The Ideal-CSP Correspondence

M.R.C. van Dongen
Cork Constraint Computation Centre
Computer Science Department
University College Cork
Cork, Ireland

September 28, 2002

Abstract

Constraint Satisfaction Problems (CSPs) are widely used to state, represent and solve problems from a wide class that includes the n-queens problem, graph colouring, circuit verification, type inference, scheduling, and many more. Polynomial ideals are a useful tool for the expression and solution of many problems occurring in mathematics, science and engineering. Ideals can be used for the decision of the satisfiability of systems of equations, for variable elimination, and so on. Gröbner basis theory provides techniques to solve each of the afforementioned problems. Varieties are sets consisting of the common zeros of polynomial ideals. As such varieties and polynomial ideals are intimately related. Certain kinds of varieties and finite constraints are also intimately related. Finite constraints, as will be pointed out in this paper, are in essence varieties. This allows for the translation of CSPs to polynomial ideals, thereby allowing for the application of algorithms from Gröbner basis theory. We shall present a 3-step algorithm to transform any CSP to an equivalent CSP which is in *directionally solved form* with respect to an elimination order. Each step heavily relies on the relationship between constraints, varieties, ideals, and Gröbner bases. First, the CSP is transformed to a polynomial ideal. Next, the ideal is transformed to its reduce Gröbner basis with respect to a lexicographical term order. Finally, the Gröbner basis is transformed to a CSP. With a small change the algorithm can be used to compute an output CSP which is in solved form with respect to all elimination orders.

1 Introduction

Constraint Satisfaction Problems (CSPs) are widely used to state, represent and solve problems from a class which includes the n-queens problem, graph colouring, circuit verification, type inference, scheduling, and many more.

Polynomial ideals are a useful tool for the expression, representation and solution of many problems (most of which are of a continuous nature) occurring in mathematics, science and engineering. They are used for the decision of the satisfiability of systems of simultaneous equations, for variable elimination, and so on. Varieties are sets consisting of the common zeros of polynomial ideals. As such, they are intimately related to polynomial ideals. It will turn out that there is also a close relationship between certain kinds of varieties and finite constraints. Finite constraints, as we shall see in this paper, are in essence varieties. This allows for the translation of constraints to polynomial ideals, thereby allowing for the application of algorithms from ideal theory. The existence of the translation technique also means that it is possible to *integrate* finite CSPs and problems of a continuous nature as opposed to the more common approach to treat them seperately. This possibility, being interesting in itself, will not be further explored in this paper.

Gröbner Basis Theory provides algorithms for each of the following problems in polynomial ideal theory:

ideal membership is a given polynomial a member of a given ideal?

consistency problem do the members of a given ideal have common zeros?

variable elimination eliminate certain variables from a given ideal.

counting if a given ideal is zero-dimensional, i.e. if the members of the ideal have a non-zero finite number of common zeros, how many such common zeros are there?

In this paper we shall study the relationship between on the one hand CSPs and on the other hand varieties, polynomial ideals and Gröbner bases. We shall use this relationship to transform any CSP with extensional constraints to an *equivalent* CSP which is in *directionally solved form* with respect to a given variable ordering and to an equivalent CSP which is in *globally solved form.* Here, two CSPs are equivalent if their solutions are the same. Both kinds of output CSPs guarantee backtrack-free search and guarantee that all solutions can be found without encountering “dead-ends.”

The general construction is as follows. Given an input constraint satisfaction problem $\mathcal{C}$ with variables X we compute a generating system of the radical ideal $I \subseteq k[X]$ whose variety is equal to the solution set of $\mathcal{C}$. Next, we compute the reduced Gröbner basis G of I with respect to a lexicographical term order $\prec$ and transform G to a constraint satisfaction problem $\mathcal{C}'$ which is equivalent to $\mathcal{C}$. The properties of the Gröbner basis ensure that $\mathcal{C}'$ is in directionally solved form with respect to $\prec$. With a minor change, the algorithm can also be used to compute CSPs which are solved with respect to all elimination orders.

The remainder of this paper is as follows. In Section 2 we shall recall the main definitions from Constraint Satisfaction Theory and its related literature. This is followed by Section 3 where we shall briefly recall the related mathematics including Gröbner Basis Theory. In Section 4 we shall discuss the relationship between constraints, varieties and ideals. We shall present the algorithm for the computation of CSPs in directionally solved form in Section 5. We shall apply the algorithm to a toy problem in Section 6. Concluding remarks and suggestions for future work will be provided in Section 7.

2 Constraint Satisfaction

For the remainder of this paper let $X = \{\, x_1, \ldots, x_n \,\}$ be a non-empty set of variables. Associated with each variable x_i in X is its domain $D(x_i)$ whose cardinality is finite. Throughout this paper we shall assume that x_i lexicographically precedes x_j if and only if i lexicographically precedes j.

Let $S = \{\, x_{i_1}, \ldots, x_{i_m} \,\}$ be a set of variables. A constraint C_S on S is a subset of the Cartesian product of the domains of the variables in S. A member of C_S is called an *S-tuple* or an *$(\, x_{i_1}, \ldots, x_{i_m} \,)$-tuple.* Intuitively, each member $(\, v_{i_1}, \ldots, v_{i_m} \,) \in C_S$ plays the role of a simultaneous "assignment" $x_{i_1} = v_{i_1}$, …, $x_{i_m} = v_{i_m}$ which is "allowed" by the constraint. This is formalised by the notion of *satisfiability.* A member of C_S is said to *satisfy* C_S. An assignment to a superset of S is said to satisfy C_S if its projection onto S is a member of C_S.

A *Constraint Satisfaction Problem* (CSP) is a triple $(\, Z, D, C \,)$, where Z is a set of variables, D is a function that maps each variable in Z to its domain, and C is a set containing constraints on non-empty subsets of Z. Without loss of generality we may assume that every variable of a CSP is constrained by at least one of its constraints.

Let $\mathcal{C} = (\, X, D, C \,)$ be a CSP, and let Z be a set of variables such that $X \subseteq Z$. A Z-tuple is said to *satisfy* $\mathcal{C}$ if it satisfies each of the constraints in C. $\mathcal{C}$ is called *satisfiable* if there is a tuple that satisfies $\mathcal{C}$ and *unsatisfiable* otherwise. A T-tuple is said to S-satisfy $\mathcal{C}$ if it satisfies all constraints $C_S \in C$ for which $S \subseteq T$. A tuple which satisfies a CSP is called a *solution* of that CSP. Two CSPs are called *equivalent* if their solutions are the same.

Definition 1 (CSP in Directionally Solved Form). Let $\mathcal{C} = (\, X, D, C \,)$ be a CSP and let $\prec$ be the ordering on the variables in X such that $x_i \prec x_j \iff i < j$. $\mathcal{C}$ is in *directionally solved form with respect to* $\prec$ if either:

- $\mathcal{C}$ is unsatisfiable and $\emptyset = C_{\{\, x_1 \,\}} \in C$; or

- $\mathcal{C}$ is satisfiable, there is a non-empty constraint $C_{\{\, x_1 \,\}} \in C$, and for all integers j, $1 < j \leq n$, it is true that if $(\, v_1, \ldots, v_{j-1} \,)$ $\{\, 1, \ldots, j-1 \,\}$-satisfies $\mathcal{C}$ then there exists a member $v_j \in D(x_j)$ such that $(\, v_1, \ldots, v_j \,)$ $\{\, 1, \ldots, j \,\}$-satisfies $\mathcal{C}$.

A CSP in directionally solved form can be solved efficiently in the sense that no backtracking is required in the process of finding one of its solutions or deciding that no solution exists. All its solutions can be found without encountering dead-ends by extending partial solutions. If the CSP is unsatisfiable then this can be found out cheaply by inspecting the unary constraint (node-consistency [Mackworth, 1977]) on the least significant variable with respect to $\prec$.

Freuder provides sufficient conditions and an algorithm for backtrack-free search for CSPs whose constraint-graph is a tree [Freuder, 1982]. He generalises this for arbitrary binary CSPs by relating the width of its constraint-graph to its level of $(\, i, j\,)$-consistency [Freuder, 1985]. As observed by Dechter and Pearl weaker properties may also ensure backtrack-free search [Dechter and Pearl, 1988]. They propose directional consistency methods for binary CSPs.

Dechter and Van Beek pose and answer the question of how to compute directionally solved CSPs [Dechter and van Beek, 1995; 1997]. They present an algorithm called DRC (Directional-Relational-Consistency) to transform *any* CSP to an equivalent CSP which is in directionally solved form. Their CSPs are created by the repeated addition of constraints and repeated restriction of constraints by removing those partial solutions that cannot be extended. A CSP is in *globally solved form* if it is in directionally solved form with respect to all variables orders. Dechter and Van Beek also present algorithm ARC (Adaptive-Relational-Consistency) to compute CSPs in globally solved form [Dechter and van Beek, 1995].

3 Related Mathematics

In this section we shall provide a brief introduction to Gröbner Basis Theory and other related mathematical issues upon which we shall rely in the remainder of this paper. It is assumed that the reader is familiar with the notion of a ring, the notion of a field and the notion of a (polynomial) ideal. Readers not familiar with these notions may wish to consult [Cox *et al.*, 1996]. The presentation will be of an informal nature.

The remainder of this section is organised as follows. In Section 3.1 we shall discuss polynomial ideals, varieties and vanishing ideals. In Section 3.2 we shall study Gröbner bases. This is followed by Section 3.3 where we shall study Gröbner basis algorithms. This section is concluded by Section 3.4 where we shall study the relationship between ideals and varieties.

3.1 Introduction to Ideals and Varieties

Let I be an ideal of ring R. A *generating system* of I is a set $F \subseteq I$ such that every $i \in I$ can be written as a sum of the form:

$$i = \sum_{f \in F} \phi_i(f) f,$$

where $\phi_i(\cdot)$ is some function from F to R which has *finite support*, i.e. $\phi_i(\cdot)$ has the property that there are only finitely many $f \in F$ such that $\phi_i(f) \neq 0$. An ideal is said to be *generated* by F if F is a generating system of I. The ideal generated by F will be denoted $\langle\, F \,\rangle$. The ideal generated by $\{\, f_1, \ldots, f_m \,\}$ will also be denoted $\langle\, f_1, \ldots, f_m \,\rangle$.

The *sum* $I + J$ of sets I and J is defined as $I + J = \{\, i + j \,:\, i \in I, j \in J \,\}$. For the remainder of this paper let k be a field. We shall write $k[X]$ or $k[x_1, \ldots, x_n]$ for the polynomial ring with coefficients in k and variables in X.

Let $F \subseteq k[X]$. The *variety* $\mathrm{V}\,(F) \subseteq k^n$ of F is the set containing the common zeros of the members of F. More formally,

$$\mathrm{V}\,(F) = \{\, (\, v_1, \ldots, v_n \,) \in k^n \,:\, F \subseteq \langle\, x_1 - v_1, \ldots, x_n - v_n \,\rangle \,\}\,.$$

Notice that $F \subseteq \langle\, x_1 - v_1, \ldots, x_n - v_n \,\rangle$ if and only if each polynomial $f \in F$ "becomes" zero as a result of substituting $(\, v_1, \ldots, v_n \,)$ for $(\, x_1, \ldots, x_n \,)$ in f.

Besides the notion of the variety of an ideal there is also the notion of the *ideal of a variety*. The ideal of a variety V is denoted $\mathrm{I}\,(V)$. It consists of all polynomials that vanish (i.e. "become" zero) at V. For obvious reasons such ideals are also called *vanishing ideals*. Formally, $\mathrm{I}\,(V) \subseteq k[X]$ is defined as

$$\mathrm{I}\,(V) = \{\, f \in k[X] \,:\, (\forall\, (\, v_1, \ldots, v_n \,) \in V)(f \in \langle\, x_1 - v_1, \ldots, x_n - v_n \,\rangle) \,\}\,.$$

An ideal of a ring is called *proper* if it is a proper subset of that ring. It is called *consistent* if it does not contain 1 and *inconsistent* otherwise. A polynomial ideal is called *zero-dimensional* if it is consistent and its variety has a finite cardinality. The following celebrated theorem relates the consistency of ideals and the cardinality of their varieties. The reader is referred to [Cox *et al.*, 1996, Hilbert's Weak Nullstellensatz] for proof and further details.

Theorem 2 (Hilbert's Weak Nullstellensatz). *Let k be an algebraically closed field and let I be an ideal of $k[X]$, then I is consistent if and only if I is a proper ideal of $k[X]$ if and only if $1 \notin I$ if and only if $\mathrm{V}\,(I) \neq \emptyset$.*

3.2 Introduction to Gröbner Bases

The set $\mathbb{T}_X$ is the set containing all terms (power products) of the members of X. A total order $\prec$ is called a *term order* over $\mathbb{T}_X$ if 1 is its unique smallest element and if it preserves the order that is induced by multiplication, i.e. for all terms t, u, and v it holds that if $u \prec v$ then $tu \prec tv$.

The leading term of a non-zero polynomial $f \in k[X]$ with respect to $\prec$ is its greatest term with respect to $\prec$. The leading term of f with respect to $\prec$ is denoted $\mathrm{lt}_\prec(f)$. The set $\mathrm{terms}(f)$ is the set consisting of the terms of f. A non-zero polynomial is called *monic* if the coefficient of its leading term with respect to $\prec$ is equal to 1. A term-order is called *lexicographical* if it orders terms according to a lexicographical rule. For example, the order $\cdot \ll \cdot$ over $\mathbb{T}_{\{x,y\}}$ such that $x^{a_1}y^{b_1} \ll x^{a_2}y^{b_2}$ if $(b_1 < b_2) \vee (b_1 = b_2 \wedge a_1 < a_2)$, is the lexicographical term order such that x precedes y.

Definition 3 (Gröbner Basis). Let $I \subseteq k[X]$ be an ideal and let $\prec$ be a term order. A set $G \subseteq I \setminus \{0\}$ is called a *Gröbner basis* of I with respect to $\prec$ if the cardinality of G is finite and if

$$(\forall f \in I \setminus \{0\})(\exists g \in G)(\operatorname{lt}_\prec(g) \mid \operatorname{lt}_\prec(f)),$$

where $u \mid v$ if u divides v.

A Gröbner basis $G \subseteq I \setminus \{0\}$ of I with respect to $\prec$ is called *reduced* if each of its members is monic and if

$$(\forall g \in G)(\forall f \in G \setminus \{g\})(\forall t \in \operatorname{terms}(f))(\operatorname{lt}_\prec(g) \nmid t).$$

Bruno Buchberger invented an algorithm to compute a (reduced) Gröbner basis of a given ideal with respect to a term order [Becker and Weispfenning, 1993; Cox *et al.*, 1996].

The *reduced terms* of an ideal $I \subseteq k[X]$ with respect to term order $\prec$ are those terms in $\mathbb{T}_X$ that cannot be divided by any of the leading terms of the reduced Gröbner basis of I with respect to $\prec$.

3.3 Gröbner Basis Algorithms

Let $W \subseteq X$ and let I be an ideal of $k[X]$. The ideal $I \cap k[W]$ is called the *elimination ideal* of I with respect to W. Using Gröbner bases the computation of a generating system of $I \cap k[W]$ is easy. The algorithm is as follows. Let $\prec$ be any lexicographical term order such that the variables in W are the least significant ones. Compute a Gröbner basis G of I with respect to $\prec$. Then $G \cap k[W]$ is a generating system of $I \cap k[W]$.

The following theorem provides an algorithm for the detection of zero-dimensional ideals. The reader is referred to [Becker and Weispfenning, 1993, Theorem 6.54 (i) and (iv)] for proof and further details.

Theorem 4 (Triangular Form). *Let I be a proper ideal of $k[X]$ and let $\prec$ be any lexicographical term order on $\mathbb{T}_X$. Then I is zero-dimensional if and only if for each $x_i \in X$ there exists a positive integer α_i such that the reduced Gröbner basis of I with respect to $\prec$ contains a polynomial f such that $\operatorname{lt}_\prec(f) = x_i^{\alpha_i}$.*

Example 5 (Triangular Form). Let $Z = \{x_0, x_1, x_2\}$, and let $I \subset k[Z]$ be the ideal generated by G, where

$$G = \{x_0, x_1 + x_0, x_2 + x_1 + x_0\}.$$

G is a Gröbner basis with respect to the lexicographical term order $\prec$ such that $x_0 \prec x_1 \prec x_2$. It is not difficult to see that I is zero-dimensional and that $\mathrm{V}(I) = \{ (0,0,0) \}$. The leading terms of the members of the Gröbner basis with respect to $\prec$ are given by x_2, x_1 and x_0. For every member x_i of Z the basis contains a polynomial whose leading terms with respect to $\prec$ is of the form x_i^1. By the Triangular Form Theorem I is zero-dimensional.

Another special kind of ideals are *radical* ideals. Radical ideals in $k[x_1, \ldots, x_n]$ and varieties in k^n are closely related. If k is algebraically closed then there is a one-to-one relationship between the two.

Definition 6 (Radical Ideal). A proper ideal I of $k[X]$ is called a *radical* ideal of $k[X]$ if it satisfies the property that:

$$(\forall m \in \mathbb{N} \setminus \{ 0 \})(\forall p \in k[X])(p^m \in I \Longrightarrow p \in I).$$

The *radical* of an ideal I is the ideal $\{ f \in k[X] : (\exists m \in \mathbb{N} \setminus \{ 0 \})(f^m \in I) \}$. The radical of I is denoted $\sqrt{I}$.

A polynomial $f \in k[x] \setminus \{ 0 \}$ is called *irreducible* if $f = gh$ implies that either g or h is a unit. A polynomial in $k[x]$ is called *separable* if it does not have multiple zeros in $K[x]$, where K is the *algebraic closure* of k. A field k is called *perfect* if every irreducible polynomial in $k[x]$ is separable. The field of the complex numbers $\mathbb{C}$ is perfect [Becker and Weispfenning, 1993, p. 311]. Finite fields are also perfect [Becker and Weispfenning, 1993, Corollary 7.73]. The following lemma can be found as [Becker and Weispfenning, 1993, Lemma 8.19].

Lemma 7 (Zero-Dimensional Radical Ideal). *Let $k = \mathbb{C}$ and let I be a zero-dimensional ideal of $k[X]$. Furthermore, let f_i be the unique monic polynomial of minimal degree in $I \cap k[x_i]$ and let g_i be the square-free part of f_i, for $1 \leq i \leq n$. Then*

$$\sqrt{I} = I + \langle g_1, \ldots, g_n \rangle .$$

Each of the polynomials f_i can be computed by computing a generating system of the elimination ideal $I \cap k[x_i]$.

Further on we shall use the following theorem to determine the cardinality of a CSP. The reader is referred to [Becker and Weispfenning, 1993, Theorem 8.32] for proof and further information.

Theorem 8 (Counting). *Let K be the algebraic closure of field k, let $\prec$ be a term order and let I be a zero-dimensional ideal of $k[x_1, \ldots, x_n]$. The number of common zeros of the members of I in K^n is less than or equal to the number of reduced terms of I with respect to $\prec$. If k is perfect and I is radical then equality holds.*

Example 9 (Counting). Let $Z = \{ x, y \}$ and let $\prec$ be any term order such that $x \prec y$. Furthermore, let $g_1 = x^2 - x$, let $g_2 = y - x$, let $G = \{ g_1, g_2 \}$, and let $I = \langle G \rangle$. G is the reduced Gröbner basis of I with respect to $\prec$ and G does not contain 1. By Hilbert's Weak Nullstellensatz I is proper. I contains the square-free polynomial $x(x-1) = x^2 - x \in I \cap k[x]$. I also contains the square-free polynomial

$$\begin{aligned} g_1 + g_2(y + x - 1) &= x^2 - x + (y - x)(y + x - 1) \\ &= x^2 - x + y^2 - x^2 - y + x \\ &= y^2 - y \\ &= y(y-1) \in I \cap k[y]. \end{aligned}$$

It follows from Lemma 7 that I is zero-dimensional and radical. Therefore, Theorem 8 can be applied. The reduced terms of I with respect to $\prec$ can be read off from the Gröbner basis G. They are 1 and x because these are the terms in $\mathbb{T}_Z$ that cannot be divided by any of the leading terms of the members of G with respect to $\prec$. It follows from Theorem 8 that the variety of I contains two members. Indeed, the zeros of x in g_1 are given by 0 and 1 and for each zero of x in g_1 there is exactly one zero for y in g_2. If $x = 0$ then $y = 0$ and if $x = 1$ then $y = 1$. The common zeros of I are $(0, 0)$ and $(1, 1)$. There is one zero for every reduced term of I with respect to $\prec$.

The following theorem can be found in slightly different form in [Cox *et al.*, 1996, Theorem 3, Page 115]. The theorem provides a sufficient condition to guarantee when partial solutions can be extended.

Theorem 10 (Extension). *Let $X = \{ x_1, \ldots, x_n \}$ be a set containing at least two variables, let $W = X \setminus \{ x_n \}$, let $k = \mathbb{C}$, let $F = \{ f_1, \ldots, f_m \} \subset k[X] \setminus \{ 0 \}$, and let $I = \langle F \rangle \subseteq k[X]$. Finally, let g_i be the leading coefficient of x_n in f_i (when f_i is viewed as a polynomial in $k[W][x_n]$), for $1 \leq i \leq m$. If $I \cap k[x_1, \ldots, x_{n-1}] \subseteq \langle x_1 - v_1, \ldots, x_{n-1} - v_{n-1} \rangle$ and $\langle g_1, \ldots, g_m \rangle \not\subseteq \langle x_1 - v_1, \ldots, x_{n-1} - v_{n-1} \rangle$ then there exists $v_n \in k$ such that $I \subseteq \langle x_1 - v_1, \ldots, x_n - v_n \rangle$.*

The Extension Theorem states that every partial solution for $x_1, \ldots, x_{n-1}$ can be extended to a partial solution for $x_1, \ldots, x_n$ if the leading coefficients of x_n of the polynomials in F (when the polynomials are viewed as polynomials in $k[W][x_n]$) do not vanish simultaneously.[1] The reader is referred to [Cox *et al.*, 1996, Theorem 3, Page 115] for proof and further details about the Extension Theorem as well as Elimination Theory.

[1] Note that the Extension Theorem only provides a sufficient condition for extension. It does not state that the extension is impossible if the leading coefficients do vanish simultaneously.

3.4 The Relationship between Ideals and Varieties

The following theorem is important because it provides information about the structure of vanishing ideals. The reader is referred to [Cox *et al.*, 1996, Hilbert's Strong Nullstellensatz, p. 174] for proof and further details.

Theorem 11 (Hilbert's Strong Nullstellensatz). *Let k be an algebraically closed field. If I is an ideal of $k[X]$ then* $\mathrm{I}\left(\mathrm{V}\left(I\right)\right) = \sqrt{I}$.

Hilbert's Strong Nullstellensatz (Theorem 11) relates varieties, ideals, and their radicals. The following theorem provides us with more information about their relationship. The reader is referred to [Cox *et al.*, 1996, Ideal-Variety Correspondence Theorem,p. 175] for proof and further details.

Theorem 12 (Ideal-Variety Correspondence). *Let k be an algebraically closed field, then the maps*

$$\textit{affine varieties} \xrightarrow{\mathrm{I}} \textit{radical ideals}$$

and

$$\textit{radical ideals} \xrightarrow{\mathrm{V}} \textit{affine varieties}$$

are inclusion-reversing bijections which are inverses of each other.

The theorem allows us to transform radical ideals to varieties and back without losing information. We shall frequently make use of this relationship.

Example 13 (Ideal-Variety Correspondence). Let $k = \mathbb{C}$, and let $I = \langle\, x^2(x-1)\,\rangle$, let $J = \langle\, x(x-1)\,\rangle$, and let $K = \langle\, x\,\rangle$ be ideals of $k[x]$. Then $I \subseteq J \subseteq K$, and it follows from the first part of Theorem 12 that $\mathrm{V}\left(I\right) \supseteq \mathrm{V}\left(J\right) \supseteq \mathrm{V}\left(K\right)$. The following demonstrates that this is, indeed, true:

$$\mathrm{V}\left(I\right) = \{\,0,1\,\} \supseteq \{\,0,1\,\} = \mathrm{V}\left(J\right) = \{\,0,1\,\} \supseteq \{\,0\,\} = \mathrm{V}\left(K\right).$$

Note that I is not radical, whereas J and K are. Since $J \subset K$, it follows from the second part of Theorem 12 that $\mathrm{V}\left(J\right) \supset \mathrm{V}\left(K\right)$. The following demonstrates that this is also true:

$$\mathrm{V}\left(J\right) = \{\,0,1\,\} \supset \{\,0\,\} = \mathrm{V}\left(K\right).$$

We shall conclude this section by studying the relationship between intersections and unions of ideals and varieties.

The following is proved in [Cox *et al.*, 1996, Chapter 4.3, Theorem 4].

Theorem 14 (Sum versus Intersection). *If I and J ideals of $k[X]$ then*

$$\mathrm{V}\left(I+J\right) = \mathrm{V}\left(I\right) \cap \mathrm{V}\left(J\right).$$

The following is proved in [Cox *et al.*, 1996, Chapter 4.3, Theorem 15].

Theorem 15 (Intersection versus Union). *If I and J ideals of $k[X]$ then*

$$\mathrm{V}\,(I \cap J) = \mathrm{V}\,(I) \cup \mathrm{V}\,(J)\,.$$

The following is proved in [Cox *et al.*, 1996, Proposition 16, Chapter 4].

Proposition 16 (Radical Ideal Intersection). *If I and J are radical ideals of $k[X]$ then $I \cap J$ is also a radical ideal of $k[X]$.*

The following is proved in [Becker and Weispfenning, 1993, Corollary 6.20].

Theorem 17 (Intersection of Ideals). *Let $I = \{\, I_1, \ldots, I_m \,\}$ be a non-empty set of ideals of $k[X]$. Furthermore, let $Y = \{\, y_1, \ldots, y_m \,\}$ be a set of variables such that Y and X are disjoint. Then*

$$\bigcap_{I_i \in I} I_i = k[X] \cap S,$$

where

$$S = \left\langle\, 1 - \sum_{i=1}^{n} y_i \,\right\rangle + \sum_{i=1}^{n} y_i I_i.$$

With the tools presented so far, this makes it a trivial exercise to compute a generating system of the intersection of a set of ideals. First compute a generating system of S and then use the algorithm sketched at the start of Section 3.3 to eliminate from S the variables that are in Y.

4 Ideals, Varieties, and Constraints

In this section we shall use Theorem 12 (the ideal-variety correspondence) to translate finite constraints to varieties and polynomial ideals and vice versa. We shall see that it will allow us to translate of finite CSPs to polynomial ideals and back. The presentation will be of an informal nature. The reader is referred to [Cox *et al.*, 1996, Chapter 4] for a more formal presentation.[2]

In the following, let $(\, X, D, C \,)$ be a finite CSP. Without loss of generality we shall assume that the domains of the variables in X are subsets of $k = \mathbb{C}$. Finally, let $R = k[X]$ and let $I_R \subseteq k[X]$ denote the R-module of ideal I, i.e. let $I_R = \{\, r \times i \,:\, r \in R, i \in I \,\}$. Note that if I is radical then so is I_R.

The following proposition which was proved in [van Dongen, 2002, Proposition 3.22] will prove itself useful further on.

[2] Note that [Cox *et al.*, 1996, Chapter 4] does not cover constraints but *does* cover the relationship between ideals and varieties in great detail.

Proposition 18 (Radicality). *Let m be a positive integer. For each positive integer i less than or equal to m let X_i be a non-empty set of variables. Furthermore, let $X = \cup_{i=1}^{m} X_i$, let I_i be a zero-dimensional radical ideal of $k[X_i]$ and let R_i be the R-module of I_i, for $1 \leq i \leq m$. Finally, let $J \subseteq k[X]$ be given by*

$$J = \sum_{i=1}^{m} R_i.$$

Then either J is inconsistent or J is a zero-dimensional radical ideal of R.

A proper ideal I of ring R is called a *maximal* ideal of R if $I + J \in \{ I, R \}$ for every ideal J of R. Maximal ideals of $k[X]$ are of the form $\langle x_1 - v_1, \ldots, x_n - v_n \rangle$, for suitably chosen $v_1, \ldots, v_n \in k$. Their varieties are of the form $\{ (v_1, \ldots, v_n) \}$, i.e. each such ideal corresponds to a single point in k^n. Note that maximal ideals of $k[X]$ are radical.

Let $S = \{ x_{i_1}, \ldots, x_{i_m} \}$ be a non-empty set of variables and let C_S be a non-empty constraint. In the following paragraphs we shall "translate" C_S to a generating system of an ideal such that the projection of the variety of this ideal onto S is equal to C_S.

Every $(v_{i_1}, \ldots, v_{i_m}) \in C_S$ corresponds to some point $(v_{i_1}, \ldots, v_{i_m})$ of k^m and hence with the maximal (as well as radical) ideal

$$\langle x_{i_1} - v_{i_1}, \ldots, x_{i_m} - v_{i_m} \rangle \subseteq k[S].$$

C_S can therefore be described as follows:

$$C_S = \bigcup_{(v_{i_1}, \ldots, v_{i_m}) \in C_S} \mathrm{V}\left(\langle x_{i_1} - v_{i_1}, \ldots, x_{i_m} - v_{i_m} \rangle \right). \tag{1}$$

Equation (1) states that C_S is the union of finitely many varieties of k^m. The union of varieties is again a variety. Therefore, C_S is a variety of k^m. Theorem 15 tells us that the union of the varieties of ideals is equal to the variety of the intersection of these ideals. Therefore, Equation (1) is tantamount to:

$$C_S = \mathrm{V}\left(I \right),$$

where $I \subset k[S]$ is given by:

$$I = \bigcap_{v \in C_S} \mathrm{I}\left(\{ v \} \right).$$

I is the intersection of radical ideals. By Proposition 16, I is radical and so is I_R. C_S is non-empty, and by Hilbert's Weak Nullstellensatz (Theorem 2), I is consistent. $\mathrm{V}\left(I \right) = C_S$ and $| \, C_S \, |$ is finite. Therefore, I is zero-dimensional. Let

$V_S = \mathrm{V}\left(I_R\right) \subset k^n$. We shall call V_S the *variety* of C_S. Note that the projection of V_S onto S is equal to C_S.

From now, for every $C_S \in C$, let V_S denote its variety in k^n, i.e. let

$$V_S = \mathrm{V}\left(\bigcap_{(\, v_{i_1},\ldots,v_{i_m}\,)\in C_S} \langle\, x_{i_1} - v_{i_1}, \ldots, x_{i_m} - v_{i_m} \,\rangle_R \right).$$

The set $\mathcal{S} \subset k^n$ of solutions of $(\, X, D, C \,)$ is equal to the intersection of the varieties of the constraints in C.

$$\mathcal{S} = \bigcap_{C_S \in C} V_S. \tag{2}$$

Theorem 14 tells us that the intersection of varieties is equal to the variety of the sum of their ideals. Therefore, Equation (2) is equivalent to

$$\mathcal{S} = \mathrm{V}\left(\sum_{C_S \in C} \mathrm{I}\left(V_S\right) \right). \tag{3}$$

Let $J = \mathrm{I}\left(\mathcal{S}\right) \subseteq k[X]$. Without loss of generality we may assume that $X = \cup_{C_S \in C} S$. By Proposition 18, J is inconsistent or zero-dimensional and radical.

Example 19 (Constraint/Variety/Ideal Relationship). Let $Z = \{\, x, y \,\}$, let $R = k[Z]$, let $D(x) = C_{\{\, x \,\}} = \{\, -2, -1, 0, 1 \,\}$, let $D(y) = C_{\{\, y \,\}} = \{\, 1, 2, 3, 4 \,\}$, let $C_{\{\, x,y \,\}} = \{\, (\, 1, 1 \,), (\, -2, 4 \,) \,\}$ and let $C = \left\{\, C_{\{\, x \,\}}, C_{\{\, y \,\}}, C_{\{\, x,y \,\}} \,\right\}$. Finally, let $\mathcal{C} = (\, Z, D, C \,)$. The variety of $C_{\{\, x \,\}}$ is given by $V_{\{\, x \,\}} = \{\, -2, -1, 0, 1 \,\} \times k$. It is the set of $(\, x, y \,)$-tuples where $x \in \{\, -2, -1, 0, 1 \,\}$ and $y \in k$. By Theorem 15

$$\begin{aligned}
C_{\{\, x \,\}} &= \{\, -2, -1, 0, 1 \,\} \\
&= \mathrm{V}\left(\langle\, x + 2 \,\rangle\right) \cup \mathrm{V}\left(\langle\, x + 1 \,\rangle\right) \cup \mathrm{V}\left(\langle\, x \,\rangle\right) \cup \mathrm{V}\left(\langle\, x - 1 \,\rangle\right) \\
&= \mathrm{V}\left(\langle\, x + 2 \,\rangle \cap \langle\, x + 1 \,\rangle \cap \langle\, x \,\rangle \cap \langle\, x - 1 \,\rangle\right) \\
&= \mathrm{V}\left(\langle\, (x + 2)(x + 1)(x - 0)(x - 1) \,\rangle\right).
\end{aligned}$$

Therefore,

$$V_{\{\, x \,\}} = \mathrm{V}\left(\left\langle\, G_{\{\, x \,\}} \,\right\rangle_R\right) \subset k^2,$$

where $G_{\{\, x \,\}}$ is given by

$$G_{\{\, x \,\}} = \{\, (x + 2)(x + 1)(x - 0)(x - 1) \,\}.$$

Similarly,

$$V_{\{\, y \,\}} = \mathrm{V}\left(\left\langle\, G_{\{\, y \,\}} \,\right\rangle_R\right) \subset k^2,$$

where $G_{\{\, y \,\}}$ is given by

$$G_{\{\, y \,\}} = \{\, (y - 1)(y - 2)(y - 3)(y - 4) \,\}.$$

Again we shall use Theorem 15 to compute a generating system, this time for the ideal of $V_{\{x,y\}}$.

$$\begin{aligned} V_{\{x,y\}} &= \{\,(\,1,1\,)\,,(\,-2,4\,)\,\} \\ &= \mathrm{V}\,(\langle\, x-1, y-1\,\rangle_R \cap \langle\, x+2, y-4\,\rangle_R)\,. \end{aligned}$$

To complete this computation we shall use Theorem 17 to compute the intersection of two ideals. This is done as follows. Let z_1 and z_2 be two new variables and let $\prec$ be the lexicographical term order such that $x \prec y \prec z_1 \prec z_2$. To compute the intersection of $\langle\, x-1, y-1\,\rangle_R$ and $\langle\, x+2, y-4\,\rangle_R$ we compute the reduced Gröbner basis of

$$\langle\, 1-z_1-z_2\,\rangle + z_1\,\langle\, x-1, y-1\,\rangle + z_2\,\langle\, x+2, y-4\,\rangle$$

with respect to $\prec$. This reduced Gröbner basis turns out to be

$$\left\{\, x^2+x-2, y+x-2, z_1 - x/3 - 2/3, z_2 + x/3 - 1/3\,\right\}.$$

Therefore,

$$\langle\, x-1, y-1\,\rangle \cap \langle\, x-2, y+4\,\rangle = \left\langle\, x^2+x-2, y+x-2\,\right\rangle.$$

This allows us to conclude that

$$V_{\{x,y\}} = \mathrm{V}\left(\langle\, G_{\{x,y\}}\,\rangle_R\right), \tag{4}$$

where $G_{\{x,y\}} = \{\, x^2+x-2, y+x-2\,\}$.

Equation (2) states that the solutions $\mathcal{S}$ of $\mathcal{C}$ are given by the intersection of the varieties of the constraints in C. This is equivalent to Equation (3) which states that $\mathcal{S}$ is equal to the variety of the sum of the ideals of the varieties of the constraints in C. Let J be the sum of the ideals of the varieties of the constraints of C, i.e. let $J = \sum_{C_S \in C} \mathrm{I}\,(V_S)$. Furthermore, let $\prec$ be the lexicographical term order, such that $x \prec y$. The Gröbner basis of J with respect to $\prec$ is given by:

$$\left\{\, x^2+x-2, y+x-2\,\right\}.$$

It is the same as the generating system of the ideal of $V_{\{x,y\}}$ from Equation (4). It follows immediately that $\mathcal{S}$ are the solutions of $\mathcal{C}$.

In the previous paragraphs we have demonstrated how to translate a CSP to a generating system of an ideal whose variety is equal to the solutions of the CSP. The translation technique proves the existence of what we shall call the "Ideal-CSP correspondence." The following proposition suggests an obvious algorithm to get back from this generating system to a CSP [van Dongen, 2002].

Proposition 20. *Let $F \subset k[X]$ be a finite set of polynomials. Then there exists an algorithm to compute $\mathrm{V}\,(F) \cap \times_{x_i \in X} D(x_i)$.*

5 Computing CSPs in Directionally Solved Form

This section describes a transformation technique from any CSP with extensional constraints to an equivalent CSP which is in directionally solved form with respect to some ordering on the variables. The resulting CSP corresponds to a reduced Gröbner basis with respect to a lexicographical term order.

In the following, let $(\, X, D, C\,)$ be a finite CSP, let $\prec$ be the lexicographical term order such that $x_1 \prec \cdots \prec x_n$, and let $\mathcal{S}$ denote the solution set of the CSP. It is recalled from the previous section that every constraint C_S corresponds to some variety $V_S \in k^n$. The set of solutions $\mathcal{S}$ of the CSP can be described as the variety of the sum of the ideals of the varieties V_S, i.e.

$$\mathcal{S} = \mathrm{V}\left(\sum_{C_S \in C} \mathrm{I}\,(V_S)\right).$$

The transformation is given by:

1. (a) For each $C_S \in C$ compute a generating system $B_S \subset k[x_1, \ldots, x_n]$ for $\mathrm{I}\,(V_S)$. After this step we have $\mathcal{S} = \mathrm{V}\left(\sum_{C_S \in C} \langle\, B_S\,\rangle\right)$.

   (b) Let $B_X = \bigcup_{C_S \in C} B_S$. After this step we have $\mathcal{S} = \mathrm{V}\,(\langle\, B_X\,\rangle)$.

2. (a) Compute the reduced Gröbner basis G_X of $\langle\, B_X\,\rangle$ with respect to $\prec$. We now have $\mathcal{S} = \mathrm{V}\,(\langle\, G_X\,\rangle)$.

3. (a) For each polynomial g occurring in G_X, let S_g denote its variables. Compute the maximal (with respect to inclusion) subset B'_{S_g} of polynomials in G_X the variables of which are given by S_g. After this step we have $\mathcal{S} = \mathrm{V}\left(\sum_{g \in G_X} \left\langle\, B'_{S_g}\,\right\rangle\right)$.

   (b) If $G_X = \{\, 1\,\}$ then set $C'_{\{\,x_1\,\}} = \emptyset$ and C' to $\left\{\, C'_{\{\,x_1\,\}}\,\right\}$. Otherwise, for each B'_{S_g} computed in the previous step compute:

   $$C'_{S_g} = \mathrm{V}\left(B'_{S_g}\right) \cap \bigtimes{}_{x_i \in S_g} D(x_i),$$

   where $\cdot \times \cdot$ is the Cartesian product operator. Set $C' = \left\{\, C'_{S_g}\ :\ g \in G_X\,\right\}$. Finally, we have $\mathcal{S} = \mathrm{V}\left(\sum_{C'_{S_g} \in C'} \left\langle\, C'{}_{S_g}\,\right\rangle\right)$.

C' is the resulting CSP..

The bases B_S in step 1.a can be computed by intersecting ideals. The constraints C'_{S_g} can be computed with the algorithm suggested by Proposition 20. If $W \neq \emptyset$ is a variety with a finite cardinality, then $I = \langle\, W\,\rangle$ is a zero-dimensional radical ideal. Theorem 10 (Extension Theorem) and Theorem 4 (Triangular

Form Theorem) guarantee that extending non-empty partial solutions of elimination ideals of I must succeed. Similarly, the existence of a unary constraint for the smallest variable is guaranteed. Therefore, the CSP is in directionally solved form with respect to $\prec$.

CSPs which are in globally solved form can be computed as follows. Replace Step (2) by: "Compute a universal Gröbner basis of $\langle B_X \rangle$." Here, a *universal Gröbner basis* of an ideal I is a set which is a Gröbner basis of I with respect to any term order. The interested reader is referred to [Becker and Weispfenning, 1993, pp. 514–515] for a short introduction to universal Gröbner bases and to [Mora and Robbiano, 1988] for more detailed information.

The technique to compute CSPs in solved form work in any field k if k is algebraically closed. Changing from an algebraically closed field to a finite field will not affect any of the results provided that the field is sufficiently large to encode the members of the largest domain. The reasons for this are two-fold. First, it can be shown that finite fields are perfect (See [Becker and Weispfenning, 1993, Corollary 7.3]). Therefore, Lemma 7 remains valid. The second reason is as follows. Our application of theorems (including the Counting Theorem) are specialised for the case where the field of computation is algebraically closed. For the case where the field of computation is finite our ideals are radical by construction and our operations (intersection and addition of ideals) do not introduce zeros "outside" the field.

If p is a prime then $\mathbb{F}_p = \mathbb{Z}/\langle p \rangle$ is a finite field containing p members [Cox *et al.*, 1997, page 359]. Our method remains valid if $k = \mathbb{F}_p[X]$ and p is a small prime greater than or equal to the maximum domain size. This will avoid large (intermediate) coefficients and should speed up the computation significantly.

6 Example Application

In this section we shall use the technique described in the previous section to transform a CSP to its equivalent in directionally solved form

Example 21 (Traffic Lights). The following constraints model a set of German traffic lights and are based on [Hower, 1995].

$$\begin{aligned} C_{\{v_i, p_i, v_{i+1 \bmod 4}, p_{i+1 \bmod 4}\}} &= \{(r,r,g,g), (r_y,r,y,r), (g,g,r,r), (y,r,r_y,r)\}; \\ C_{\{v_i\}} &= \{r,g,r_y,y\}; \\ C_{\{p_i\}} &= \{r,g\}, \end{aligned}$$

for $i \in \{0,1,2,3\}$. The eight variables are given by p_0, p_1, p_2, p_3, v_0, v_1, v_2, and v_3. The variables p_i correspond to pedestrian lights. The remaining variables are vehicle lights. There are four 4-ary constraints $C_{\{v_0,p_0,v_1,p_1\}}$, $C_{\{v_1,p_1,v_2,p_2\}}$, $C_{\{v_2,p_2,v_3,p_3\}}$, $C_{\{v_3,p_3,v_0,p_0\}}$, and eight unary constraints corresponding to a domain of each of the variables. The macro-structure of the CSP is depicted in Figure 1. Every variable x is represented by the circle containing x. The 4-ary constraint C_S is represented by the square which is connected to the variables in S by straight lines. Assume $g = 0$, $r_y = 1$, $y = 2$, $r = 3$. Computing the generating systems for the constraints with the algorithm suggested by Theorem 17 results in the following systems:

$$\begin{aligned}
B_{\{\, v_i, p_i, v_{i+1 \bmod 4}, p_{i+1 \bmod 4}\,\}} &= \{\, v_{i+1 \bmod 4}^4 - 6v_{i+1 \bmod 4}^3 + 11v_{i+1 \bmod 4}^2 - 6v_{i+1 \bmod 4}, \\
&\qquad v_i + v_{i+1 \bmod 4} - 3, \\
&\qquad p_{i+1 \bmod 4} - v_{i+1 \bmod 4}^3 + 6v_{i+1 \bmod 4}^2 - 11v_{i+1 \bmod 4}, \\
&\qquad p_i + v_{i+1 \bmod 4}^3 - 3v_{i+1 \bmod 4}^2 + 2v_{i+1 \bmod 4} - 6\,\}; \\
B_{\{\, v_i \,\}} &= \left\{\, v_i^4 - 6v_i^3 + 11v_i^2 - 6v_i \,\right\}; \\
B_{\{\, p_i \,\}} &= \left\{\, p_i^2 - 3p_i \,\right\},
\end{aligned}$$

for $i \in \{\, 0, 1, 2, 3 \,\}$.

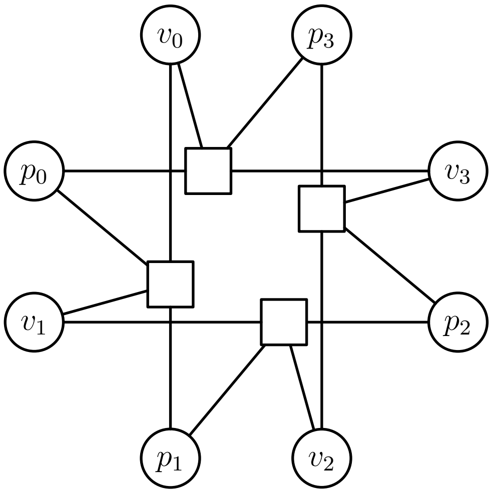

Figure 1: Original CSP.

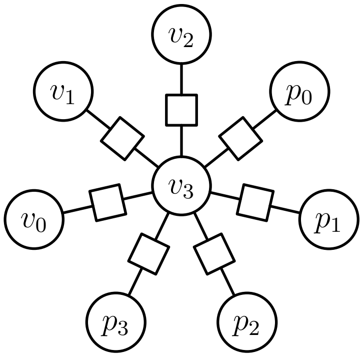

Figure 2: CSP in solved form.

The union B_X of these generating systems consists of 12 binomials and 8 monomials. Let $\prec$ be the lexicographical term order given by $v_3 \prec v_2 \prec v_1 \prec v_0 \prec p_3 \prec p_2 \prec p_1 \prec p_0$. The reduced Gröbner basis G_X of $\langle\, B_X \,\rangle$ with respect to $\prec$ is given by:

$$\begin{aligned}
G_X = \{\, & v_3^4 - 6v_3^3 + 11v_3^2 - 6v_3, v_2 + v_3 - 3, v_1 - v_3, v_0 + v_3 - 3, \\
& 2p_3 - v_3^3 + 6v_3^2 - 11v_3, 2p_2 + v_3^3 - 3v_3^2 + 2v_3 - 6, \\
& 2p_1 - v_3^3 + 6v_3^2 - 11v_3, 2p_0 + v_3^3 - 3v_3^2 + 2v_3 - 6 \,\}.
\end{aligned}$$

The reduced Gröbner basis has revealed a structure which was implicit in the original CSP. The basis is not equal $\{\, 1 \,\}$. By Hilbert's Weak Nullstellensatz $\langle\, G_X \,\rangle$ is consistent and by the Ideal-CSP correspondence the CSP is satisfiable.

Proposition 18 guarantees that $\langle\, G_X \,\rangle$ is either inconsistent or zero-dimensional and radical. Since $\langle\, G_X \,\rangle$ is consistent it is zero-dimensional and radical This allows us to apply the Counting Theorem to count the number of common zeros of $\langle\, G_X \,\rangle$. According to the theorem the number of common zeros of $\langle\, G_X \,\rangle$ is equal to the number of reduced terms of $\langle\, G_X \,\rangle$. The reduced terms of $\langle\, G_X \,\rangle$ with respect to $\prec$ are given by $\{\, 1, v_3, v_3^2, v_3^3 \,\}$. Therefore, there are four common zeros of the members of $\langle\, G_X \,\rangle$. By the Ideal-CSP correspondence there are exactly four solutions to our resulting CSP.

The zeros of each polynomial in G_X correspond to one of the following constraints of the CSP which is in directionally solved form with $\prec$. The macro-structure of this CSP is depicted in Figure 2:

$$\begin{aligned}
C'_{\{\, v_3 \,\}} &= \{\, g, r_y, y, r \,\}\,; \\
C'_{\{\, v_2,v_3 \,\}} &= \{\, (\, r, g \,)\,, (\, y, r_y \,)\,, (\, r_y, y \,)\,, (\, g, r \,) \,\}\,; \\
C'_{\{\, v_1,v_3 \,\}} &= \{\, (\, g, g \,)\,, (\, r_y, r_y \,)\,, (\, y, y \,)\,, (\, r, r \,) \,\}\,; \\
C'_{\{\, v_0,v_3 \,\}} &= \{\, (\, r, g \,)\,, (\, y, r_y \,)\,, (\, r_y, y \,)\,, (\, g, r \,) \,\}\,; \\
C'_{\{\, p_3,v_3 \,\}} &= \{\, (\, g, g \,)\,, (\, r, r_y \,)\,, (\, r, y \,)\,, (\, r, r \,) \,\}\,; \\
C'_{\{\, p_2,v_3 \,\}} &= \{\, (\, r, g \,)\,, (\, r, r_y \,)\,, (\, r, y \,)\,, (\, g, r \,) \,\}\,; \\
C'_{\{\, p_1,v_3 \,\}} &= \{\, (\, g, g \,)\,, (\, r, r_y \,)\,, (\, r, y \,)\,, (\, r, r \,) \,\}\,; \\
C'_{\{\, p_0,v_3 \,\}} &= \{\, (\, r, g \,)\,, (\, r, r_y \,)\,, (\, r, y \,)\,, (\, g, r \,) \,\}\,.
\end{aligned}$$

7 Concluding Remarks

In this paper, we have studied the relationship between ideals, varieties and CSPs. Let X be a set containing n variables, let $\mathcal{C} = (\, X, D, C \,)$ be a CSP and let $C_S \in C$ be a constraint. We have established that C_S is in one-to-one correspondence with some ideal $I_S \subseteq k[X]$. The variety $V_S = \mathrm{V}\,(I_S) \subset k^n$ of I_S is called the *variety of* C_S. The projection of V_S onto S is equal to C_S. Furthermore, the solutions $\mathcal{S}$ of $\mathcal{C}$ are equal to the intersection of the varieties of the constraints in C. $\mathcal{S}$ is also equal to the variety of the sum of the ideals of these varieties. More formally we have established that $\mathcal{S} = \bigcap_{C_S \in C} V_S = \mathrm{V}\left(\sum_{C_S \in C} \mathrm{I}\,(V_S)\right)$. We have coined the relationship between on the one hand ideals and varieties and on the other hand CSPs the Ideal-CSP correspondence.

We have used the Ideal-CSP correspondence to transform a CSP to an equivalent CSP which is in directionally solved form with respect to a given variable ordering. The transformation process consists of three steps. First, the input CSP $(\, X, D, C \,)$ is translated to a generating system of the polynomial ideal $\sum_{C_S \in C} \mathrm{I}\,(V_S)$. Next, the generating system is transformed to its reduced Gröbner basis with respect to the lexicographical term order which agrees with the variable ordering. Finally, the reduced Gröbner basis is transformed to a CSP. Suggestions have been presented on how to improve the algorithm.

Acknowledgement

The Cork Constraint Computation Centre is supported by Science Foundation Ireland.

References

[Becker and Weispfenning, 1993] T. Becker and V. Weispfenning. *Gröbner Bases* A Computational Approach to Commutative Algebra. Graduate Texts in Mathematics. Springer, 1993.

[Cox *et al.*, 1996] D. Cox, J. Little, and J. O'Shea. *Ideals, Varieties, and Algorithms* An Introduction to Computational Algebraic Geometry and Commutative Algebra. Springer, 1996.

[Cox *et al.*, 1997] D. Cox, J. Little, and J. O'Shea. *Using Algebraic Geometry.* Springer, 1997. preprint.

[Dechter and Pearl, 1988] R. Dechter and J. Pearl. Network-based heuristics for constraint-satisfaction problems. *Artificial Intelligence*, 34(1):1–38, 1988.

[Dechter and van Beek, 1995] R. Dechter and P. van Beek. Local and global relational consistency—summary of recent results. In U. Montanari and F. Rossi, editors, *PPCP*, number 976 in Lecture Notes in Computer Science, pages 240–257. Springer, 1995.

[Dechter and van Beek, 1997] R. Dechter and P. van Beek. Local and global relational consistency. *Theoretical Computer Science*, 173(1):283–308, 1997.

[Freuder, 1982] E.C. Freuder. A sufficient condition for backtrack-free search. *Journal of the ACM*, 29(1):24–32, 1982.

[Freuder, 1985] E.C. Freuder. A sufficient condition for backtrack-bounded search. *Journal of the ACM*, 32(4):755–761, 1985.

[Hower, 1995] W. Hower. Constraint satisfaction — algorithms and complexity analysis. *Information Processing Letters*, 55(3):171–178, 1995.

[Mackworth, 1977] A.K. Mackworth. Consistency in networks of relations. *Artificial Intelligence*, 8:99–118, 1977.

[Mora and Robbiano, 1988] T. Mora and L. Robbiano. The Gröbner fan of an ideal. *Journal of Symbolic Computation*, 6(2-3):183–208, 1988.

[van Dongen, 2002] M.R.C. van Dongen. *Constraints, Varieties, and Algorithms.* PhD thesis, Department of Computer Science, University College, Cork, Ireland, 2002.