The Ideal-CSP Correspondence

M.R.C. van Dongen
Compute Science Department UCC
Cork Constraint Computation Centre
Homepage: `http://csweb.ucc.ie/~dongen.html`
Email: `dongen@cs.ucc.ie`

July 19, 2002

Outline

- Ideals and Varieties;
- Gröbner Bases;
- Constraint Satisfaction Problems (CSPs);
- CSPs in Solved Form;
- Summary.

Ideals and Varieties

Let $X = \{x_1, \ldots, x_n\}$ be a set of variables, let k be a field and let $k[X]$ the *polynomial ring* in the variables X over k.

A set $I \subseteq k[X]$ is called an *ideal* of $k[X]$ if

- $0 \in I$;
- $f + g \in I$, for all $f, g \in I$;
- $r \times f \in I$, for all $f \in I$ and $r \in k[X]$.

Let $F = \{ f_1, \ldots, f_m \} \subset k[X]$ be finite. The *ideal* $\langle F \rangle$ *generated* by $F \subseteq k[X]$ is the set

$$\{ r_1 \times f_1 + \cdots + r_m \times f_m \, : \, (r_1, \ldots, r_m) \in k[X]^m \},$$

If I is generated by F then F is called a *generating set* of I.

Thanks to Hilbert we know that if k is a field, then every ideal in $k[X]$ is generated by some finite generating set.

The *variety* $V(F) \subseteq k^n$ of $F \subseteq k[X]$ is the set:

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

The *(vanishing) ideal* $I(V) \subseteq k[X]$ of a variety $V \subseteq k^n$ is the ideal containing all members of $k[X]$ that vanish at V:

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

Gröbner Bases (Term Orders)

Let $\mathbb{T}_X$ denote the set of terms in X. A total order $\prec$ is called a *term order* on $\mathbb{T}_X$ if

- $(\forall t \in \mathbb{T}_X \setminus \{1\})(1 \prec t)$; and
- $(\forall u, v, t \in \mathbb{T}_X)(u \prec v \implies t \times u \prec t \times v)$.

The *leading term* $\mathrm{in}_\prec(f)$ of $f \in k[X] \setminus \{0\}$ w.r.t. term order $\prec$ is the greatest term of f w.r.t. $\prec$.

There are no sequences of the form

$$\cdots \prec t_2 \prec t_1.$$

Gröbner Bases (Definition)

Let $I \subseteq k[X]$ be an ideal and let $\prec$ be a term order. A finite set $G \subseteq k[X] \setminus \{0\}$ is called a *Gröbner basis* of I w.r.t. $\prec$ if it is a generating set of I and

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

where $u|v$ if u divides v.

Applications of Gröbner Bases

- Decide the *ideal membership* problem $f \in I$.
- Decide the *consistency* problem $1 \in I$.
- Compute *elimination ideals*;
- Compute *intersection* of ideals;
- . . . .

Constraints

Let k be a field, let X be a set of variables, let $\emptyset \subset S = \{ x_{i_1}, \ldots, x_{i_m} \} \subseteq X$ and let $R \subseteq k^{i_m}$ be a finite set. Then $\mathcal{C} = (S, R)$ is called a *constraint* over k.

The simultaneous "assignment" $x_{i_1} = v_{i_1}$, . . . , $x_{i_m} = v_{i_m}$ is allowed if $t = (v_{i_1}, \ldots, v_{i_m}) \in R$. If $t \in R$ it is said to *satisfy* $\mathcal{C}$.

In general an assignment to X satisfies a constraint if the projection of the assignment onto the scope of the constraint is in the relation of the constraint.

The Constraint-Ideal Relationship

Let $X = \{ x_1, \ldots, x_n \}$ and let $S = \{ x_{i_1}, \ldots, x_{i_m} \} \subseteq X$ be a non-empty sets of variables. Finally, let $\mathcal{R} = k[X]$ and let $\mathcal{C} = (S, R)$ be a constraint over k.

Every point $(v_{i_1}, \ldots, v_{i_m}) \in k^{i_m}$ is in one-to-one correspondence with the maximal ideal $I = \langle x_{i_1} - v_{i_1}, \ldots, x_{i_m} - v_{i_m} \rangle_{\mathcal{R}}$.

Note that I corresponds to the variety $V(I) \subseteq k^n$.

It is well known that

$$V \cup W = V(I(V) \cap I(W)).$$

Definition 1. *Let* $X = \{ x_1, \ldots, x_n \}$ *and let* $S = \{ x_{i_1}, \ldots, x_{i_m} \} \subseteq X$ *be a non-empty sets of variables. Finally, let* $\mathcal{R} = k[X]$ *and let* $\mathcal{C} = (S, R)$ *be a constraint over* k*. The* ideal, $I(\mathcal{C})$*, of* $\mathcal{C}$ *w.r.t.* X *is given by:*

$$I(\mathcal{C}) = \bigcap_{(r_{i_1},\ldots,r_{i_m}) \in R} \langle x_{i_1} - r_{i_1}, \ldots, x_{i_m} - r_{i_m} \rangle_{\mathcal{R}}.$$

Note that the simultaneous assignment $(x_{i_1}, \ldots, x_{i_m}) = (r_{i_1}, \ldots, r_{i_m})$ satisfies $\mathcal{C}$ if and only if

$$\langle x_{i_1} - r_{i_1}, \ldots, x_{i_m} - r_{i_m} \rangle_{\mathcal{R}} \subseteq I(\mathcal{C}).$$

Let $X = S_1 \cup S_2$. Furthermore, let $\mathcal{C}_1 = (S_1, R_1)$ and $\mathcal{C}_2 = (S_2, R_2)$ be two constraints over k. Then the simultaneous assignment $(x_1, \ldots, x_n) = (t_1, \ldots, t_n)$ satisfies both $\mathcal{C}_1$ and $\mathcal{C}_2$ if and only if

$$\langle x_1 - t_1, \ldots, x_n - t_n \rangle_{\mathcal{R}} \subseteq I(\mathcal{C}_1) + I(\mathcal{C}_2).$$

Computing CSPs in Solved Form

Application: Transform CSPs into "nicer" problems.

1. Transform every constraint $\mathcal{C}$ to a generating set $G_{\mathcal{C}}$ of its ideal;
2. Select a (lexicographical) term order order $\prec$, s.t. $x_1 \prec \cdots \prec x_n$;
3. Compute a Gröbner basis of $\sum_{\mathcal{C} \in \mathsf{CSP}} \langle G_{\mathcal{C}} \rangle$ w.r.t. $\prec$;
4. Transform the Gröbner basis to a CSP.

Four Queens Problem

Position four queens on a four by four chessboard without any queen threatening any other.

variables $X = \{ q_1, q_2, q_3, q_4 \}$;

unary constraints $(\{ q_i \}, \{ 1, 2, 3, 4 \})$, for $1 \leq i \leq 4$;

binary constraint $(\{ q_i, q_j \}, R_{ij})$, for $1 \leq i < j \leq 4$, where

$$R_{ij} = \left\{ (i', j') \in \{1, 2, 3, 4\}^2 : i' \neq j' \wedge |i' - j'| \neq |i - j| \right\}.$$

Computation of the Generating Bases

Let $\mathcal{C}_i = (\{q_i\}, \{1, 2, 3, 4\})$, let $\mathcal{R} = k[q_1, q_2, q_3, q_4]$, and let $G_{\{q_i\}}$ be a generating set of $I(\mathcal{C}_i)$. Then

$$G_{\{q_i\}} = \{(q_i - 1) \times (q_i - 2) \times (q_i - 3) \times (q_i - 4)\}.$$

Using ideal intersection we can compute generating bases for each of the other constraints.

Properties of Solutions Set

If I and J are ideals in $\mathrm{k}[\mathrm{X}]$ then

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

The solutions $\mathcal{S}$ of the problem are given by

$$\mathcal{S} = \bigcap_{\mathcal{C} \in \mathsf{CSP}} \mathrm{V}(\mathrm{I}(\mathcal{C})).$$

Therefore,

$$\mathcal{S} = \mathrm{V}\Big(\sum_{\mathcal{C} \in \mathsf{CSP}} \mathrm{I}(\mathcal{C})\Big).$$

Computation of the Gröbner Basis

Let $\prec$ be the lexicographical term order where $q_4 \prec q_3 \prec q_2 \prec q_1$. The following is a Gröbner basis w.r.t. $\prec$ of the solutions to the four-queens problem.

$$\{\, q_4^2 - 5q_4 + 6,\ q_3 + 3q_4 - 10,\ q_2 - 3q_4 + 5,\ q_1 + q_4 - 5 \,\}\,.$$

Summary

- Constraints are varieties;
- We can translate CSPs to (generating sets of) ideals and back;
- The relationship between CSPs and ideals opens the door for the application of Gröbner basis techniques to CSPs;
- Gröbner bases make explicit the underlying structure of the relationships between the variables that was implicit in the original CSPs.

Questions Anybody?