An Improved Projection Operator for CAD using Groebner Bases

Josef Schicho
Antonín Tesáček
{jschicho, atesacek}@risc.uni-linz.ac.at

January 20, 1999

1 Introduction

The cylindrical algebraic decomposition (CAD) of Collins [4] is an algorithm for constructing a partition of $\mathcal{R}^n$ which is very useful for solving many important mathematical problems involving algebraic constraints.

The first phase of the CAD algorithm, projection phase, proceeds recursively: applying projection operator on given set of polynomials it produces a set of polynomials in one variable less, which is related to the given set in some geometric meaning.

The original projection operator produces redundant output set and this makes subsequent computations much more complicated.

There are some improvements of projection operator (due to McCallum [7] and Hong [6]. In this paper we give a new improvement based on Groebner bases algorithm of Buchberger [1]. The main idea of our improvement is: If some polynomials do not have a common solution, then we can omit some other polynomials in the projection set. Here we use Groebner basis to decide existence of common solution.

The organization of the paper is as follow. In Section 2 we present our projection operator and prove that it satisfies the requirements that any projection operator must satisfy. We implemented this new projection operator and carried some experiments on our implementation. About these experiments we report in Section 3, where are presented some empirical comparisons between original projection and ours.

2 An Improvement of Projection

In this section we introduce a mapping PROJC_{GB} and prove that it is a projection operator. For basic terminology, including delineability, sign-invariance and principal subresultant coefficient we refer to [4].

Let R_r be set of all r-variate polynomials with real coefficients, $r \geq 0$. By *projection operator* we mean a mapping PROJ : $2^{R_r} \longrightarrow 2^{R_{r-1}}$ such that for any finite subset $\mathcal{A}$ of R_r and any connected $S \subset \mathbb{R}^{r-1}$ in which every element of PROJ($\mathcal{A}$) is sign invariant, $\mathcal{A}$ is delineable on S.

Let $\mathcal{A} \subset R_r$ be finite, $A \in \mathcal{A}$. If $A(x_1, \ldots, x_r) = \sum_{i=0}^{n} A_i(x_1, \ldots, x_{r-1}) \cdot x_r^i$ and $A_n(x_1, \ldots, x_{r-1}) \neq 0$ then $\mathrm{ldcf}(A) = A_n(x_1, \ldots, x_{r-1})$ is *leading coefficient* of A and $\mathrm{ldt}(A) = A_n(x_1, \ldots, x_{r-1}) \cdot x_r^n$ is *leading term* of A. Let $\mathrm{red}(A) = A - \mathrm{ldt}(A)$ be *reductum* of A.. Let $\mathrm{red}^0(A) = A$ be 0-*th reductum* of A and $\mathrm{red}^k(A) = \mathrm{red}(\mathrm{red}^{k-1}(A))$, for $k \geq 1$, be k-*th reductum* of A. Let $\mathrm{ldcf}^k(A) = \mathrm{ldcf}(red^k(A))$, for $k \in \mathbb{N}$.

2.1 Original Projection Operator

Collins [4] proposed the following mapping PROJC and proved that it is a projection operator:

$$\begin{aligned}
\mathrm{PROJC}(\mathcal{A}) &= \mathcal{L}(\mathcal{A}) \cup \mathcal{S}_1(\mathcal{A}) \cup \mathcal{S}_2(\mathcal{A}), \\
\mathcal{L}(\mathcal{A}) &= \left\{ \mathrm{ldcf}^k(A) \,\middle|\, A \in \mathcal{A},\, k \geq 0,\, \deg(\mathrm{red}^k(A)) \geq 1 \right\}, \\
\mathcal{S}_1(\mathcal{A}) &= \left\{ \mathrm{psc}_k(\mathrm{red}^l(A), \mathrm{red}^l(A')) \,\middle|\, A \in \mathcal{A},\, l \geq 0,\, \deg(\mathrm{red}^l(A)) \geq 1, \right. \\
&\qquad \left. 0 \leq k < \deg(\mathrm{red}^l(A')) \right\}, \\
\mathcal{S}_2(\mathcal{A}) &= \left\{ \mathrm{psc}_k(\mathrm{red}^h(A), \mathrm{red}^l(B)) \,\middle|\, A, B \in \mathcal{A},\, h \geq 0,\, l \geq 0, \right. \\
&\qquad 0 \leq k < \min(\deg(\mathrm{red}^h(A)), \deg(\mathrm{red}^l(B))), \\
&\qquad \left. \deg(\mathrm{red}^h(A)) \geq 1,\, \deg(\mathrm{red}^l(B)) \geq 1 \right\}.
\end{aligned}$$

2.2 Improved Projection Operator

At first we introduce predicate ISSOLV(.,.), which will be used in definition of our improved projection operator.

Definition 1. Let $f_1, \ldots, f_k \in \mathbb{R}[x_1, \ldots, x_m]$. Let $S \subseteq \mathbb{C}^m$.
We say that ISSOLV($\{f_1, \ldots, f_k\}, S$) is true iff there exists $x \in S$ such that

$$\begin{aligned}
f_1(x) &= 0 \\
&\vdots \\
f_k(x) &= 0.
\end{aligned}$$

Now we propose mapping PROJC_{GB}:

$$
\begin{aligned}
\mathrm{PROJC}_{GB}(\mathcal{A}) &= \mathcal{L}_{GB}(\mathcal{A}) \cup \mathcal{S}_{1,GB}(\mathcal{A}) \cup \mathcal{S}_{2,GB}(\mathcal{A}),\\
\mathcal{L}_{GB}(\mathcal{A}) &= \Big\{ \mathrm{ldcf}^k(A) \;\Big|\; A \in \mathcal{A},\, k \geq 0,\, \deg(\mathrm{red}^k(A)) \geq 1,\\
&\quad \mathrm{ISSOLV}(\{\mathrm{ldcf}^0(A), \ldots, \mathrm{ldcf}^{k-1}(A)\}, \mathbb{C}^{r-1}) \Big\},\\
\mathcal{S}_{1,GB} &= \Big\{ \mathrm{psc}_k(\mathrm{red}^l(A), \mathrm{red}^l(A')) \;\Big|\; A \in \mathcal{A},\, l \geq 0,\, \deg(\mathrm{red}^l(A)) \geq 1,\\
&\quad 0 \leq k < \deg(\mathrm{red}^l(A')),\\
&\quad \mathrm{ISSOLV}\Big(\{\mathrm{ldcf}^0(A), \ldots, \mathrm{ldcf}^{l-1}(A),\\
&\quad \mathrm{psc}_0(\mathrm{red}^l(A), \mathrm{red}^l(A')), \ldots, \mathrm{psc}_{k-1}(\mathrm{red}^l(A), \mathrm{red}^l(A'))\}, \mathbb{C}^{r-1}\Big) \Big\},\\
\mathcal{S}_{2,GB} &= \Big\{ \mathrm{psc}_k(\mathrm{red}^h(A), \mathrm{red}^l(B)) \;\Big|\; A, B \in \mathcal{A},\, h \geq 0,\, l \geq 0,\\
&\quad 0 \leq k < \min(\deg(\mathrm{red}^h(A)), \deg(\mathrm{red}^l(B))),\\
&\quad \deg(\mathrm{red}^h(A)) \geq 1,\, \deg(\mathrm{red}^l(B)) \geq 1,\\
&\quad \mathrm{ISSOLV}\Big(\{\mathrm{ldcf}^0(A), \ldots, \mathrm{ldcf}^{h-1}(A), \mathrm{ldcf}^0(B), \ldots, \mathrm{ldcf}^{l-1}(B),\\
&\quad \mathrm{psc}_0(\mathrm{red}^h(A), \mathrm{red}^l(B)), \ldots, \mathrm{psc}_{k-1}(\mathrm{red}^h(A), \mathrm{red}^l(B))\}, \mathbb{C}^{r-1}\Big) \Big\}.
\end{aligned}
$$

In the rest of this Section we show that PROJC_{GB} is a projection operator.

At the beginning we repeat some important Theorems [4].

Theorem 1. *Let $A(x_1, \ldots, x_r)$ be a real polynomial, $r \geq 2$. Let S be a connected subset of $\mathbb{R}^{r-1}$. If $\mathrm{ldcf}(A) \neq 0$ on S and the number of distinct roots of A is invariant on S, then the roots of A are delineable on S.*

Theorem 2. *Let A and B be non-zero polynomials over a unique factorization domain. Then $\deg(\gcd(A, B)) = k$ if and only if k is the least j such that $\mathrm{psc}_j(A, B) \neq 0$.*

Theorem 3. *Let $A(x)$ be a real univariate polynomial with $\deg(A) = m \geq 1$ and let $k = \deg(\gcd(A, A'))$. Then $m - k$ is the number of distinct roots of A.*

The proofs of Theorems 1,2 and 3 are given in [4].

Let $\mathrm{nr}(A, x)$ be the number of (complex) roots of $A(x, x_r)$ in $x \in \mathbb{R}^{r-1}$. Let $f_1, \ldots, f_k$ be some polynomials, then $\mathrm{NGB}(f_1, \ldots, f_k)$ will stand for a normed Groebner basis of ideal $< f_1, \ldots, f_k >$.

Lemma 1. *Let $f_1, \ldots, f_k \in \mathbb{R}[x_1, \ldots, x_m]$. Then $\mathrm{ISSOLV}(\{f_1, \ldots, f_k\}, \mathbb{C}^m)$ if and only if $1 \notin \mathrm{NGB}(f_1, \ldots, f_k)$.*

The proof is given in ([9], pp. 191).

Lemma 2. *Let $f_1, \ldots, f_k \in \mathbb{Z}[x_1, \ldots, x_m]$.*
If $\mathrm{ISSOLV}(\{f_1, \ldots, f_k\}, \mathbb{C}^{r-1})$ then $\mathrm{ISSOLV}(\mathcal{C}, \mathbb{C}^{r-1})$ for each $\mathcal{C} \subseteq \{f_1, \ldots, f_k\}$.

Proof. Let $\mathcal{C} = \{g_1, \ldots, g_l\} \subseteq \{f_1, \ldots, f_k\}$. Then each solution of

$$\begin{aligned} f_1(x) &= 0 \\ &\vdots \\ f_k(x) &= 0 \end{aligned}$$

is also solution of

$$\begin{aligned} g_1(x) &= 0 \\ &\vdots \\ g_l(x) &= 0. \end{aligned}$$

□

Theorem 4. *Let $A(x_1, \ldots, x_r)$ be a real polynomial, $r \geq 2$. Let S be a connected subset of $\mathbb{R}^{r-1}$. Let $A \not\equiv 0$ on S. Let*

$$\begin{aligned} \mathcal{L} &= \Big\{ \mathrm{ldcf}^k(A) \,\Big|\, k \geq 0,\, \deg(\mathrm{red}^k(A)) \geq 1, \\ &\qquad \mathrm{ISSOLV}(\{\mathrm{ldcf}^0(A), \ldots, \mathrm{ldcf}^{k-1}(A)\}, \mathbb{C}^{r-1}), \Big\} \\ \mathcal{S}_1 &= \Big\{ \mathrm{psc}_k(\mathrm{red}^l(A), \mathrm{red}^l(A')) \,\Big|\, l \geq 0,\, \deg(\mathrm{red}^l(A)) \geq 1,\, 0 \leq k < \deg(red^l(A')), \\ &\qquad \mathrm{ISSOLV}\Big(\{\mathrm{ldcf}^0(A), \ldots, \mathrm{ldcf}^{l-1}(A), \\ &\qquad \mathrm{psc}_0(\mathrm{red}^l(A), \mathrm{red}^l(A')), \ldots, \mathrm{psc}_{k-1}(\mathrm{red}^l(A), \mathrm{red}^l(A'))\}, \mathbb{C}^{r-1}\Big)\Big\}, \\ \mathcal{P} &= \mathcal{L} \cup \mathcal{S}_1. \end{aligned}$$

If every element of $\mathcal{P}$ is invariant on S, then the roots of A are delineable on S.

Proof. If $\deg(A) \leq 1$ then the theorem is obvious, so let $\deg(A) = n > 1$. Let

$$l = \max\Big\{ i \in \mathbb{N} \,\Big|\, \deg(\mathrm{red}^i)(A) \geq 1, \mathrm{ISSOLV}\left(\{\mathrm{ldcf}^0(A), \ldots, \mathrm{ldcf}^{i-1}(A)\}, \mathbb{C}^{r-1}\right)\Big\}.$$

Then by Lemma 2 $\mathcal{L} = \{\mathrm{ldcf}^0(A), \ldots, \mathrm{ldcf}^l(A)\}$. By assumption, elements of $\mathcal{L}$ are invariant on S. If all elements of $\mathcal{L}$ are 0 on S then $\deg(\mathrm{red}^{l+1}(A)) = 0$, and since $A \not\equiv 0$ on S there is no root of A in S and theorem is obvious. So let k be the least $j \leq l$ such that $\mathrm{ldcf}^j(A) \neq 0$ on S. Then $A = \mathrm{red}^k(A)$ on S so it suffices to show that the roots of $B = \mathrm{red}^k(A)$ are delineable on S. Let

$$\begin{aligned} m &= \max\Big\{ i \in \mathbb{N} \,\Big|\, 0 \leq i < \deg(B'), \\ &\qquad \mathrm{ISSOLV}(\{\mathrm{ldcf}^0(A), \ldots, \mathrm{ldcf}^{l-1}(A), \mathrm{psc}_0(B, B'), \ldots, \mathrm{psc}_{i-1}(B, B')\}, \mathbb{C}^{r-1})\Big\}. \end{aligned}$$

Then by Lemma 2 $\{\mathrm{psc}_0(B, B'), \ldots, \mathrm{psc}_m(B, B')\} \subseteq \mathcal{S}_1$.
Since $psc_{\deg(B)-1}(B, B') = \deg(B) \cdot \mathrm{ldcf}(B) \neq 0$ and all elements of $\mathcal{S}_1$ are invariant on S, there exists $h < \deg(B')$ which is the least such that $\mathrm{psc}_h(B, B') \neq 0$

on S. By Theorem 2, $\deg(\gcd(B, B')) = h$ on S. By Theorem 3, the number of distinct roots of B on S is invariant $\deg(B) - h$. By Theorem 1, the roots of B are delineable on S. □

A similar consideration leads to the following theorem which is analogous to Collins' Theorem 5 [4] and shows that PROJC_{GB} is a projection operator.

Theorem 5. *Let $\mathcal{A} = \{A_1, \ldots, A_n\}$ be a non-empty set of non-zero real polynomials in r real variables, $r \geq 2$. Let S be a connected subset of $\mathbb{R}^{r-1}$. If every element of PROJC_{GB} is invariant on S, then the roots of $\mathcal{A}$ are delineable on S.*

Unfortunately, we cannot give a proof, because a gap was found in the proof of Collins' Theorem 5 [4], and this problem have not been fixed yet.

3 Empirical Results

In this section we present empirical comparisons between the original projection operator and our projection operator.

The new projection operator has been implemented by authors using Saclib library [2] as part of QEPCAD system [5], for computation of Groebner bases is used Groebner library [8].

We run experiments on the following sets of input polynomials.

Input Set 1. The following three polynomials in $\mathbb{Z}[a, b, r, s, t]$ are obtained from a condition that a cubic polynomial has three real roots, counting multiplicities.

$$\begin{gathered} r + s + t \\ rs + st + tr - a \\ rst - b \end{gathered}$$

Input Set 2. The following three polynomials in $\mathbb{Z}[a, b, c, x, y]$ are obtained from the x-axis ellipse problem (Arnon and Mignotte 1988).

$$\begin{gathered} b^2x^2 - 2b^2xc + b^2c^2 + a^2y^2 - a^2b^2 \\ x^2 + y^2 - 1 \\ ab \end{gathered}$$

Input Set 3. The following polynomial in $\mathbb{Z}[x, y, z]$ was constructed in order to test whether our implementation of the new projection operator is done correctly.

$$(x^2y^2)z^3 + (x^2y^2 + 1)z^2 - (x + y)z - 1$$

Table 1, 2, and 3 show the performance comparisons on Input Set 1, 2, and 3, respectively. In these tables T_{proj} is time (in milliseconds) taken to carry out the whole computation of projection set and T_{GB} time spent to compute only Groebner bases. The numbers N_{proj} and N_{fact} are the number of the polynomials in projection set and the number of the factors of projection set.

All the experiments were done on SPARC-ULTRA running SunOS using 20 megabytes of memory for lists. The times in columns T_{proj} and T_{GB} are in millisecond. The time value 0 means that specified kind of computation has been carried, but the spent time is less then 10 ms, and the value N/A means that this computation has not taken place.

Table1: Comparison on Input Set 1

k	Proj.	T_{proj}	T_{GB}	N_{proj}	N_{fact}
5	PROJC	0	N/A	9	8
	PROJC_{GB}	0	0	8	8
4	PROJC	20	N/A	50	54
	PROJC_{GB}	40	30	40	45
3	PROJC	420	N/A	479	665
	PROJC_{GB}	460	280	284	375
2	PROJC	582890	N/A	4369	3311
	PROJC_{GB}	145140	N/A	1483	1087
Total	PROJC	583330	N/A	N/A	N/A
time	PROJC_{GB}	145640	310	N/A	N/A

Table2: Comparison on Input Set 2

k	Proj.	T_{proj}	T_{GB}	N_{proj}	N_{fact}
5	PROJC	0	N/A	7	13
	PROJC_{GB}	10	0	8	15
4	PROJC	10	N/A	22	32
	PROJC_{GB}	20	20	26	34
3	PROJC	40	N/A	130	147
	PROJC_{GB}	100	60	169	171
2	PROJC	930	N/A	482	725
	PROJC_{GB}	600	N/A	482	820
Total1	PROJC	980	N/A	N/A	N/A
time	PROJC_{GB}	730	80	N/A	N/A

Table3: Comparison on Input Set 3

k	Proj.	T_{proj}	T_{GB}	N_{proj}	N_{fact}
3	PROJC	0	N/A	6	9
	PROJC_{GB}	10	0	4	8
2	PROJC	310	N/A	18	23
	PROJC_{GB}	280	N/A	13	17
Total	PROJC	310	N/A	N/A	N/A
time	PROJC_{GB}	290	0	N/A	N/A

On all considered input sets (1, 2 and 3) we can see that what was spent on the computation of Groebner bases came back in the subsequent levels, where the computations have been carried on smaller sets. Moreover, it seems that more polynomials is in input for the given projection step the proportionally shorter time is spent on Groebner basis computations. But this observation can be hardly proved, since it strongly depends on generality of polynomials in the input set (coefficients can be constants or more complicated expressions).

There are also other ideas to improve projection operator (test for a constant leading coefficient, test for finitely many common zeros). These ideas are already incorporated in QEPCAD system by H.Hong, but we switched them off in order to obtain original Collins' projection operator as is Section 2. It seems that the test for constant leading coefficient helps a lot, but our new projection operator is more general and can help in more case, namely when the leading coefficients are not constant.

References

[1] Buchberger, B.: *An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal.* Ph. D. thesis, Universität Innsbruck, Institut für Mathematik. 1965.

[2] Buchberger, B., Collins, G. E., Encarnacion, M. J., Hong, H., Johnson, J. R., Krandick, W., Loos, R., Mandache, A. M., Neubacher, A., Vielhaber, H.: *SACLIB 1.1 User's Guide.* Technical Report RISC-Linz Series 93-19, University of Linz, Austria, 1993.

[3] Collins, G.E.: *Quantifier elimination for the theory of real closed fields by cylindrical algebraic decomposition.* In: Brakhage, H. (Ed.), Automata Theory and Formal Languages. Springer, Berlin Heidelberg New York Tokyo, pp. 134-183 (Lect. Notes Comput. Sci., vol. 33), 1975.

[4] Collins, G.E.: *Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition.* In: Caviness, B. F., Johnson, J. R. (Ed.), Quantifier Elimination and Cylindrical Algebraic Decomposition. Springer, Wien New York, pp. 85-121, 1998.

[5] Hong, H.: *Programmer's Guide to QEPCAD system.* RISC, University of Linz, Austria, 1991.

[6] Hong, H.: *An Improvement of the Projection Operator in Cylindrical Algebraic Decomposition.* In: Caviness, B. F., Johnson, J. R. (Ed.), Quantifier Elimination and Cylindrical Algebraic Decomposition. Springer, Wien New York, pp. 166-173, 1998.

[7] McCallum, S.: *An Improved Projection Operation for Cylindrical Algebraic Decomposition.* In: Caviness, B. F., Johnson, J. R. (Ed.), Quantifier Elimination and Cylindrical Algebraic Decomposition. Springer, Wien New York, pp. 85-121, 1998.

[8] Windsteiger, W., Buchberger, B.: *GROEBNER: A Library for Computing Groebner Bases based on SACLIB.* Technical Report RISC-Linz Series 93-72, University of Linz, Austria, 1993.

[9] Winkler, F.: *Polynomial Algorithms in Computer Algebra.* Springer, Wien New York, 1996.