An Improvement of the Projection Operator in Cylindrical Algebraic Decomposition

Hoon Hong
Department of Computer Science, Ohio State University,
Columbus, Ohio 43210, USA

Abstract

The Cylindrical Algebraic Decomposition (CAD) method of Collins [5] decomposes r–dimensional Euclidean space into regions over which a given set of polynomials have constant signs. An important component of the CAD method is the projection operation: given a set A of r–variate polynomials, the projection operation produces a set P of $(r-1)$–variate polynomials such that a CAD of r–dimensional space for A can be constructed from a CAD of $(r-1)$–dimensional space for P. In this paper, we present an improvement to the projection operation. By generalizing a lemma on which the proof of the original projection operation is based, we are able to find another projection operation which produces a smaller number of polynomials. Let m be the number of polynomials contained in A, and let n be a bound for the degree of each polynomial in A in the projection variable. The number of polynomials produced by the original projection operation is dominated by m^2n^3 whereas the number of polynomials produced by our projection operation is dominated by m^2n^2.

1 Introduction

The cylindrical algebraic decomposition (CAD) of Collins [5] provides a potentially powerful method for solving many important mathematical problems, provided that the required amount of computation can be sufficiently reduced. An important component of the CAD method is the projection operation. Given a set A of r–variate polynomials, the projection operation produces a certain set P of $(r-1)$–variate polynomials such that a CAD of r–dimensional space for A can be constructed from a CAD of $(r-1)$–dimensional space for P. The CAD algorithm begins by applying the projection operation repeatedly, beginning with the input polynomials, until univariate polynomials are obtained. This process is called the projection phase.

McCallum [9] made an important improvement to the original projection operation. He showed, using a theorem from real algebraic geometry, that the original projection set can be substantially reduced in size, provided that input polynomials are well-oriented.

In this paper, we present another improvement to the original projection operation. However our improvement does not impose any restrictions on input polynomials. This improvement is essentially obtained by generalizing a lemma used in Collins' original proof.

Let m be the number of polynomials contained in A, and let n be a bound for the degree of each polynomial in A in the projection variable. The number of polynomials produced by the original projection operation is dominated by m^2n^3 whereas the number of polynomials produced by our projection operation is dominated by m^2n^2.

Preliminary experiments show that our projection operation can sometimes significantly speed up the projection phase of the CAD method. In fact, we present an experimental result that shows 85 times speedup.

The organization of the paper is as follow. In Section 2 we present our projection operation and prove that it satisfies the requirements that any projection operation must satisfy. In Section 3 we analyze and compare the original projection operation and ours in terms of the number of polynomials produced by the projection operations. In Section 4 we present some empirical comparisons between the original projection operation and ours.

2 Idea

In this section, we present our projection operation and prove its validity. We assume that the reader is familiar with the basic terminology of [2, 5], including reducta, principal subresultant coefficients, sign invariance, delineability, regions, sections, sectors, cylinders, and stacks.

Let I_r be the set of all r–variate polynomials with integral coefficients, $r \geq 2$. A ***projection operator*** is a mapping $PROJ : 2^{I_r} \longrightarrow 2^{I_{r-1}}$ such that for any finite subset A of I_r and any $PROJ(A)$–invariant region R in E^{r-1} the following two conditions hold: (1) every element of A is either delineable or identically zero on R, and (2) the sections of $Z(R)$ belonging to different $F, G \in A$ are either disjoint or identical.

2.1 Original Projection Operator

Collins proposed the following mapping $PROJC$ as a projection operator in his pioneering paper on cylindrical algebraic

decomposition [5]:

$$PROJC(A) = PROJ_1(A) \cup PROJ_2(A),$$
$$PROJ_1(A) = \bigcup_{\substack{F \in A \\ F^* \in RED(F)}} (\{ldcf(F^*)\} \cup PSC(F^*, F^{*\prime})),$$
$$PROJ_2(A) = \bigcup_{\substack{F,G \in A \\ F<G}} \bigcup_{\substack{F^* \in RED(F) \\ G^* \in RED(G)}} PSC(F^*, G^*),$$

where "$<$" denotes an arbitrary linear ordering of the elements of A, and for any $F, G \in I_r$, $PSC(F,G)$ denotes the set

$$\{psc_k(F,G) | 0 \leq k < min(deg(F), deg(G)), psc_k(F,G) \neq 0\},$$

and $RED(F)$ denotes the set

$$\{red^i(F) | 0 \leq i \leq deg(F), red^i(F) \neq 0\}.$$

2.2 Improved Projection Operator

Now we propose another mapping $PROJH$ as a projection operator:

$$PROJH(A) = PROJ_1(A) \cup PROJ_2^*(A),$$
$$PROJ_2^*(A) = \bigcup_{\substack{F,G \in A \\ F<G}} \bigcup_{F^* \in RED(F)} PSC(F^*, G),$$

where $PROJ_1(A)$ is defined as above.

A proof that $PROJH$ is a projection operator is almost the same as the proof for $PROJC$. Therefore we will show only the differences between these two proofs. First we recall the following. Let F, G be two polynomials in I_r, $r \geq 2$, such that $deg(F) = m \geq 1$ and $deg(G) = n \geq 1$. Let $\alpha \in E^{r-1}$ such that $ldcf(F)(\alpha) \neq 0$ and $ldcf(G)(\alpha) \neq 0$. Then

$$psc_k(F,G)(\alpha) = psc_k(F(\alpha, x_r), G(\alpha, x_r)),$$

for $0 \leq k < min(m,n)$. This obvious equality is used in proving $PROJC$ to be a projection operator. Now we give a lemma which generalizes this observation. In fact, this lemma contains the key idea leading to the new projection operator $PROJH$.

Lemma 1 *Let F, G be two polynomials in I_r, $r \geq 2$, such that $deg(F) = m \geq 1$ and $deg(G) = n \geq 1$. Let $\alpha \in E^{r-1}$ such that $ldcf(F)(\alpha) \neq 0$ and $deg(G(\alpha, x_r)) = \ell \geq 1$. Then we have*

$$psc_k(F,G)(\alpha) = [ldcf(F)(\alpha)]^{n-\ell}\ psc_k(F(\alpha, x_r), G(\alpha, x_r))$$

for $0 \leq k < min(m, \ell)$.

The lemma follows immediately from the definition of principal subresultant coefficients (psc).

Now we recall two more lemmas which were used in proving $PROJC$ to be a projection operator and which will also be used in proving $PROJH$ to be a projection operator.

Lemma 2 *Let A be a finite subset of I_r, $r \geq 2$, and let R be a $PROJ_1(A)$-invariant region in E^{r-1}. Then every element of A is either delineable or identically zero on R.*

The original proof is given in [5] (Theorem 4). A slightly different proof is also given in [1].

Lemma 3 *Let A be a finite subset of I_r, $r \geq 2$, and let R be a $PROJ_1(A)$-invariant region in E^{r-1}. Let F and G be any two different polynomials in A. If the least integer k such that $psc_k(F(\alpha, x_r), G(\alpha, x_r)) \neq 0$ is constant for $\alpha \in R$, then the sections of $Z(R)$ belonging to F and G are either disjoint or identical.*

The original proof is given in [5] (Theorem 5). A slightly different proof is also given in [1] (Theorem 3.7).

Now we are ready to prove that $PROJH$ is a projection operator.

Theorem 1 *$PROJH$ is a projection operator. To be specific, let A be a finite subset of I_r, $r \geq 2$. Then for any $PROJH(A)$-invariant region R in E^{r-1} the following two conditions hold: (1) every element of A is either delineable or identically zero on R, and (2) the sections of $Z(R)$ belonging to different F, $G \in A$ are either disjoint or identical.*

Proof. Let R be a $PROJH(A)$-invariant region R in E^{r-1}. Since the set $PROJH(A)$ contains the set $PROJ_1(A)$, clearly R is also $PROJ_1(A)$-invariant. Then, by Lemma 2, every element of A is either delineable or identically zero on R. Therefore $PROJH$ satisfies the first condition. So we continue to prove that $PROJH$ satisfies the second condition also.

Let F, G be two polynomials in A such that $F < G$. Since $PROJH(A)$ contains every nonzero coefficient of F and G, each coefficient of F and G either vanishes everywhere or nowhere on R. Hence $deg(F(\alpha, x_r))$ and $deg(G(\alpha, x_r))$ are constant for $\alpha \in R$. Let m denote the constant $deg(F(\alpha, x_r))$ and let ℓ denote the constant $deg(G(\alpha, x_r))$. Let n denote $deg(G)$.

If $m \leq 0$ or $\ell \leq 0$, then the second condition is trivially satisfied. So from now on assume that $m \geq 1$ and $\ell \geq 1$. Let F^* be the unique reductum of F such that $m = deg(F^*) = deg(F^*(\alpha, x_r)) = deg(F(\alpha, x_r))$ and let k be any integer such that $0 \leq k < min(m, \ell)$. Then $psc_k(F^*, G)$ is contained in $PROJH(A)$ and thus the sign of $psc_k(F^*, G)(\alpha)$ is constant for $\alpha \in R$. Then, by Lemma 1, the sign of $[ldcf(F^*)(\alpha)]^{n-\ell}\ psc_k(F^*(\alpha, x_r), G(\alpha, x_r))$ is constant for $\alpha \in R$.

Since $ldcf(F^*)$ is contained in $PROJH(A)$, the sign of $ldcf(F^*)(\alpha)$ is constant for $\alpha \in R$. Also from the way F^* is defined, $ldcf(F^*)(\alpha)$ is nonzero for $\alpha \in R$. Thus the sign of $[ldcf(F^*)(\alpha)]^{n-\ell}$ is nonzero and constant for $\alpha \in R$. Hence the sign of $psc_k(F^*(\alpha, x_r), G(\alpha, x_r))$ is constant for $\alpha \in R$. Then, since $F^*(\alpha, x_r) = F(\alpha, x_r)$ for $\alpha \in R$, the sign of $psc_k(F(\alpha, x_r), G(\alpha, x_r))$ is constant for $\alpha \in R$. Hence the least k such that $psc_k(F(\alpha, x_r), G(\alpha, x_r)) \neq 0$ is also constant for $\alpha \in R$. Then, by Lemma 3, the sections of $Z(R)$ belonging to F and G are either disjoint or identical. Therefore the second condition is satisfied. □

3 Analysis

In this section, we analyze and compare Collins' projection operator and our projection operator in terms of the number of polynomials produced by the projection operators. In the following discussion, let A be a finite subset of I_r, let m be the number of polynomials contained in A, and let n be a bound for the degree of each polynomial in A in the projection variable.

Theorem 2 (PROJC) *The number of polynomials contained in $PROJC(A)$ is dominated by m^2n^3.*

A proof is given in [5] (page 161,163).

Theorem 3 (PROJH) *The number of polynomials contained in $PROJH(A)$ is dominated by m^2n^2*

Proof. The set $PROJ_1(A)$ contains at most $m(n+1) + m(n-1) = 2mn$ polynomials. So let us now continue with the set $PROJ_2^*(A)$.

In the set $PROJ_2^*(A)$, a pair (F, G) can be chosen in $\binom{m}{2}$ ways. So let us count the number of psc's such as $psc_k(red^i(F), red(G))$ for a fixed pair (F, G).

Since $0 \leq k < min(deg(red^i(F)), deg(B)) \leq n-i$, k can be chosen in $n-i$ ways for a given i, $0 \leq i \leq n-1$. Hence (i,k) can be chosen in $\sum_{i=0}^{n-1}(n-i) = \frac{n(n+1)}{2}$ ways. So the set $PROJ_2^*(A)$ contains at most $\binom{m}{2}\frac{n(n+1)}{2}$ polynomials. Therefore $PROJH(A)$ contains at most $2mn + \binom{m}{2}\frac{n(n+1)}{2}$ polynomials. Hence the number of polynomials in $PROJH(A)$ is dominated by m^2n^2. □

4 Empirical Results

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

We implemented both projection operators as a part of the QEPCAD system [6] which carries out quantifier elimination with a partially built CAD. The QEPCAD system is implemented in the ALDES/SAC-2 computer algebra system [4].

The QEPCAD system, given a set A of r–variate integral polynomials, applies a projection operator repeatedly, until univariate projection polynomials are obtained. Following the suggestions made in Section 5 of [5], it computes a squarefree basis of the polynomials each time before applying the projection operation. Explicitly, the following algorithm is used, in which finest squarefree bases are computed.

Projection Phase

(1) Set $J_r \leftarrow A$. Set $k \leftarrow r$.
(2) Compute the contents C_k and the primitive parts P_k of J_k.
(3) Compute the finest square-free basis B_k of the primitive parts P_k.
(4) If $k = 1$, then return. Set $R_{k-1} \leftarrow PROJ(B_k)$. Set $J_{k-1} \leftarrow C_k \cup R_{k-1}$. Remove from J_{k-1} all the constant polynomials if there are any. Set $k \leftarrow k-1$. Go to Step 2. □

To both projection operators, we also made additional refinments as described in [5, 8].

We have carried out experiments on the following sets of input polynomials.

Input Set 1

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

$$r+s+t$$
$$rs+st+tr-a$$
$$rst-b$$

Table 1: Comparison on Input Set 1

k	Proj.	T_2	T_3	T_4	N_B	N_R	N_J
5	Orig.	0.4	1.6	14.2	3	8	7
	Impr.	0.4	1.6	10.6	3	8	7
4	Orig.	0.5	9.2	60.3	6	42	30
	Impr.	0.5	9.2	33.2	6	32	21
3	Orig.	1.6	26.2	1513.1	14	324	228
	Impr.	1.0	20.1	50.9	8	64	44
2	Orig.	4.3	415.5	16167.4	77	3079	2031
	Impr.	0.5	17.0	73.4	16	151	106
1	Orig.	3.3	998.9	N/A	1	N/A	N/A
	Impr.	0.2	17.6	N/A	1	N/A	N/A
Total time	Orig.			21620.2		N/A	
	Impr.			256.2		N/A	

Table 2: Comparison on Input Set 2

k	Proj.	T_2	T_3	T_4	N_B	N_R	N_J
5	Orig.	0.3	26.6	37.4	2	6	6
	Impr.	0.3	26.6	37.2	2	6	6
4	Orig.	1.3	35.0	124.0	5	22	22
	Impr.	1.3	34.7	27.3	5	18	18
3	Orig.	1.6	18.2	177.8	13	135	74
	Impr.	1.1	5.8	17.8	7	32	25
2	Orig.	1.6	58.2	53.7	30	482	280
	Impr.	0.3	12.5	2.2	9	49	32
1	Orig.	0.9	125.1	N/A	111	N/A	N/A
	Impr.	0.1	17.6	N/A	7	N/A	N/A
Total time	Orig.			727.0		N/A	
	Impr.			179.5		N/A	

Table 3: Comparison on Input Set 3

k	Proj.	T_2	T_3	T_4	N_B	N_R	N_J
4	Orig.	0.2	1.7	0.9	3	7	6
	Impr.	0.2	1.6	0.8	3	7	6
3	Orig.	0.2	0.7	3.3	5	15	10
	Impr.	0.2	0.7	3.1	5	15	10
2	Orig.	0.1	2.2	0.6	6	21	11
	Impr.	0.1	2.2	0.6	6	21	11
1	Orig.	0.1	1.5	N/A	4	N/A	N/A
	Impr.	0.1	1.5	N/A	4	N/A	N/A
Total time	Orig.			12.6		N/A	
	Impr.			12.5		N/A	

Input Set 2

The following three polynomials in $Z[a,b,c,x,y]$ are obtained from the x-axis ellipse problem [3].

$$b^2x^2 - 2b^2xc + b^2c^2 + a^2y^2 - a^2b^2$$
$$x^2 + y^2 - 1$$
$$ab$$

Input Set 3

The following five polynomials in $Z[d,c,b,a]$ are from a formula used by Davenport and Heintz [7] in order to show the time complexity of the quantifier elimination in elementary algebra and geometry.

$$a-d$$
$$b-c$$
$$a-c$$
$$b-1$$
$$a^2-b$$

Table 1, 2, and 3 show the performance comparisons on Input Sets 1, 2, and 3, respectively. In these tables, T_2,

T_3, and T_4 are the times (in seconds) taken to carry out Step 2, 3, and 4 of the above algorithm **Projection Phase** respectively. The numbers N_B and N_J are the numbers of polynomials in the sets B_k and J_{k-1} respectively. N_R is the size of the set R_{k-1} considered as a multiset; that is, it counts the number of times each polynomial in R_{k-1} is produced by the projection operator. The last rows show the total times taken, including the times taken for garbage collection. All the experiments were done on a SUN3/50 running Unix using 4 megabytes of memory for lists.

For Input Set 1, our projection operator speeds up the projection phase $21620.2/256.2 \approx 85$ times.

For Input Set 2, our projection operator speeds up the projection phase $727.0/179.5 \approx 4$ times. Note also that the number of univariate basis polynomials (N_B when $k = 1$) is reduced from 111 to 7. A similar improvement was obtained by Arnon and Mignotte [3]; however their approach, unlike ours, is based on problem specific information.

Reducing the size of the projection set is important because it causes additional speedup in the following phases of CAD algorithm, namely the base phase and the extension phase [2].

For Input Set 3, our projection operator does not show any improvement either on the time taken for the projection phase or the number of basis polynomials produced at each iteration. It is mainly because the input polynomials are very simple.

5 Acknowledgment

This research was done as a part of the author's PhD dissertation research. The author is grateful for all the guidance given by his PhD adviser, Professor G. E. Collins, who also made several valuable suggestions on both the structure and the content of this paper.

References

[1] D. S. Arnon, G. E. Collins, and S. McCallum. Cylindrical algebraic decomposition I: The basic algorithm. Technical Report CSD-427, Computer Science Dept, Purdue University, 1982.

[2] D. S. Arnon, G. E. Collins, and S. McCallum. Cylindrical algebraic decomposition I: The basic algorithm. ***SIAM J. Comp.***, 13:865–877, 1984.

[3] D. S. Arnon and M. Mignotte. On mechanical quantifier elimination for elementary algebra and geometry. ***J. Symbolic Comp.***, 5(1,2):237–260, 1988.

[4] G. E. Collins and R. Loos. The ALDES-SAC2 computer algebra system. Technical report, 1980.

[5] George E. Collins. Quantifier elimination for the elementary theory of real closed fields by cylindrical algebraic decomposition. In ***Lecture Notes In Computer Science***, pages 134–183. Springer-Verlag, Berlin, 1975. Vol. 33.

[6] George E. Collins and Hoon Hong. Partial cad construction in quantifier elimination. Technical Report OSU-CISRC-10/89 TR45, Computer Science Dept, The Ohio State University, 1989. Submitted to ***Journal of Symbolic Computation.***

[7] James H. Davenport and Joos Heintz. Real quantifier elimination is doubly exponential. ***J. Symbolic Comp.***, 5(1,2), 1988.

[8] Hoon Hong. An improvement of the projection operator in cylindrical algebraic decomposition. Technical Report OSU-CISRC-12/89 TR55, Computer Science Dept, The Ohio State University, 1989.

[9] S. McCallum. ***An Improved Projection Operator for Cylindrical Algebraic Decomposition.*** PhD thesis, University of Wisconsin-Madison, 1984.