Adjacency Algorithms for Cylindrical Algebraic Decompositions of Three and Higher Dimensional Space I: Adjacencies Over a Non-nullifying $\{0,1\}$ Adjacency

GEORGE E. COLLINS
Research Institute for Symbolic Computation
Johannes Kepler University
A-4040 Linz
Austria
gcollins@risc.uni-linz.ac.at

SCOTT MCCALLUM
Department of Computing
Macquarie University NSW 2109
Australia
scott@mpce.mq.edu.au

March 19, 1997

Abstract

Let A be a set of trivariate irreducible integral polynomials and let D be an A-invariant cylindrical algebraic decomposition (cad) of three-dimensional space. This paper presents a new algorithm for determining the interstack adjacencies in D over a given non-nullifying (for A) 0-cell, 1-cell adjacency in the cad D' of the plane induced by D. We show that this new adjacency algorithm for three-dimensional space can be extended to four-dimensional space.

1 Introduction

The basic theory of and terminology about cylindrical algebraic decomposition (cad) can be found in [1]. Let A be a set of bivariate irreducible integral polynomials. In [2] is presented an algorithm which, given such a set A of bivariate polynomials, constructs an A-invariant cad of the plane, and determines all pairs of adjacent cells in that cad. The algorithm of [2] determines which sections are adjacent to a given 0-cell c^0 in the plane by analyzing the sides of a suitable box constructed around c^0. For this reason we call the adjacency algorithm of [2] the "box algorithm" in the plane.

Now let A be a set of trivariate irreducible integral polynomials. In [3] is presented an algorithm which, given such a set A of trivariate polynomials, constructs an A-invariant cad of three-space having the so-called boundary property, and determines all pairs of adjacent cells in that cad.

Let $r \geq 3$ and let A be a set of r-variate irreducible integral polynomials. We say that a set X in $(r-1)$-space is *nullifying* (for A) if for some $A_i \in A$, with positive degree in the main variable x_r, we have $A_i(\alpha, x_r) = 0$ for all $\alpha \in X$. We say that an adjacency $\{c, d\}$ of an A-invariant cad of $\mathbf{R}^r$ is non-nullifying (for A) provided that neither c nor d is nullifying (for A). If, for example, the dimension of c is 0 and the dimension of d is 1, then we might call the adjacency $\{c, d\}$ a $\{0, 1\}$ adjacency. The notation and terminology of this paragraph was introduced in [3] (our notion of a nullifying set is slightly different from that in [3]).

In this paper we present a new algorithm for determining in a cad of three-space section-section interstack adjacencies over a given non-nullifying $\{0, 1\}$ adjacency in the induced cad of the plane. We show that the new adjacency algorithm for three-space can be extended to four-space. Hence in a cad of r-space, where $r = 3$ or $r = 4$, our algorithm can be applied to yield all the interstack adjacencies over a given non-nullifying $\{0, 1\}$ adjacency in the induced cad of $(r-1)$-space.

This research was conducted while the first author was a Visiting Scholar at Macquarie University early in 1995. The Visiting Scholarship was funded by the Macquarie University Research Grants Scheme.

2 A new three-space adjacency algorithm

Let $C(x, y, z)$ be a trivariate primitive integral polynomial with positive degree in z. We present a new algorithm, which we call the *box algorithm* (after the adjacency algorithm of [2]), for determining the limit point of a given section of C over a 1-cell S_i in the plane in the extended cylinder over a 0-cell $c_0 = (\alpha, \beta_j)$ in the plane, such that c_0 and S_i are adjacent and c_0 is non-nullifying for $C(x, y, z)$.

The following theorem will be used in the validity proof of the box algorithm in $\mathbf{R}^3$.

Theorem 2.1 *Let $A(x) and B(x, y)$ be irreducible integral polynomials of positive degrees in their main variables. Let $C(x, y, z)$ be a primitive integral polynomial of positive degree in z. Let (a_1, a_2) be an open isolating interval for a root*

α of A such that B is delineable over $(\alpha, a_2]$. Let S be a section of B over $(\alpha, a_2]$ such that S is adjacent to (α, β) with $B(\alpha, \beta) = 0$. Suppose that the polynomial $C(\alpha, \beta, z)$ is nonzero, that C is delineable over S and that T is a section of C over S. Then T has a unique limit point $p = (\alpha, \beta, \gamma)$ in the extended cylinder over (α, β) and, if γ is finite, then $C(\alpha, \beta, \gamma) = 0$.

Proof. The section S determines a function $y = f(x)$ on $(\alpha, a_2]$. Likewise T determines a function $z = g(x, y)$ on S. We define $h(x) = g(x, f(x))$, for $x \in (\alpha, a_2]$. Let $P(x, z)$ be the resultant of $B(x, y)$ and $C(x, y, z)$ with respect to y in case the degree of C in y is positive and let $P(x, z) = C(x, 0, z)$ otherwise. Now $P(x, z)$ is a nonzero polynomial, since B is irreducible and C is primitive. Now $P(x, h(x)) = 0$ for every $x \in (\alpha, a_2]$. Thus, where $\overline{P}(x, z)$ is the greatest squarefree divisor (with respect to both x and z) of $P(x, z)$, $\overline{P}(x, h(x)) = 0$, for every $x \in (\alpha, a_2]$. Hence, by Theorem 1 of [8], there exists a_2', with $\alpha < a_2' \leq a_2$, such that h is differentiable in (α, a_2').

We will now show that h is monotone in a subinterval (α, a_2''). Suppose first that $\frac{\partial}{\partial x}\overline{P}$ has positive degree in z. Let $Q(x) = \mathrm{res}_z(\overline{P}, \frac{\partial}{\partial x}\overline{P})$, a nonzero polynomial since $\overline{P}$ is squarefree with respect to x. It is not difficult to show, using the chain rule for differentiation, that every zero of $h'(x)$ is a zero of $Q(x)$. Let (α, a_2'') be the largest subinterval of (α, a_2') which contains no root of $Q(x)$. Then h is monotone in (α, a_2''). Suppose on the other hand that $\frac{\partial}{\partial x}\overline{P}$ is independent of z. Then $\overline{P}(x, z) = \overline{P}_1(x) + \overline{P}_2(z)$ and $\frac{\partial}{\partial x}\overline{P} = \overline{P}_1'(x)$. If $\overline{P}_1'(x) = 0$ then h is constant. Otherwise, if (α, a_2'') is the largest subinterval of (α, a_2') which contains no root of $\overline{P}_1'(x)$, then h is monotone in (α, a_2'').

Hence where $(x_1, x_2, \ldots)$ is a sequence of points in (α, a_2) converging to α, the sequence $(h(x_1), h(x_2), \ldots)$ converges to a limit γ in the extended real line, and p is the unique limit point of T in the extended cylinder over (α, β). Suppose γ is finite. Then $C(\alpha, \beta, \gamma) = 0$, since the variety of C is closed. QED

Box algorithm in $\mathbf{R}^3$ over a non-nullifying $\{0, 1\}$ adjacency in the plane.

Inputs:

1. $A(x), B(x, y)$: irreducible integral polynomials of positive degrees in their main variables.
2. $C(x, y, z)$: primitive integral polynomial of positive degree in z.
3. (a_1, a_2): an open isolating interval with rational endpoints for a root α of A such that B is delineable over $(\alpha, a_2]$.
4. i, j: positive integers such that S_i, the ith section of B over $(\alpha, a_2]$, is adjacent to (α, β_j) where β_j is the jth real root of $B(\alpha, y)$, $C(\alpha, \beta_j, z) \neq 0$ and C is delineable over S_i.

5. k: the index of a section T_k of C over S_i.

Output:

l: an integer, $0 \leq l \leq m+1$, such that T_k is adjacent to $(\alpha, \beta_j, \gamma_l)$, where $\gamma_1 < \ldots < \gamma_m$ are the real roots of $C(\alpha, \beta_j, z)$, $\gamma_0 = -\infty$ and $\gamma_{m+1} = +\infty$.

Steps:

1. If $\deg_y(C(x,y,z)) > 0$ then set $R(x,z) = \mathrm{res}_y(B(x,y), C(x,y,z))$ and otherwise set $R(x,z) = C(x,0,z)$. Set $P(x,z) = \mathrm{pp}(R(x,z))$ and $c(x) = \mathrm{cont}(R(x,z))$.
2. Compute a list $(I_1, \ldots, I_m)$ of isolating intervals for the real roots $\gamma_1 < \ldots < \gamma_m$ of $C(\alpha, \beta_j, z)$.
3. Refine the isolating intervals I_h for the real roots of $C(\alpha, \beta_j, z)$ until there exist among the endpoints of the I_h rational numbers $c_0, c_1, \ldots c_m$ such that $c_0 < \gamma_1 < c_1 < \ldots < c_{m-1} < \gamma_m < c_m$ and $P(\alpha, c_h) \neq 0$ for every h, $0 \leq h \leq m$.
4. Refine the isolating interval (a_1, a_2) for α to an interval (a_1', a_2') such that no $P(x, c_h)$ has a root in $[a_1', a_2']$, $0 \leq h \leq m$, and $c(x)$ has no root in $[a_1', a_2']$ except possibly for α.
5. Compute an isolating interval for β_i', the ith real root of $B(a_2', y)$.
6. Isolate the real roots $\gamma_1', \ldots, \gamma_t'$ of $C(a_2', \beta_i', z)$ and refine the isolating interval for γ_k' until it is contained in some (c_{l-1}, c_l), $0 \leq l \leq m+1$, with $c_{-1} = -\infty$ and $c_{m+1} = +\infty$.
7. Return l. □

Correctness proof for the box algorithm. The refinement process in Step 3 of the algorithm eventually yields rational numbers $c_0, \ldots, c_m$ satisfying the required properties because $P(\alpha, z) \neq 0$. To see why a refinement process required by Step 4 of the algorithm always terminates, the reader can consult Theorem 3.2 of [2]. The refinement process specified in Step 6 can clearly be performed provided that γ_k' is different from each c_h, $0 \leq h \leq m$. Suppose, to the contrary, that $\gamma_k' = c_h$, with $0 \leq h \leq m$. Then $C(a_2', \beta_i', c_h) = 0$ and $B(a_2', \beta_i') = 0$. Therefore $R(a_2', c_h) = 0$. Therefore either $P(a_2', c_h) = 0$ or $c(a_2') = 0$. Either possibility is contrary to the property of $[a_1', a_2']$ obtained in Step 4. The above arguments show that the algorithm always terminates.

We proceed to show that the output l of the algorithm satisfies the condition asserted in the specification. The sections S_i and T_k together determine a continuous function $z = h(x)$ on the interval $(\alpha, a_2']$. For each x in $(\alpha, a_2]$ there is a unique real number y such that $(x, y) \in S_i$. Thus S_i determines a function $y = f(x)$ defined, and indeed continuous, on $(\alpha, a_2']$. Similarly T_k determines a continuous function $z = g(x, y)$ defined for $x \in (\alpha, a_2']$ and $(x, y) \in \overline{S_i}$, the closure of S_i. The function h is defined by $h(x) = g(x, f(x))$, for $x \in (\alpha, a_2']$. We claim that $h(x) \in (c_{l-1}, c_l)$, for every $x \in (\alpha, a_2']$. Suppose that this is not the case. Therefore, by continuity of h, there exists $x_0 \in (\alpha, a_2']$ such that either $h(x_0) = c_{l-1}$ or $h(x_0) = c_l$. Suppose without loss of generality that $h(x_0) = c_l$. It follows easily from previous definitions that $R(x_0, c_l) = 0$. Therefore $P(x_0, c_l) = 0$ or $c(x_0) = 0$. Either possibility contradicts the property of $[a_1', a_2']$ obtained in Step 4, completing the proof of the claim. By Theorem 2.1, T_k has a unique limit point $(\alpha, \beta_j, \gamma)$ in the extended cylinder over (α, β_j). By definition of h, γ is the limit of h as x approaches α. Hence $\gamma \in [c_{l-1}, c_l]$. Suppose that $1 \leq l \leq n$. Then γ is finite. Hence, by Theorem 2.1, $C(\alpha, \beta_j, \gamma) = 0$. Therefore $\gamma = \gamma_l$. Suppose instead that $l = 0$. If γ were finite then, again by Theorem 2.1, $C(\alpha, \beta_j, \gamma) = 0$, contradicting the definition of c_0. Therefore $\gamma = -\infty = \gamma_0$. The case $l = n + 1$ is analogous. QED

Algorithm SSADJ3 from [3] is the key subalgorithm of [3] for $\mathbf{R}^3$ adjacency determination. Algorithm SSADJ3 has inputs somewhat analogous to those of the box algorithm presented in this section, except that SSADJ3 does not have an analogue of k, the index of a specific section T_k of C over S_i and does not assume that it works over a non-nullifying $\{0, 1\}$ adjacency in the plane. The output of SSADJ3 is a list L of all section-section interstack adjacencies over the 0-cell and 1-cell in the plane. In principle an analogue of SSADJ3 for a non-nullifying $\{0, 1\}$ adjacency could be obtained by iterating the box algorithm over every value of k. In practice much of the work which the box algorithm performs need be performed once only by such an analogue of SSADJ3.

3 A four-space adjacency algorithm

Let $D(x, y, z, w)$ be a primitive integral polynomial with positive degree in w. We describe an extension of the box algorithm of the previous section which determines the limit point of a given section of D over a 1-cell T_k in $\mathbf{R}^3$ in the extended cylinder over a 0-cell c_0 in $\mathbf{R}^3$, such that c_0 and T_k are adjacent and c_0 is non-nullifying for $D(x, y, z, w)$.

We first present, somewhat informally, an algorithm which will be used as a subalgorithm of the box algorithm for $\mathbf{R}^4$.

Real Projection Algorithm

Inputs :

1. $A(x), B(x, y)$ and $C(x, y, z)$: irreducible integral polynomials of positive

degrees in their main variables.

2. $D(x,y,z,w)$: primitive integral polynomial of positive degree in w.

3. (a_1,a_2): an open isolating interval with rational endpoints for a root α of A such that B is delineable over $(\alpha,a_2]$, C is delineable over all sections of B over $(\alpha,a_2]$, and D is delineable over all sections of C over all sections of B over $(\alpha,a_2]$.

Outputs:

A nonzero polynomial $c(x)$ and a primitive polynomial $P(x,w)$ satisfying the following conditions. If $c(x)$ has a root in (α,a_2), let η be the smallest such root. Otherwise let $\eta = a_2$. For all real numbers x, y, z and w, if $x \in (\alpha,\eta), B(x,y) = 0, C(x,y,z) = 0$ and $D(x,y,z,w) = 0$ then $P(x,w) = 0$.

Steps:

1. Apply the program qepcad [5] to the input formula $(\exists y)(\exists z)[a_1 < x \leq a_2 \wedge B(x,y) = 0 \wedge C(x,y,z) = 0 \wedge D(x,y,z,w) = 0]$ with variable ordering (x,w,y,z) with user interaction as follows. As soon as the cad of $\mathbf{R}^1$ has been computed, if there is a 0-cell between $\{\alpha\}$ and the 0-cell $\{a_2\}$ let the smallest such be $\{\eta\}$ and set $c(x)$ to the minimal polynomial of η. Otherwise let $\eta = a_2$ and set $c(x) = 1$.

2. Construct a single stack over the interval (α,η).

3. Construct stacks as long as possible in $\mathbf{R}^3$ and $\mathbf{R}^4$.

4. Now each section of the stack in $\mathbf{R}^2$ has a truth value. For each such section with the value true, extract the irreducible polynomial in x and w of which it is a section.

5. Set $P(x,w)$ to the product of the extracted polynomials. $\square$

Correctness proof for the real projection algorithm. By the definition of $c(x)$ and η, if $c(x)$ has a root in (α,a_2), η is the smallest such. Let $x \in (\alpha,\eta)$. By the delineability of B over (α,η) there exist only finitely many values of y such that $B(x,y) = 0$. By the delineability of C over the sections of B, for each such value of y there are only finitely many values of z such that $C(x,y,z) = 0$. And by the delineability of the sections of D over the sections of C, for each such z there are only finitely many values of w such that $D(x,y,z,w) = 0$. Thus there are only finitely many values of w for which the input formula is true. It follows that in the stack in $\mathbf{R}^2$, only sections can have the value true. Therefore, if $x \in (\alpha,\eta), B(x,y) = 0, C(x,y,z) = 0$ and $D(x,y,z,w) = 0$, then (x,w) belongs to some section of the stack in $\mathbf{R}^2$. Let $P_i(x,w)$ be the irreducible polynomial of which it is a section. Then $P_i(x,w) = 0$, P_i is a divisor of P and hence $P(x, w) = 0$. QED

We can now state a four-dimensional analogue of Theorem 2.1.

Theorem 3.1 *Let $A(x)$, $B(x,y)$ and $C(x,y,z)$ be irreducible polynomials of positive degree in their main variables. Let $D(x,y,z,w)$ be a primitive integral polynomial of positive degree in w. Let (a_1,a_2) be an open isolating interval for a root α of A such that B is delineable over $(\alpha,a_2]$. Let S be a section of B over $(\alpha,a_2]$ such that S is adjacent to (α,β), with $B(\alpha,\beta)=0$, and C is delineable over S and over all other sections of B over $(\alpha,a_2]$. Let T be a section of C over S such that T is adjacent to (α,β,γ), with $C(\alpha,\beta,\gamma)=0$, and D is delineable over T and over all other sections of C over sections of B over $(\alpha,a_2]$. Suppose $D(\alpha,\beta,\gamma,w)\neq 0$. Let U be a section of D over T.Then U has a unique limit point $p=(\alpha,\beta,\gamma,\delta)$ in the extended cylinder over (α,β,γ) and, if δ is finite, then $D(\alpha,\beta,\gamma,\delta)=0$.*

Proof. The section S determines a function $y=f(x)$ on $(\alpha,a_2]$. Likewise T and U determine functions $z=g(x,y)$ on S and $w=h(x,y,z)$ on T, respectively. We define $\phi(x)=h(x,f(x),g(x,f(x)))$, for $x\in(\alpha,a_2]$. We claim that there exists a nonzero polynomial $P(x,w)$ such that $P(x,\phi(x))=0$, for all $x\in(\alpha,a_2]$. To prove this claim, let $Q(x,y,w)$ be the resultant with respect to z of C and D, and first suppose that B is not a divisor of Q. In this case, we can set $P(x,w)$ to be the resultant with respect to y of B and Q. If, on the other hand, B is a divisor of Q, then a polynomial $P(x,w)$ satisfying the requirements of the claim is supplied as the second output of an application of the real projection algorithm presented above. The rest of the proof is quite analogous to that of the proof of Theorem 2.1. QED

We can now describe our four-space adjacency algorithm.

Box Algorithm in $\mathbf{R}^4$ over a non-nullifying $\{0,1\}$ adjacency in $\mathbf{R}^3$.

Inputs :

1. $A(x), B(x,y), C(x,y,z)$: irreducible integral polynomials of positive degrees in their main variables.
2. $D(x,y,z,w)$: primitive integral polynomial of positive degree in w.
3. (a_1,a_2): an open isolating interval with rational endpoints for a root α of A such that B is delineable over $(\alpha,a_2]$, C is delineable over all sections of B over $(\alpha,a_2]$, and D is delineable over all sections of C over all sections of B over $(\alpha,a_2]$.

4. i, j: positive integers such that S_i, the ith section of B over $(\alpha, a_2]$, is adjacent to (α, β_j) where β_j is the jth real root of $B(\alpha, y)$.

5. $h(z)$: a squarefree element of $\mathbf{Q}(\gamma)[z]$, where γ is a primitive element for (α, β_j), whose roots define a stack in $\mathbf{R}^3$ over (α, β_j).

6. k, l: positive integers such that T_k, the kth section of C over S_i, is adjacent to $(\alpha, \beta_j, \gamma_l)$, where γ_l is the lth real root of $h(z)$, and $D(\alpha, \beta_j, \gamma_l, w) \neq 0$.

7. m: the index of a section U_m of D over T_k.

Output:

n: an integer, $0 \leq n \leq p+1$, such that U_m is adjacent to $(\alpha, \beta_j, \gamma_l, \delta_n)$, where $\delta_1 < \ldots < \delta_p$ are the real roots of $D(\alpha, \beta_j, \gamma_l, w)$, $\delta_0 = -\infty$ and $\delta_{p+1} = -\infty$.

Steps:

1. While $B(x, y)$ divides $\mathrm{lc}C(x, y, z)$ replace C by its reductum. While $B(x, y)$ divides $\mathrm{lc}_z D(x, y, z, w)$ replace D by its reductum with respect to z. Set $Q(x, y, w) = \mathrm{res}_z(C, D)$. If $B(x, y)$ is not a divisor of Q then set $R(x, w) = \mathbf{res}_y(B, Q)$ in case $\deg_y(Q) > 0$ and set $R(x, w) = Q(x, 0, w)$ in case $\deg_y(Q) = 0$. Then, further, set $P(x, w) = \mathrm{pp}(R)$ and $c(x) = \mathrm{cont}(R)$. If $B(x, y)$ is a divisor of Q then apply the real projection algorithm to the inputs A, B, C, D and (a_1, a_2), obtaining a polynomial $P(x, w)$ and a polynomial $c(x)$.

2. Compute a list $(I_1, \ldots, I_p)$ of isolating intervals for the real roots $\delta_1 < \ldots < \delta_p$ of $D(\alpha, \beta_j, \gamma_l, w)$.

3. Refine the isolating intervals for the real roots of $D(\alpha, \beta_j, \gamma_l, w)$ until there exist among the endpoints of the I_h rational numbers $d_0, d_1, \ldots, d_p$ such that $d_0 < \delta_1 < d_1 < \ldots < d_{p-1} < \delta_p < d_p$ and $P(\alpha, d_h) \neq 0$ for every $h, 0 \leq h \leq p$.

4. Refine the isolating interval (a_1, a_2) to an interval (a_1', a_2') such that $a_2' < a_2$, $c(x)$ has no root in $[a_1', a_2']$ except possibly for α, and no $P(x, d_h)$ has a root in $[a_1', a_2']$, $0 \leq h \leq p$.

5. Compute an isolating interval for β_i', the ith real root of $B(a_2', y)$.

6. Compute an isolating interval for γ_k', the kth real root of $C(a_2', \beta_i', z)$.

7. Isolate the real roots $\delta_1', \ldots, \delta_t'$ of $D(a_2', \beta_i', \gamma_k', w)$ and refine the isolating interval for δ_m' until it is contained in some (d_{n-1}, d_n), $0 \leq n \leq p+1$, with $d_{-1} = -\infty$ and $d_{p+1} = +\infty$.

8. Return n. □

Correctness proof for the box algorithm for $\mathbf{R}^4$. The polynomial $P(x, w)$ obtained in Step 1 is a nonzero polynomial of positive degree in w. Suppose first that B is not a divisor of Q. Let $x \in (\alpha, a_2)$ with $c(x) \neq 0$ and let (x, y, z, w) be the corresponding point of U_m. Then $B(x, y) = 0, C(x, y, z) = 0$ and $D(x, y, z, w) = 0$. ¿From $C(x, y, z) = 0$ and $D(x, y, z, w) = 0$ it follows that $Q(x, y, w) = 0$. ¿From $B(x, y) = 0$ and $Q(x, y, w) = 0$ it follows that $R(x, w) = 0$. ¿From $R(x, w) = 0$ and $c(x) \neq 0$ it follows that $P(x, w) = 0$. Since B is irreducible and not a divisor of Q, R is a nonzero polynomial and hence so also is P. This together with $P(x, w) = 0$ implies that P has positive degree in w. Now assume that B is a divisor of Q so that the real projection algorithm is used. Let $x \in (\alpha, \eta)$ and let (x, y, z, w) be the corresponding point of U_m. Then it is clear that (x, w) belongs to a true section of the stack in $\mathbf{R}^2$. Therefore P is the product of one or more irreducible polynomials in x and w of positive degree in w and hence is a nonzero polynomial of positive degree in w.

In Step 3 it follows from the primitivity of P that $P(\alpha, w)$ is a nonzero polynomial, guaranteeing the possibility of the specified refinement process as in the corresponding step of the algorithm for $\mathbf{R}^3$.

The refinement process specified in Step 7 can clearly be performed provided that δ'_m is different from each d_h, $0 \leq h \leq p$. Suppose, to the contrary, that $\delta'_m = d_h, 0 \leq h \leq p$. Suppose first that B is not a divisor of Q. Then $D(a'_2, \beta'_i, \gamma'_k, d_h) = 0$ and $C(a'_2, \beta'_i, \gamma'_k) = 0$. Therefore $Q(a'_2, \beta'_i, d_h) = 0$. Also $B(a'_2, \beta'_i) = 0$ and so $R(a'_2, d_h) = 0$. Therefore either $P(a'_2, d_h) = 0$ or $c(a'_2) = 0$. Either possibility is contrary to the property of $[a'_1, a'_2]$ obtained in Step 4. Now suppose that B is a divisor of Q. Then $D(a'_2, \beta'_i, \gamma'_k, d_h) = 0$. It follows that $C(a'_2, \beta'_i, \gamma'_k) = 0$ and $B('_2, \beta'_i) = 0$. With η as defined in the real projection algorithm, $a'_2 \in (\alpha, \eta)$. Therefore $P(a_2, d_h) = 0$, contrary to the property of $[a'_1, a'_2]$ obtained in Step 4. The above arguments show that the algorithm always terminates.

A proof that the output n of the algorithm satisfies the condition asserted in the specification can now be modelled in a straightforward way on the proof that the output l of the box algorithm for $\mathbf{R}^3$ satisfies the condition required of it. QED

4 Discussion

The astute reader will have noticed that our box algorithm in $\mathbf{R}^3$ over a given non-nullifying $\{0, 1\}$ adjacency in the plane assumes that the 1-cell in question is a section. But in an arbitrary non-nullifying $\{0, 1\}$ adjacency $\{c^{(0)}, c^{(1)}\}$ in the plane, $c^{(1)}$ could be a sector of the cylinder in which $c^{(0)}$ resides. However this case can be handled similarly. With respect to the box algorithm for $\mathbf{R}^4$ there are still more possibilities for an arbitrary non-nullifying $\{0, 1\}$ adjacency in $\mathbf{R}^3$. Again, every case can be treated in a manner similar to that in which is treated the special case of the algorithm description. A somewhat more serious restriction on the applicability of the box algorithm for $\mathbf{R}^4$ is the rather strong set of delineability assumptions stated in the condition on Input 3.

In [3] the following four categories of adjacencies in an induced cad of the plane are distinguished and treated individually: $\{1, 2\}$, $\{0, 1\}$, non-nullifying $\{0, 2\}$ and nullifying $\{0, 2\}$. Our algorithm of Section 2 provides an alternative treatment of the $\{0, 1\}$ category (more precisely, the subcategory non-nullifying $\{0, 1\}$). This presentation of [3] suggests that a full treatment of adjacency determination in cad's of four-space may require consideration of both the nullifying and non-nullifying cases of the following categories of adjacencies in an induced cad of three-space: $\{0, 1\}$, $\{0, 2\}$, $\{0, 3\}$, $\{1, 2\}$, $\{1, 3\}$ and $\{2, 3\}$. (Presumably the nullifying $\{2, 3\}$ case does not need to be considered.)

Presumably the box algorithm in $\mathbf{R}^4$ over a non-nullifying $\{0, 1\}$ adjacency in $\mathbf{R}^3$, together with its real projection subalgorithm, can be extended to r-dimensional space, where $r > 4$.

References

[1] D. S. Arnon, G. E. Collins, and S. McCallum. Cylindrical algebraic decomposition I: The basic algorithm. *SIAM J. on Computing*, 13(4):865–877, 1984.

[2] D. S. Arnon, G. E. Collins, and S. McCallum. Cylindrical algebraic decomposition II: An adjacency algorithm for the plane. *SIAM J. on Computing*, 13(4):878–889, 1984.

[3] D. S. Arnon, G. E. Collins, and S. McCallum. An adjacency algorithm for cylindrical algebraic decompositions of three-dimensional space. *J. Symbolic Comp.*, 5(1,2):163–187, 1988.

[4] D. S. Arnon. *Algorithms for the Geometry of Semi-Algebraic Sets.* PhD thesis, Comp. Sci. Dept., Univ. of Wisconsin-Madison, 1981. Tech. Report No. 436.

[5] G. E. Collins and H. Hong. Quantifier elimination by partial CAD construction. *J. Symbolic Comp.*, 12(3):299–328, Sept. 1991.

[6] G. E. Collins. Quantifier elimination for the elementary theory of real closed fields by cylindrical algebraic decomposition. In H. Brakhage, editor, *Automata Theory and Formal Languages*, volume 33 of *Lec. Notes Comp. Sci.*, pages 134–183. Springer-Verlag, Berlin, 1975.

[7] H. Hong. *Improvements in CAD-Based Quantifier Elimination.* PhD thesis, Ohio State University, 1990. Tech. Report No. OSU-CISRC-10/90-TR29.

[8] S. McCallum. An improved projection operation for cylindrical algebraic decomposition. To appear.