,0,0), (2,1,2)\}$ (see Tables 1a and 1c). The reduced Gröbner basis of the vanishing ideal of V_1 is $\{x+y+z-3, P_1(y,z)\}$. Similarly that of V_2 is $\{x+y-z-1, P_3(y,z)\}$ with the ordering $x > y > z$.*

Note that each column of V_1 and V_2 contains all elements of D and the projection along any two columns x_i, x_j is $\mathbf{V}(\{P_a(x_i, x_j)\})$ for some $a \in [4]$.

Table 1 Plausible varieties of $x+y+z-3$ and $x+y-z-1$.

(a) V_1.

x	y	z
0	1	2
1	2	0
2	0	1

(b) V_1'.

x	y	z
0	2	1
1	0	2
2	1	0

(c) V_2.

x	y	z
0	2	1
1	0	0
2	1	2

(d) V_2'.

x	y	z
0	1	0
1	2	2
2	0	1

▶ **Lemma 15.** *If V is of arity 3 and ∇-closed such that $x+y+z-3$ belongs to the reduced Gröbner basis of $\mathbf{I}(V)$, then V is either V_1 or V_1'. Similarly, if $x+y-z-1$ belongs to the reduced Gröbner basis, , then V is either V_2 or V_2'.*

For the case of $x+y+z-3$, the set of points in $|D^3|$ that satisfy $x+y+z-3=0$ is $V_1 \cup V_1' \cup \{(1,1,1)\}$. Using the fact that V is L-closed and $x+y+z-3$ is in the reduced Gröbner basis of $\mathbf{I}(V)$, it can be deduced that V is either V_1 or V_1'. We can see from Lemmas 14 and 15 that the following is true.

▶ **Lemma 16.** *If V is of arity 3 and ∇-closed such that $f \in \{x+y+z-3, x+y-z-1\}$ belongs to the reduced Gröbner basis of $\mathbf{I}(V)$, then the reduced Gröbner basis of $\mathbf{I}(V)$ is $\{f, P_a(y,z)\}$ for some $a \in [4]$ assuming $x > y > z$.*

We now define a set of polynomials $\mathcal{G}$ which we later prove to contain all the polynomials that appear in the reduced Gröbner basis of vanishing ideals of ∇-closed varieties.

[1] For example, considering $p = x - \alpha$ (where $\alpha \in D$), the variety of $\langle p, dom(x), dom(y)\rangle$ is $\{(\alpha,0), (\alpha,1), (\alpha,2)\}$. This variety having three elements implies we are in Case 3 of Lemma 12, from which we can see that the reduced Gröbner basis of $\langle p, dom(x), dom(y)\rangle$ is $\{p, dom(y)\}$.

▶ **Definition 17.** *For distinct $i, j, k \in [n]$, $\alpha, \alpha_1, \alpha_2, \beta, \beta_1, \beta_2 \in D$, $\alpha_1 \neq \alpha_2$ and $\beta_1 \neq \beta_2$, let $\mathcal{G} = \mathcal{D} \cup \mathcal{Q} \cup \mathcal{L} \cup \mathcal{Z}$ where*

$$\begin{aligned}
\mathcal{D} &= \{x_i(x_i-1)(x_i-2) : i \in [n]\} \\
\mathcal{Q} &= \{P_a(x_i, x_j) : i, j \in [n], a \in [4]\} \cup \{(x_i-\alpha)(x_i-\beta) : i \in [n]\} \cup \\
&\qquad \{(x_i-\alpha)(x_j-\beta) : i, j \in [n]\} \\
\mathcal{L} &= \{x_i - \alpha : i \in [n]\} \cup \{x_i - \alpha_2 - (x_j-\beta_2)(\alpha_1-\alpha_2)/(\beta_1-\beta_2) : i, j \in [n]\} \cup \\
&\qquad \{x_i + x_j + x_k - 3 : i, j, k \in [n]\} \cup \{x_i + x_j - x_k - 1 : i, j, k \in [n]\} \\
\mathcal{Z} &= \{0, 1\}.
\end{aligned}$$

4.2 $\mathcal{G}$ contains the reduced Gröbner basis

From Lemmas 9 and 12, we know that for an instance $\mathcal{C}$ of CSP(Γ), where the dual discriminator is a polymorphism of Γ, $\mathcal{I}_\mathcal{C}$ can be described by a set of input polynomials which is a subset of $\mathcal{G}$ as defined in Definition 17. For every $f, g \in \mathcal{G}$, if it were true that $S(f, g)|_{f,g} \in \mathcal{G}$, then we would be able to find a Gröbner basis of $\mathcal{I}_\mathcal{C}$ by using Buchberger's algorithm as explained by Mastrolilli [16]. However, this is true only for the Boolean case, and in order to generalize this to a 3-element domain, we look at $\mathcal{I}_\mathcal{C}$ rather than f and g alone.

The sum of two ideals I and J is defined as the set $I + J$ that contains $f + g$ for every f in I and every g in J [8] (see Ch.4, p.189). Not only is $I + J$ the smallest ideal containing I and J, but the union of the set of generators of I and J generates $I + J$. Subsequently, if $V = Sol(\mathcal{C})$, we see that

$$V = \bigcap_{1 \leq i < j \leq n} V_{i,j} \text{ (see Lemma 9)} \implies \mathbf{I}(V) = \sum_{1 \leq i < j \leq n} \mathbf{I}(V_{i,j}) \tag{1}$$

where the second equality comes from [8] (see Th.4 p.190). Thus the polynomials from Lemma 12 can generate $\mathbf{I}(V) = \mathcal{I}_\mathcal{C}$, but this need not mean that the reduced Gröbner basis of $\mathcal{I}_\mathcal{C}$ also comes from Lemma 12.

One of the crucial elements of this paper is that, given that a polynomial $p \in \mathcal{G}$ belongs to the reduced Gröbner basis of $\mathbf{I}(V)$ for some ∇-closed variety V with arity at least two, we can say with certainty that a few other polynomials from $\mathcal{G}$ belong to $\mathbf{I}(V)$ as well. We list out these polynomials in Table 2. We call p the representative polynomial and denote the list of polynomials that accompany p as $A(p)$ and call them accompanying polynomials. We see that this is true for p with less than three variables from Corollary 13, and for p with exactly three variables from Lemma 16. It also follows that not only do the accompanying polynomials belong to $\mathbf{I}(V)$, but $\{p, A(p)\}$ is the reduced Gröbner basis of $\langle p, A(p)\rangle$.

▶ **Theorem 18.** *Suppose $f, g \in \mathcal{G}$ and $I_f = \langle f, A(f)\rangle$ and $I_g = \langle g, A(g)\rangle$, then the reduced Gröbner basis of $I_f + I_g$ is contained in $\mathcal{G}$.*

Proof. For every pair of $f, g \in \mathcal{G}$, we produce $G \subset \mathcal{G}$ and claim it is the reduced Gröbner basis of $I_f + I_g$. We prove the theorem (as done similarly in section 2) by observing that $\mathbf{V}(\langle G\rangle) = \mathbf{V}(I_f + I_g)$ and proving that *(i)* $\langle G\rangle = I_f + I_g$ (i.e., $\langle G\rangle$ is a radical ideal) and *(ii)* G is the reduced Gröbner basis of $I_f + I_g$. We do this by fixing an order of the elements of G and proving that for all $h \in I_f + I_g$, we have $h|_G = p$ is the zero polynomial.

The case when either f or g is a domain polynomial or 1 is straightforward. So we prove the claim by distinguishing between the following cases:

Table 2 Representative and accompanying polynomials.

Representative polynomial (p)	Accompanying polynomials ($A(p)$)
$dom(x)$ or $dom(y)$	$dom(y)$ or $dom(x)$ respectively
Any polynomial of $P_a(x, y)$	The other two polynomials of $P_a(x, y)$
$(x-\alpha)(x-\beta)$ or $(y-\alpha)(y-\beta)$	$dom(y)$ or $dom(x)$ respectively
$(x-\alpha)(y-\beta)$	$dom(x), dom(y)$
$x-\alpha$ or $y-\alpha$	$dom(y)$ or $dom(x)$ respectively
$x+y-2$ or $x-y$	$dom(y)$
Lines that pass through only $(\alpha_1, \beta_1), (\alpha_2, \beta_2)$	$(y-\beta_1)(y-\beta_2)$
$x+y+z+3$ or $x+y-z-1$	$P_a(y, z)$ for some $a \in [4]$
1	None

1. Case $\mathcal{Q}$: where both $f, g \in \mathcal{Q}$.
2. Case $\mathcal{L}$: where both $f, g \in \mathcal{L}$.
3. Case $\mathcal{Q}$-$\mathcal{L}$: where $f \in \mathcal{Q}$ and $g \in \mathcal{L}$.

The proofs for these cases can be found in the full version of this paper. ◀

For $V = Sol(\mathcal{C})$, using Theorem 18, Equation (1) and a result in [8] (see Cor.3, p.190),

$$\mathbf{I}(V) = \sum_{1 \le i < j \le n} \mathbf{I}(V_{i,j}) \implies \mathbf{I}(V) = \sum_{i=1}^{s} \langle f_i \rangle = \sum_{i=1}^{s} \langle f_i, A(f_i) \rangle$$

where every $f_i \in \mathcal{G}$ since we know the reduced Gröbner basis of each $\mathbf{I}(V_{i,j})$ is a subset of $\mathcal{G}$ from Lemma 12. It is to be noted that it could be possible that $\langle f_i, A(f_i) \rangle = \langle f_j, A(f_j) \rangle$ for $i \neq j$ (this happens when $f_i, f_j \in P_a(x, y)$ and $f_i \neq f_j$). In this case the ideals are retained because the representative polynomials offer different leading monomials which is needed to find the reduced Gröbner basis.

▶ **Lemma 19.** *The reduced Gröbner basis of* $\mathbf{I}(V) = \sum \langle f_i, A(f_i) \rangle$ *is a subset of* $\mathcal{G}$.

Proof. Consider just $\langle f_1, A(f_1) \rangle + \langle f_2, A(f_2) \rangle$. Suppose this ideal has $\{p_1, \ldots, p_u\} \subset \mathcal{G}$ as the reduced Gröbner basis (from Theorem 18). We then replace $\langle f_1, A(f_1) \rangle + \langle f_2, A(f_2) \rangle$ with $\langle p_1, \ldots, p_u \rangle = \sum_{i=1}^{u} \langle p_i, A(p_i) \rangle$.

Thus, for every pair of ideals, we have two representative polynomials and their accompanying polynomials which are always in $\mathcal{G}$. We repeat this process of summing ideals, using Theorem 18 and using accompanying polynomials until we have

$$\mathbf{I}(V) = \sum_{i=1}^{v} \langle q_i, A(q_i) \rangle$$

where the reduced Gröbner basis of $\langle q_i, A(q_i) \rangle + \langle q_j, A(q_j) \rangle$ is a subset of $\{q_1, q_2, \ldots, q_v\}$ for every $i, j \in [v]$. This process terminates as the degrees of the leading monomials do not increase.

We now claim that the reduced Gröbner basis of $\mathbf{I}(V)$ is $\{q_1, \ldots, q_v\}$. We have $\mathbf{I}(V) = \langle q_1, \ldots, q_v, A(q_1), \ldots, A(q_v) \rangle$. We drop those polynomials in $A(q_i)$ that are equal to some q_j. Hence we have $\mathbf{I}(V) = \langle q_1, \ldots, q_v, h_{k_1,1}, h_{k_1,2}, \ldots, h_{k_2,1}, h_{k_2,2}, \ldots, h_{k_r,1}, h_{k_r,2}, \ldots \rangle$ where $k_1, \ldots, k_r \in [v]$ $(r \le v)$ and $h_{k_j,i}$ is in $A(q_{k_j})$. We now prove that $h_{k_j,i}|_{\{q_1,\ldots,q_v\}} = 0$ for $1 \le j \le r$. Since $h_{k_j,i}$ is not equal to any q_m $(m \in [v])$, $h_{k_j,i}$ does not not belong to the reduced Gröbner basis of $\langle q_{k_j}, A(q_{k_j}) \rangle + \langle q_m, A(q_m) \rangle$. Let the reduced Gröbner basis of $\langle q_{k_j}, A(q_{k_j}) \rangle + \langle q_m, A(q_m) \rangle$ be $Q \subseteq \{q_1, \ldots, q_v\}$. Since $h_{k_j,i}$ belongs to the ideal, $h_{k_j,i}|_Q = 0$. Hence we have $\mathbf{I}(V) = \langle q_1, \ldots, q_v \rangle$, and since we have the property that $q_i|_{q_j} = q_i$ for every distinct $i, j \in [v]$, $\{q_1, \ldots, q_v\}$ is the reduced Gröbner basis of $\mathbf{I}(V)$. ◀

By Lemma 19 and Theorem 18, the proof the main theorem follows, which is restated below:

▶ **Theorem.** *The reduced Gröbner basis of a combinatorial ideal, whose variety is over the domain* $\{0, 1, 2\}$ *and is closed under the dual discriminator polymorphism, is a subset of* $\mathcal{G}$ *and can be computed in polynomial time assuming the graded lexicographic ordering of monomials.*

5 Conclusions and Future Work

It is only relatively recently that the solvability of CSP problems in ternary domain was characterized, at least when compared to that of the Boolean domain. There are also fewer polymorphims to deal with in the case of solvabilty of IMP in the Boolean case (for example there is only one majority polymorphism in the Boolean domain when comapared to 3^6 majority polymorphisms in the ternary domain). We have dealt with the IMP of constrained problems with respect to the dual discriminator, which we have mentioned to be a good representative for the general majority polymorphim [2].

In the case for the 3-element domain examined in this paper, $\mathcal{G}$ can be constructed only by looking at ∇-closed varieties of arity 3. We believe this should extend to a general domain as well. So we ask, for the dual discriminator polymorphism and a domain D of size $k = O(1)$, do all possible polynomials in the reduced Gröbner basis of the corresponding ideal come from that of the vanishing ideal of ∇-closed varieties of arity k? This would imply that the combinatorial ideal of problems preserved by the dual discriminator for any finite domain has a Gröbner basis that can be computed in polynomial time. It would certainly be unexpected and interesting if this does not extend to majority polymorphisms in general. This is a step in identifying the borderline of tractability, if it exists, for the general IMP_d. We believe that generalizing the dichotomy results of solvability of the IMP_d for a finite domain is an interesting and challenging goal that we leave as an open problem.

References

1 Libor Barto. The constraint satisfaction problem and universal algebra. *The Bulletin of Symbolic Logic*, 21(3):319–337, 2015. URL: `http://www.jstor.org/stable/43556439`.

2 Libor Barto, Andrei Krokhin, and Ross Willard. Polymorphisms, and How to Use Them. In Andrei Krokhin and Stanislav Zivny, editors, *The Constraint Satisfaction Problem: Complexity and Approximability*, volume 7 of *Dagstuhl Follow-Ups*, pages 1–44. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 2017. `doi:10.4230/DFU.Vol7.15301.1`.

3 Bruno Buchberger. Bruno buchberger's phd thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *Journal of Symbolic Computation*, 41(3):475–511, 2006. Logic, Mathematics and Computer Science: Interactions in honor of Bruno Buchberger (60th birthday). `doi:10.1016/j.jsc.2005.09.007`.

4 Andrei A. Bulatov. A dichotomy theorem for constraint satisfaction problems on a 3-element set. *J. ACM*, 53(1):66–120, January 2006. `doi:10.1145/1120582.1120584`.

5 Andrei A. Bulatov. A dichotomy theorem for nonuniform CSPs (best paper award). In *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017*, pages 319–330, 2017.

6 Andrei A. Bulatov. Constraint satisfaction problems: Complexity and algorithms. *ACM SIGLOG News*, 5(4):4–24, November 2018. `doi:10.1145/3292048.3292050`.

7 Hubie Chen. A rendezvous of logic, complexity, and algebra. *ACM Comput. Surv.*, 42(1):2:1–2:32, December 2009. `doi:10.1145/1592451.1592453`.

8 David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer Publishing Company, Incorporated, 4th edition, 2015.

9 João Gouveia, Pablo A. Parrilo, and Rekha R. Thomas. Theta bodies for polynomial ideals. *SIAM Journal on Optimization*, 20(4):2097–2118, 2010.

10 David Hilbert. Ueber die theorie der algebraischen formen. *Mathematische Annalen*, 36:473–534, 1890. doi:10.1007/BF01208503.

11 David Hilbert. Ueber die vollen invariantensysteme. *Mathematische Annalen*, 42:313–373, 1893. URL: http://eudml.org/doc/157652.

12 Peter Jeavons. On the algebraic structure of combinatorial problems. *Theoretical Computer Science*, 200(1):185–204, 1998. doi:10.1016/S0304-3975(97)00230-2.

13 Peter Jeavons, David Cohen, and Marc Gyssens. Closure properties of constraints. *J. ACM*, 44(4):527–548, July 1997. doi:10.1145/263867.263489.

14 Monique Laurent. Sums of squares, moment matrices and optimization over polynomials. In Mihai Putinar and Seth Sullivant, editors, *Emerging Applications of Algebraic Geometry*, pages 157–270. Springer New York, New York, NY, 2009. doi:10.1007/978-0-387-09686-5_7.

15 László Lovász. On the shannon capacity of a graph. *IEEE Transactions on Information Theory*, 25:1–7, 1979.

16 Monaldo Mastrolilli. The complexity of the ideal membership problem for constrained problems over the boolean domain. In *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '19, pages 456–475, Philadelphia, PA, USA, 2019. Society for Industrial and Applied Mathematics. URL: http://dl.acm.org/citation.cfm?id=3310435.3310464.

17 Ernst W. Mayr. Membership in polynomial ideals over q is exponential space complete. In B. Monien and R. Cori, editors, *STACS 89*, pages 400–406, Berlin, Heidelberg, 1989. Springer Berlin Heidelberg.

18 Ernst W. Mayr and Albert R. Meyer. The complexity of the word problems for commutative semigroups and polynomial ideals. *Advances in Mathematics*, 46(3):305–329, 1982. doi:10.1016/0001-8708(82)90048-2.

19 Ernst W. Mayr and Stefan Toman. Complexity of membership problems of different types of polynomial ideals. In Gebhard Böckle, Wolfram Decker, and Gunter Malle, editors, *Algorithmic and Experimental Methods in Algebra, Geometry, and Number Theory*, pages 481–493. Springer International Publishing, Cham, 2017. doi:10.1007/978-3-319-70566-8_20.

20 Ryan O'Donnell. SOS Is Not Obviously Automatizable, Even Approximately. In Christos H. Papadimitriou, editor, *8th Innovations in Theoretical Computer Science Conference (ITCS 2017)*, volume 67 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 59:1–59:10, Dagstuhl, Germany, 2017. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.ITCS.2017.59.

21 Prasad Raghavendra and Benjamin Weitz. On the Bit Complexity of Sum-of-Squares Proofs. In Ioannis Chatzigiannakis, Piotr Indyk, Fabian Kuhn, and Anca Muscholl, editors, *44th International Colloquium on Automata, Languages, and Programming (ICALP 2017)*, volume 80 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 80:1–80:13, Dagstuhl, Germany, 2017. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.ICALP.2017.80.

22 Thomas J. Schaefer. The complexity of satisfiability problems. In *Proceedings of the Tenth Annual ACM Symposium on Theory of Computing*, STOC '78, pages 216–226, New York, NY, USA, 1978. ACM. doi:10.1145/800133.804350.

23 Amir Shpilka. Recent results on polynomial identity testing. In Alexander Kulikov and Nikolay Vereshchagin, editors, *Computer Science – Theory and Applications*, pages 397–400, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

24 Dmitriy Zhuk. A proof of CSP dichotomy conjecture (best paper award). In *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017*, pages 331–342, 2017. doi:10.1109/FOCS.2017.38.