On Delineability of Varieties in CAD-Based Q E

S. McCallum (Macquarie University) and
C. W. Brown (US Naval Academy)

A key notion in the algorithmic theory of CADs is *delineability*: roughly speaking, the real variety of a single real polynomial $f(x_1, \ldots, x_r)$ is *delineable* on a connected subset $S \subset \mathbb{R}^{r-1}$ if the distinct real roots of $f(p_1, \ldots, p_{r-1}, x_r)$ remain a finite constant in number, and vary continuously, as $(p_1, \ldots, p_{r-1})$ varies in S.

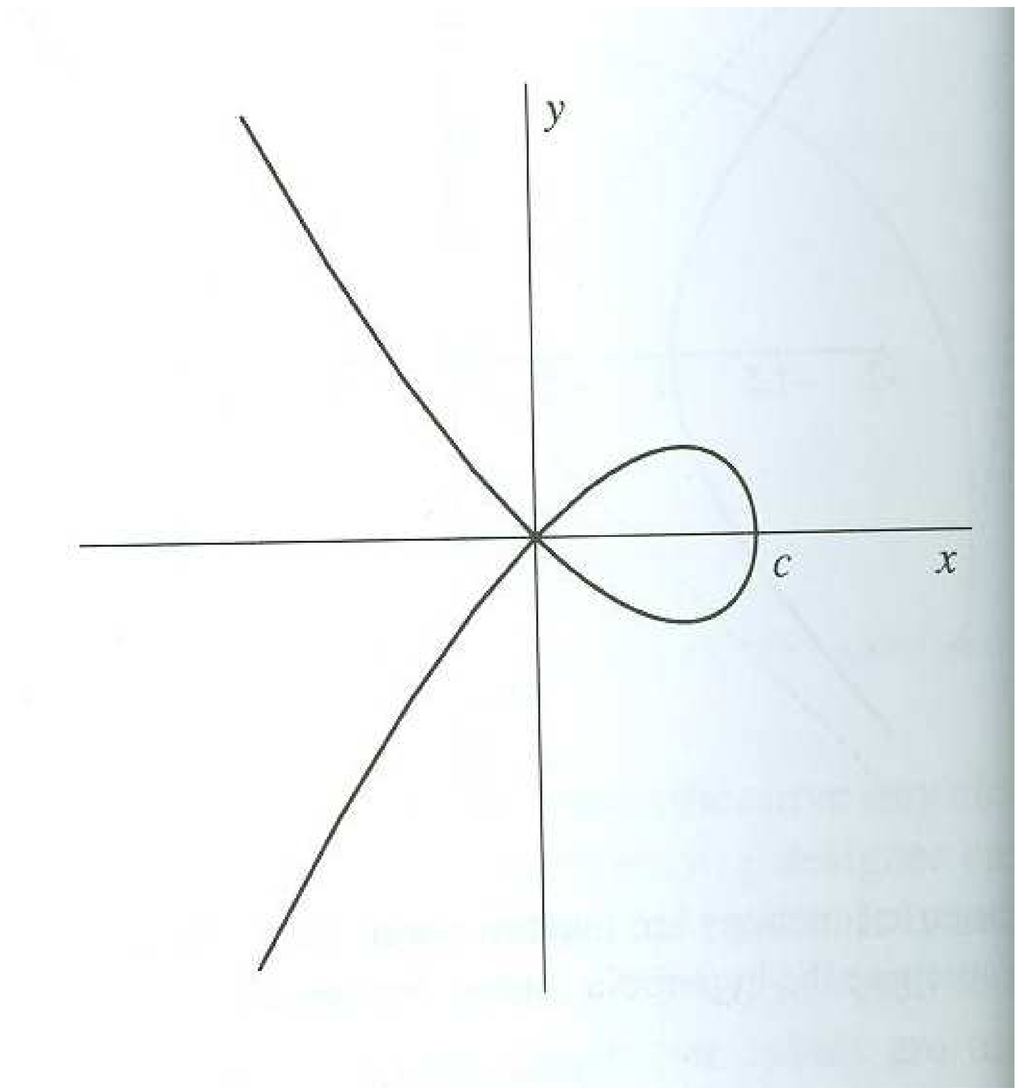
In this talk we propose the more general notion of the delineability of a real variety $V(f_1, \ldots, f_t)$, (where the $f_i \in \mathbb{R}[x_1, \ldots, x_r]$) on a connected subset $S \subset \mathbb{R}^{r-t}$. We
* concentrate on the case $t = 2$;
* prove an analogue of the CAD lifting theorem for this case; and
* sketch a CAD-like algorithm for this case based on this theorem.

Review

Let $c > 0$ be some constant and let

$$r(x, y) = y^2 - cx^2 + x^3.$$

The real algebraic curve $r(x, y) = 0$ is pictured below.



This curve is delineable on $(-\infty, 0)$. It is also delineable on $\{0\}$, $(0, c)$, $\{c\}$ and (c, ∞).

CAD lifting theorem for $r > 1$ (1980s).

Let $f(x_1, \ldots, x_r)$ be squarefree with discriminant $D(x_1 \ldots x_{r-1}) \neq 0$. Let S be a connected submanifold of $\mathbb{R}^{r-1}$ in which f has finite constant degree and D is order-invariant. Then f is delineable on S. (Moreover the real roots define analytic functions with f order-invariant in the graph of each real root function.)

Consequence
The above result suggests a recursive strategy to construct a CAD $\mathcal{D}$ of $\mathbb{R}^r$ relative to some given r-variate f. Namely:
* if $r = 1$ construct $\mathcal{D}$ directly using real root isolation;
* if $r > 1$ recursively construct CAD $\mathcal{D}'$ of $\mathbb{R}^{r-1}$ relative to $D = \text{discr}(f)$ (together with enough coefficients of f), then "lift" $\mathcal{D}'$ to $\mathcal{D}$ using lifting theorem.

Note relatively recent works (ISSACs '99, '01, '05) on using equational constraints to simplify projection (elimination) steps.

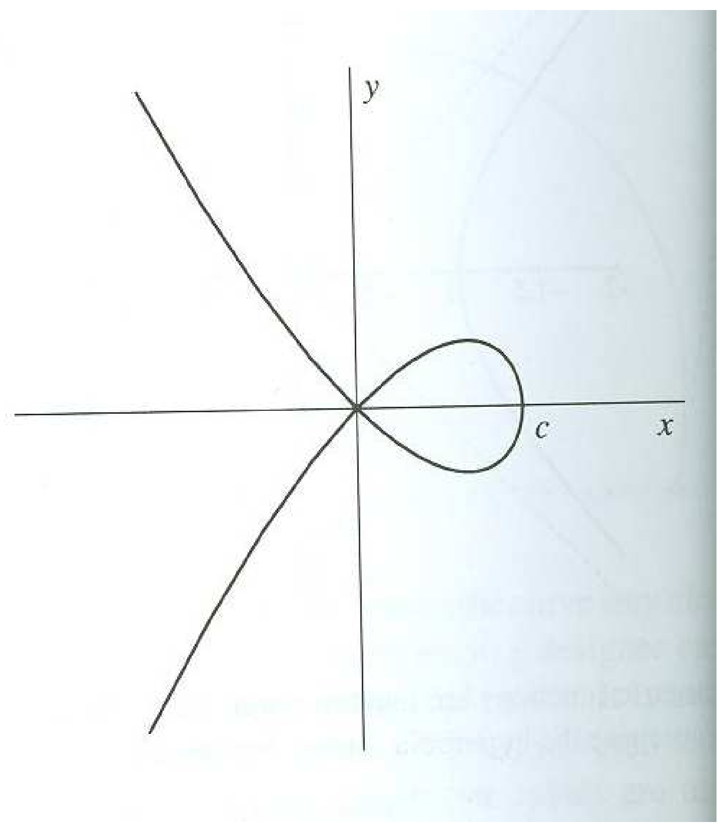
In the present paper we shall speak of the delineability of a real variety defined by a system $f_1, \ldots, f_t$. We shall concentrate on the case $t = 2$. We'll try to extend the CAD lifting theorem for this case, and pursue an algorithmic consequence.

We denote the $(r-2)$-tuple $(x_1, \ldots, x_{r-2})$ by x; x_{r-1} and x_r by y and z, resp.; and f_1 and f_2 by f and g, resp.

We say that the real variety $V(f, g)$ is *delineable* on $S \subset \mathbb{R}^{r-2}$ (with respect to y and z) if the distinct real common zeros of $f(p, y, z)$ and $g(p, y, z)$ remain a finite constant in number, and vary continuously, as p varies in S.

Notes. This is a slight simplification of the notion defined precisely in our paper. There are other ways to express this notion. The notion seems to be implicit in the work of Lazard and Rouillier [JSC, 2007] on solving parametric systems using the discriminant variety.

We consider an **example** for which $r = 3$. Let $c > 0$ be some constant. Let $f(x, y, z) = z^2 + x - c$ and $g(x, y, z) = z^3 - cz + y$. Let V be the real algebraic variety defined by $f = 0 \wedge g = 0$. Then V is delineable on $(-\infty, c)$. Indeed, V is the union of the disjoint graphs of the continuous functions $\theta_1(x) = (x\sqrt{c-x}, \sqrt{c-x})$ and $\theta_2(x) = (-x\sqrt{c-x}, -\sqrt{c-x})$ over $(-\infty, c)$. V is also delineable on $\{c\}$ and (c, ∞). Notice that the image of V under the canonical projection $\pi : \mathbb{R}^3 \to \mathbb{R}^2$ with $\pi(x, y, z) = (x, y)$ is the real algebraic curve defined by $\text{res}_z(f, g) = r(x, y) = y^2 - cx^2 + x^3 = 0$ which we saw in a previous slide.



Discussion about example

With f and g defined above, suppose we want to solve the following QE problem:

$$(\exists y)(\exists z)[f(x,y,z) = 0 \wedge g(x,y,z) = 0].$$

Let us first apply the specialized CAD algorithm from our ISSAC'05 paper ("On Using Bi-equational Constraints ..."). We need to eliminate z, obtaining $r(x,y)$, then to eliminate y, obtaining $\{x, x-c\}$. The lifting process from $\mathbb{R}^1$ to $\mathbb{R}^2$ yields 6 cells of the curve $r(x,y) = 0$; then from $\mathbb{R}^2$ to $\mathbb{R}^3$ yields 7 cells of the variety V. Finally we use these cells to eliminate the quantifiers from our formula.

Instead we could perform a combined projection, putting $D(x)$ equal to the generator of the ideal $(f, g, f_y g_z - g_y f_z) \cap \mathbb{R}[x]$, that is, $D(x) = x - c$. Lifting over $(-\infty, c)$, $\{c\}$ and $\{c, \infty\}$ yields only 3 cells of V. We could just as well use these cells to eliminate the quantifiers.

The above discussion sets the stage for us to state our main contribution. First we formalise the combined projection operator introduced in the discussion.

Given $f(x, y, z)$ and $g(x, y, z) \in \mathbb{R}[x, y, z]$, we call an element of the elimination ideal $(f, g, f_y g_z - g_y f_z) \cap \mathbb{R}[x]$ a *generalised discriminant* of f and g (with respect to y and z).

Remark. One can find the concept of the discriminant of f and g (with respect to y and z) defined in the literature, but it seems to be not well known.

Main theorem for $r > 2$. Let $f(x, y, z)$ and $g(x, y, z)$ be real polynomials and let $D(x)$ be a generalised discriminant of f and g with $D(x) \neq 0$. Let S be a simply connected submanifold of $\mathbb{R}^{r-2}$ such that the total number of common zeros of f and g in $\mathbb{C}^2$ is finite constant in S and $D(x)$ is order-invariant in S. Suppose further that there is no common zero of f, g, f_y, f_z, g_y, g_z. Then the variety V of f and g is delineable on S.

Some words about the proof

* By simple connectedness of S and continuity of the common zeros, the result is essentially a *local* one. That is, for an arbitrary point p of S, it suffices to show that each real common zero of $f(p,y,z)$ and $g(p,y,z)$ does not "split" into many common zeros as p varies a little within S. Assume p is origin and common zero is $(0,0)$.

* The nonsplitting of a common zero is clear in case the dimension s of S is $r-2$, since D vanishes nowhere in S in this case.

* The case $s < r-3$ (i.e. codimension > 1) can be reduced to the case $s = r-3$ (i.e. codimension $= 1$). To simplify we now take $r = 4$ and $S =$ the x_1-axis.

Some words about the proof (cont'd)

* The last hypothesis implies that at least one partial derivative, say f_z, does not vanish at origin. Hence $f = 0$ can be represented by the expansion $z = \xi(x_1, x_2, y)$ near the origin. The key assumption implies that the roots of $r(x_1, x_2, y) := g(x_1, x_2, y, \xi(x_1, x_2, y))$ are distinct when $x_2 \neq 0$. So we can apply Zariski's theorem to deduce nonsplitting of the roots of $r(x_1, x_2, y)$ in x_1-axis.

A CAD-like algorithm CADV2 based on the main theorem

Input: polys f, g, $h_1, h_2, \ldots$ in r variables x, y, z.
Output: formula $\alpha(x)$ and description of h_i-invariant "CAD" $\mathcal{D}$ of variety V of f and g under assumption $\alpha(x)$.

(1) Construct assumption $\alpha(x)$ so that $\alpha(x)$ implies that f, g, f_y, f_z, g_y, g_z have no common zeros over x; and f and g have only finitely many common zeros over x.

(2) Compute combined projection set P.

(3) Construct description of CAD $\mathcal{D}'$ of $\mathbb{R}^{r-2}$, order-invariant for P, under assumption α.

(4) Lift $\mathcal{D}'$ to "CAD" $\mathcal{D}$ of V using main theorem.

Sample problem (Brown)

When does a real polynomial $p(z) = z^3 + az + b$ have a non-real root $z = x + iy$ such that $xy < 1$?

That is, eliminate the quantifiers from

$$(\exists x)(\exists y)[x^3 - 3xy^2 + ax + b = 0 \wedge$$

$$3x^2 - y^2 + a = 0 \wedge$$

$$y \neq 0 \wedge xy - 1 < 0].$$

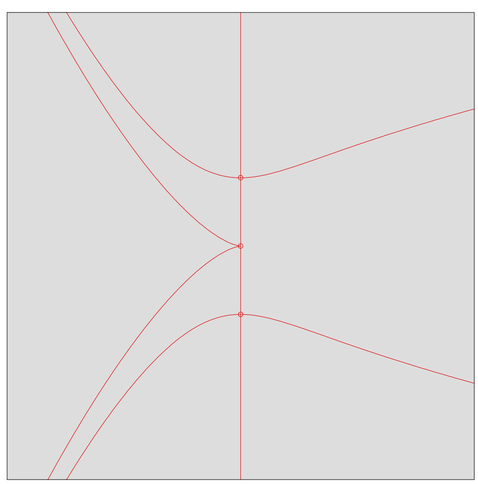
CADV2 can be applied with inputs f, g, h_1, h_2 equal to the four polynomials occuring in the formula with variable ordering a, b, x, y.

Sample problem (cont'd)

Step 1 constructs assumption $a \neq 0 \vee b \neq 0$ as $\alpha(a, b)$.

Step 2 computes $P = \{4a^3 + 27b^2,$
$4a^3b^2 - 4096 - 16a^4 + 27b^4 - 512a^2\}$.

Step 3 computes CAD $\mathcal{D}'$ of the a, b-plane, order-invariant for P under assumption α, illustrated below.



Step 4 lifts $\mathcal{D}'$ to h_i-invariant "CAD" $\mathcal{D}$ of V under assumption α.