

Title	Cylindrical Algebraic Decomposition と実代数制約(数式処理における理論とその応用の研究)
Author(s)	下山, 武司
Citation	数理解析研究所講究録 (1995), 920: 247-257
Issue Date	1995-08
URL	<a href="http://hdl.handle.net/2433/59697">http://hdl.handle.net/2433/59697</a>
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

27.

## Cylindrical Algebraic Decomposition と 実代数制約

富士通情報研 下山武司  
shimo@iiias.flab.fujitsu.co.jp

### 27.1 Introduction

代数制約問題,あるいは代数方程式を扱う手段として現在一般的に用いられる方法として, Gröbner basis, や Ritt & Wu's method は, すでによく紹介され知名度もある. これらの二つは, おおまかに言って代数閉体上での方程式の根を扱っている. その一方で, 実根のみを扱うことを主眼に置いている研究も, すで行われており, その代表的なものとして, 今回紹介する Cylindrical Algebraic Decomposition が挙げられる. この方法の日本における知名度は, 初めの二つに比べるとそれほど高いと思われませんが, 今後発展する可能性を秘めていると思われる.

実代数と代数閉体との違いと言えば, 簡単なところでは  $(\exists x) x^2 + bx + c = 0$  は, 代数閉体上では恒真命題であるが, 実代数では,  $b^2 - 4c \geq 0$  と同値となるといったことが, 挙げられる. 又, 科学技術計算に現実に表れる問題の多く (特にロボット制御など) は, 実空間で解を持つか持たないかが重要である場合が少なくない. この様に, 実代数制約問題は, より現実味を帯びた問題ともいえ, ここ数年, 世界的にこの分野の研究が盛んになってきた. 今後は更に, この分野の研究の発展が科学技術計算全体に大きく影響するものと思われる.

1975 年に Collins によって発表された Cylindrical Algebraic Decomposition Algorithm (略して CAD) は, 限定記号 (quantifier)  $(\forall, \exists)$  を含む代数制約式を, 限定記号を含まない同値な表現へと変換 (quantifier elimination) するために用意された sub-algorithm で, その後, Collins らを中心とした者たちによって, CAD の計算の効率化のための改良や, その応用が行われてきた.

CAD を一口で言えば, 多変数版 sturm 法による空間分割法である. Gröbner basis が, 多項式の作るイデアルの標準系で, Ritt & Wu's method が, イデアルの radical (多項式の零点集合と同値) の標準系を与えたのに対し, CAD は, 多項式に空間の点を代入した値の符号を不変とするような空間分割を与えていると言える. また, それぞれの基本となる演算が, Gröbner basis は, M-reduction, Ritt & Wu's method は, pseudo-division, であるのに対し, CAD は, sub-resultant であると言った所からも, それぞれの特徴が表れている. 次の section から, CAD 理論の概要を述べる.

## 27.2 Preliminary

$\mathbf{R}$  は実数の集合,  $\mathbf{Q}$  は有理数の集合,  $\mathbf{Q}[X] = \mathbf{Q}[x_1, \dots, x_r]$  は整数係数多項式環,  $\mathbf{R}^r$  は  $r$  次元  $\mathbf{R}$ -ベクトル空間であるとする.

**Definition 27.2.1**(region, cylinder, section, sector,  $i$ -cell)

$\mathbf{R}^r$  の連結部分集合を region という. region  $K$  に対し,  $K \times \mathbf{R}$  を  $K$  の cylinder といい  $Z(K)$  で表す.  $f$  を  $K$  から  $\mathbf{R}$  への実数値連続関数としたとき,  $\{(a, f(a)) | a \in K\}$  を  $Z(K)$  の section, あるいは  $f$ -section と呼ぶ.  $f_1, f_2$  を二つの実数値連続関数としたとき,  $f_1(a) < f_2(a)$  が, 任意の  $a \in K$  で成り立つとき,  $f_1 < f_2$  と書く. この時,  $\{(\alpha, b) | \alpha \in K, f_1(\alpha) < b < f_2(\alpha)\}$  を  $Z(K)$  の sector, あるいは  $(f_1, f_2)$ -sector と呼ぶ.  $f_1, f_2$  はそれぞれ,  $f_1 = -\infty$  あるいは  $f_2 = \infty$  も許すことにする. (section も sector も region である.)  $\mathbf{R}^r$  の部分集合で,  $\mathbf{R}^i$  と位相同型なものを  $i$ -cell と呼ぶ.

**Definition 27.2.2**(cylindrical decomposition)

$\mathbf{R}^r$  の部分集合  $L$  が, 共通部分のない有限個の region の和集合として表されたとき, それを  $L$  の decomposition という. region  $K$  上の実連続関数  $f_1 < \dots < f_k$  が与えられているとき,  $Z(K)$  の  $(f_i, f_{i+1})$ -sector ( $i \in \{0, \dots, k\}, f_0 = -\infty, f_{k+1} = \infty$ ) 及び  $Z(K)$  の  $f_i$ -section ( $i \in \{1, \dots, k\}$ ) で決まる  $Z(K)$  の decomposition を  $(f_1, \dots, f_k$  で決まる)  $K$  の stack と呼ぶ.  $\mathbf{R}^r$  の decomposition  $\Phi$  が次の (1) あるいは (2) が成り立つとき,  $\Phi$  は, cylindrical であるという. (1)  $r = 1$  かつ,  $\Phi$  は  $\mathbf{R}$  の stack である. (2)  $r > 1$  かつ, ある  $\mathbf{R}^{r-1}$  の cylindrical decomposition  $\Phi'$  が存在して,  $\Phi$  は,  $\Phi'$  のすべての region  $K$  の stack で構成されている.

( $\Phi$  に対する,  $\Phi'$  は, 一意に決まる. これを  $\Phi$  の induced cylindrical decomposition とよび, 逆に  $\Phi$  を  $\Phi'$  の extension と呼ぶ.)

**Definition 27.2.3**(semi-algebraic, formula)

$\mathbf{R}^r$  の部分集合  $K$  が, 集合  $\{x \in \mathbf{R}^r | f(x) \geq 0\}$ , ( $f \in \mathbf{Q}[X]$ ) の共通部分, 和集合, 補集合を組み合わせたものとして表されるとき,  $K$  は semi-algebraic であるという. また, 多項式と等号, 不等号を用いて表された式及び, 限定記号のついた変数 ( $\forall x_i$  あるいは  $\exists x_i$ ) が組み合わせられた論理式を formula と呼ぶ. 限定記号がつかない formula を quantifier free formula とよぶ.

**Example 1**(Quartic problem)

次の 1 及び 2 は, 同値である. 1 から 2 を構成する事を *quantifier elimination* と呼ぶ.

(*quantifier free formula* は, 一意的には決まらない.) '&' は *and*, '||' は *or* を表す事とする.

1. *formula* :  $(\forall x)(x^4 + px^2 + qx + r \geq 0)$

2. *quantifier free formula* :  $\delta \geq 0 \& [p \geq 0 || L < 0 || (L = 0 \& q = 0)]$ ,

where  $\delta = 256r^3 - 128p^2r^2 + 144pq^2r + 16p^4r - 27q^4 - 4p^3q^2$ ,  $L = 8pr - 9q^2 - 2p^3$ .

**Definition 27.2.4**(*cylindrical algebraic decomposition*)

$\mathbf{R}^r$  の *decomposition* の各 *region* が *semi-algebraic* であるときその *decomposition* は *algebraic* であるといい, 加えて, *cylindrical* であるときに, *cylindrical algebraic decomposition* (CAD) という.

**Definition 27.2.5**(*cylindrical algebraic sample*)

$\mathbf{R}^r$  の CAD  $\Phi$  が与えられた時,  $\Phi$  の *cell* から選んだ代表点を *sample point* とよび, すべての *cell* から取った *sample point* の集合を *sample* と呼ぶ.  $\Phi$  の *induced CAD*  $\Phi'$  の任意の *cell*  $R$  に対し, *cylinder*  $Z(R)$  に含まれるすべての *sample point* が, 等しい  $x_1, \dots, x_{r-1}$  座標を持つとき, その  $x_1, \dots, x_{r-1}$  座標の集合 ( $\Phi'$  の *sample*) を *induced sample* という. *sample* が, *cylindrical* であるとは, それが *induces sample* をもち, その *induced sample* が *cylindrical* であるときをいう. 更にその座標が *algebraic* の時, *cylindrical algebraic sample* (CAS) という.

**Definition 27.2.6**(*invariant*)

$R$  を  $\mathbf{R}^r$  の部分集合とし,  $f$  を  $\mathbf{Q}[X]$  の要素とする.  $R$  の任意の点  $\alpha$  で  $f(\alpha)$  の符号が不変であるとき,  $f$  は  $R$  で *invariant*, (あるいは,  $R$  は  $f$ -*invariant*) であるという. 多項式集合  $A = \{f_1, \dots, f_n\}$  について, すべての  $f_i$  が  $X$ -*invariant* であるとき,  $R$  は  $A$ -*invariant* という. 更に,  $\mathbf{R}^r$  の部分集合の集合  $S$  については, その要素がすべて  $A$ -*invariant* の時, 同じく  $A$ -*invariant* であるという.

**Definition 27.2.7**(*delineable, identically zero*)

$K$  を  $\mathbf{R}^{r-1}$  の *region* とし,  $f$  を  $\mathbf{Q}[X]$  の要素とする.  $Z(K)$  ( $K$  によって作られる  $\mathbf{R}^r$  の *cylinder*) 上にある  $f$  の零点集合が, 互いに共通部分のない *section* からなる場合,  $f$  は  $K$  上 *delineable* であるという. この時, これらの *section* によって出来る *stack* を  $S(f, K)$  と書く. ( $S(f, K)$  は,  $f$ -*invariant* である.)

$\mathbf{R}^{r-1}$  の部分集合  $K$  及び,  $\mathbf{Q}[X]$  の要素  $f$  に対し,  $K$  の任意の点  $\alpha$  で  $f(\alpha, x_r) \equiv 0$  であるとき,  $f$  は,  $K$  上 *identically zero* であるという.

**Example 2**多項式  $f = y^4 - 2y^3 + y^2 - 3x^2y + 2x^4$  に対し,  $f$ -*invariant* な  $\mathbf{R}^2$  の *cylindrical decomposition* を考える.  $g = \text{res}_y(f, f') = 2048x^{12} - 4608x^{10} + 37x^8 + 12x^6$  を取る.  $g = 0$  の *real root* は, 計 5 個で, それらより形成される  $\mathbf{R}$  の *decomposition* を  $\Psi$  とする.  $\Psi$  は, 11 個の *cell* から成る.  $f$  は,  $\Psi$  の各 *cell* の上で *delineable* となっており, 各 *cylinder* 上  $f$  で定まる *stack* の和集合が,  $f$ -*invariant* な  $\mathbf{R}^2$  の *cylindrical decomposition* を定めている. これを Fig 0 に記す. この *cylindrical decomposition* は, 55 個の *cell* から成っている.

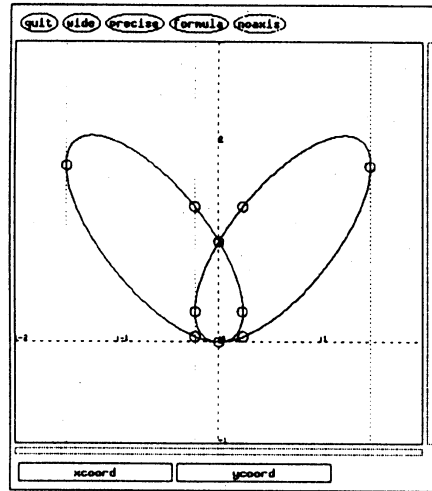


Fig 0.

## 27.3 CAD algorithm

$\mathbb{Q}[X] = \mathbb{Q}[x_1, \dots, x_r]$  の多項式の変数順序は  $x_r > \dots > x_1$  であるとする.  $f, g \in \mathbb{Q}[X]$  に対し,  $\text{subres}_j(f, g)$  ( $f, g$  の  $j$ -th sub-resultant) を  $S_j(f, g)$  とし,  $S_j(f, g)$  の  $x_r^j$  の係数 ( $f, g$  の  $j$ -th principal subresultant coefficient) を  $\text{psc}_j(f, g)$  と書く.  $n = \min(\deg(f), \deg(g))$  の時,  $\text{psc}_n(f, g) = 1$  と定める.

$f \in \mathbb{Q}[X]$  に対し,  $\text{ldcf}(f)$  を  $f$  の  $x_r$  についての leading coefficient とし,  $\text{ldt}(f)$  を leading term すなわち  $\text{ldcf}(f)x_r^{\deg(f)}$  とし, 更に  $\text{red}(f)$  を  $f - \text{ldt}(f)$  とする.  $k \geq 0$  に対して,  $\text{red}^k(f) = \text{red}(\text{red}^{k-1}(f))$  ( $\text{red}^0(f) = f$ ) とする. ここで,  $\text{RED}(f) = \{\text{red}^k(f)\} \setminus \{0\}$ ,  $\text{PSC}(f, g) = \{\text{psc}_j(f, g)\} \setminus \{0\}$  とする. また,  $\text{der}(f) = f'$  を  $f$  の  $x_r$  についての微分とし,  $\text{der}^0(f) = f$ ,  $\text{der}^k(f) = \text{der}(\text{der}^{k-1}(f))$  とする.

**Definition 27.3.1** (projection)

$A = \{f_1, \dots, f_n\}$  を  $\mathbb{Q}[X]$  の有限部分集合, に対して,  $\text{Proj}(A) = \text{Proj1}(A) \cup \text{Proj2}(A)$  を  $A$  の projection と呼ぶ. ただし,  $R_i = \text{RED}(f_i)$ , としたとき  $\text{Proj1}(A) = \cup_i \cup_{g_i \in R_i} (\{\text{ldcf}(g_i)\} \cup \text{PSC}(g_i, g'_i))$ ,  $\text{Proj2}(A) = \cup_{i < j} \cup_{g_i, g_j \in R_i} \text{PSC}(g_i, g_j)$  である.

**Theorem 27.3.1A** を  $\mathbb{Q}[X]$  の部分集合,  $K$  を  $\text{Proj}(A)$ -invariant な  $\mathbb{R}^{r-1}$  の region とする. この時,  $A$  の任意の要素は,  $K$  上で, delineable であるか, あるいは, identically zero である. また, 任意の異なる  $A$  の要素  $f, g$  について,  $Z(K)$  の  $f$ -section 及び  $g$ -section は, 共通部分を持たない.

**Definition 27.3.2** (augmented projection)

$\text{Aproj}(A) = \text{Proj}(A) \cup \text{Aproj1}(A)$  を  $A$  の augmented projection と呼ぶ. ただし,  $\text{Aproj1}(A) = \cup_i \cup_{g_i \in D_i} \text{PSC}(g_i, g'_i)$ ,  $D_i = \{\text{der}^k(f) \mid f \in R_i, 0 < k < \deg(f)\}$  である.

$Der(A) = \cup_i D_i$  とする. すると, Theorem 27.3.1 に続いて, 次が成り立つ.

**Theorem 27.3.2A** を  $\mathbf{Q}[X]$  の部分集合,  $K$  を  $Aproj(A)$ -invariant な  $\mathbf{R}^{r-1}$  の region とする. この時,  $K$  が algebraic に定義されていれば,  $K$  の cylinder  $Z(K)$  内の各 cell は, algebraic に定義できる.

続いて, CAD algorithm について述べる. この algorithm を用いた CAD 計算の具体例は, §6 で示す.

**Procedure 1(main)**

(変数の個数  $n$  に関する帰納的 Procedure.)

入力 :  $n$  変数多項式の集合  $A$ .

出力 :  $A$ -invariant な CAD  $\Phi$

$n = 1$  の時

通常の一変数 sturm 法を  $A$  に適応し CAD を求める.

$n > 1$  の時

$A$  の Augmented Projection を  $A'$  とする.

$A'$  の変数の個数は  $A$  より小さいので, この procedure を帰納的に  $A'$  に適応する.

$D'$  を  $A'$  invariant な  $\mathbf{R}^{n-1}$  の CAD とする.

$D'$  の cell を  $\{\Psi_1, \dots, \Psi_\ell\}$  とする.

$f$  を  $\prod_{h \in A} h$  の maximal square free part とする.

$i = 1, \dots, \ell$  について,

$f$  の  $\Psi_i$  上の CAD  $\Phi_i$  を, Procedure 2 で求める.

$\{\Phi_1, \dots, \Phi_\ell\}$  が求める  $A$  の CAD である.

**Procedure 2(sub)**

( $f = f_r$  の次数  $r$  に関する帰納的 Procedure.)

入力 :  $\mathbf{R}^{n-1}$  の region  $\Psi$ ,  $\Psi$ -invariant で  $x_n$  について  $r$  次の多変数多項式  $f$ .

出力 :  $f$ -invariant な CAD  $\Phi$ .

$r = 1$  の時,

$D_0 = \{\{f(\alpha, x_n) < 0, \Psi(\alpha)\}, \{f(\alpha, x_n) = 0 \ \& \ \Psi(\alpha)\}, \{f(\alpha, x_n) = 0 \ \& \ \Psi(\alpha)\}\}$  が, 求めるもの.

$r > 1$  の時,

$f_{r-1}$  を  $f_r$  の  $x_n$  に関する微分  $\frac{d}{dx_n} f_r$  の maximal square free part とする.

$f_{r-1}$  の  $x_n$  に関する次数は,  $f_r$  より小さいので, 帰納的にこの procedure を  $f_{r-1}$  に適応.

$f_{r-1}$  の CAD を  $\Xi$  と置く.

$\Xi$  の cell を,  $x_n$  座標が小さいほうから  $\Xi_1, \dots, \Xi_t$  と置く.

$i = 1, \dots, t$  について,

$\Phi_{3i} = \{f(\alpha, \beta) = 0 \ \& \ \Psi(\alpha) \ \& \ f_n(\beta) > 0, \Xi_i(\beta)\}$ ,

$$\begin{aligned}\Phi_{3i-1} &= \{f(\alpha, \beta) = 0 \& \Psi(\alpha) \& f_n(\beta) = 0, \Xi_i(\beta)\}, \\ \Phi_{3i-2} &= \{f(\alpha, \beta) = 0 \& \Psi(\alpha) \& f_n(\beta) < 0, \Xi_i(\beta)\}, \\ \Phi &= \{\Phi_1, \dots, \Phi_{3t}\} \text{ は, } f_n \text{ の CAD}\end{aligned}$$

**Remark 27.3.1**

*Procedure 2* において,  $f_r$  の,  $\Psi$  で定まる *cylinder* の各 *sector* は,  $D''$  のいずれかの *cell* に, 高々一つしか含まれていない. よって,  $\Phi$  が,  $f_n$  の CAD となる.

**Remark 27.3.2**

*Procedure 2* の出力  $\Phi$  には, *null set* が, 明らかに, 多く含まれている.

**Remark 27.3.3**

*Collins (1975)* の方法では, 同時に *sample point* も求めることで, 無駄な *formula* が多少押さえられている. ただし, *Procedure* は, いささか複雑である.

## 27.4 CAD の問題点

CAD は, 他の代数制約の手法である Gröbner basis や, Ritt & Wu's method 等よりも歴史がやや新しく, また, 研究者の数も, 他に比べると少ないため, その応用や効率化などの面でやるべきことが, まだまだ多く残されている. 課題となっているものの中で, 特に本質的と思われるものは, 次の三点である.

- Projection,
- Real root isolation,
- Evaluation.

これらは, アルゴリズムの効率化の面でも特に注目されている事であり, それらに関する論文も多い. この三点について一つ一つまとめながら, 今後の課題について議論を進めてみる.

### 27.4.1 Projection

Projection は, 多変数多項式を sub-resultant 等によって, 変数消去する操作であり, これによって結局, 一変数多項式の実根を求めることに, 帰着される.  $n$  変数多項式であれば, 当然  $n$  回の Projection が行われるわけであるが, その操作によって表れる多項式の集合は, 回を増す毎に巨大なものになるという性質があり, 特に変数の個数が多い場合には, 多項式の数ばかりでなく, その一つ一つのサイズも大きなものとなる場合が少なくない. 特に, *Collins (1975)* にある, オリジナルなもの (augmented projection) では, その様な性格が著しく表れる. 一方, Projection は, 上記の Theorem 27.3.1 ある

いは Theorem 27.3.2 が成り立てばいいわけで、Theorem を成立させるような多項式集合をもっと小さくできないかと考えるのは、自然なことと思われる。

Arnon, Collins, McCallum (1984) では、CAD の sample point に注目し、sample point のみを考える場合には、augmented projection は、必要ないことを示し、McCallum (1988) では、'order invariant' というものを定義し、その条件の元で、Projection を更に小さいものにした。ただし、McCallum (1988) の方法は、(私見ではあるが) いささか理論的であり、実計算には向かないかも知れない。

これらの論文以降での、Projection の改良は、個々の問題に依存した場合には、いくつかなされているが、一般的な場合での成果は、あまり見かけられない。

もし、ここに挙げたものが理論的限界であるならば、それを示す必要がある。また、特殊な場合についての考察もまだ充分ではなく、課題は、まだ残されている。

## 27.4.2 Real root isolation

再帰的な Projection の操作によって変数消去された多項式集合は、やがて一変数多項式の集合となる。これらの一変数多項式の実根の分離が、real root isolation の第一段階である。これは、sturm 法によってなされ、実際に多項式  $f$  の根  $\alpha$  は  $f(\alpha) = 0$  と  $a < \alpha < b$  と表される。これらの実根を用いて、 $\mathbf{R}$  の cylindrical algebraic decomposition  $\Phi_1$  が構成される。一変数多項式の根の分離については、Collins & Loos (1982) や、Collins & Johnson (1989) 等に、まとめられている。

次の段階として、 $\Phi_1$  の各 region 上で、二変数多項式の根を分離し、それらを section とする stack を構成することで、 $\mathbf{R}^2$  の cylindrical algebraic decomposition  $\Phi_2$  が求まる。同じことを変数の個数だけ段階をふんで、最終的に  $\mathbf{R}^n$  の cylindrical algebraic decomposition が得られる。

理論的には、この様な形で求められるわけであるが、実際の計算では、様々な問題が出てくる。根の表現は一変数の場合ならば、一点であるからまだ簡単だが、多変数の場合には、一般に高次曲線あるいは、高次曲面を表現しなくてはならない。よってそれを表現する方法によっては、CAD アルゴリズムの効率性に影響するため、この部分に関する研究も、比較的盛んである。特徴的なものでは、次の様なものが挙げられている。

1. 多変数版 sturm 法を用いる方法 (Collins, 1975)
2. 限定記号を用いた方法 (Arnon & Collins & McCallum, 1984)
3. cylinder を輪切り (slice) する方法. (Arnon & Mignotte, 1988)

これらは、それぞれに長所短所があって、決定版は今の所ない。(1) は理論的にしっかりしており、すべての cell が、機械的に quantifier free formula として、記述できるため、インプリメントしやすく、quantifier elimination への応用も簡単である。しかし、本質的に augmented projection を用いているため、Projection が巨大になる傾向がある。(2) は、簡便な方法ではあるが quantifier elimination には使いづらい。(3) は、人為的な操作が加わる分、結果が見易く判りやすい。しかし、輪切りの方法が与えられた問題に依存していて、一般論が作りづらい。



これらの他にも、細かな改良が他の論文にも至る所に表れるが、本質的解決になってない。結局、問題に応じて戦略を変えるしかないのかも知れない。

### 27.4.3 Evaluation

cylindrical algebraic decomposition の応用は、主として、quantifier elimination の計算である。その際、各 cell の sample point の座標を多項式に代入し、その値の正負あるいは 0 を判定しなくてはならない。

一般に、各 sample point の座標は、代数的数で表示されている。一例を挙げれば、 $\alpha = \sqrt[3]{5}$  は、 $\alpha^3 - 5 = 0$  and  $1 < \alpha < 2$  と表され、この値を  $f(x) = 2x^4 - 4x^2 - 5 \in \mathbf{Q}[x]$  に代入した値  $f(\alpha)$  の正負を求める、といった様な事が要求される。(ちなみに、 $f(\alpha) > 0$  である。)

この場合は、多項式  $x^3 - 5$  の根である  $\alpha$  を含む区間を sturm 法で狭めていき、その区間で、 $f$  の符号が変わらないようにすればよい。しかし、sturm 法は、その係数が、有理数のもの以外では、実行が難しく、 $\alpha$  の定義多項式に別の代数的数  $\beta_1, \dots, \beta_i$  を含んでいるときには、別の考察が必要である。Collins (1975) 以来、CAD algorithm 実行中に複数の代数的数が表れた場合、それらの primitive element を求め、その最小多項式から、sturm 法で、区間を狭める方法が取られてきた。

しかし、この方法のように、一々 primitive element を計算するのは、経験上、非常に重たい事である。よって、primitive element を計算しないで、sturm 法を実行する事が出来れば、計算効率がずいぶん上がるはずである。

## 27.5 最近の動き

### 27.5.1 Partial CAD

CAD の最も大きな応用分野は、何度も言っている通り quantifier elimination である。しかし CAD の計算は、非常に大きな計算で、quantifier elimination をするためだけに、 $\mathbf{R}^n$  全体の空間分割を計算するのは、いささか大げさすぎる事が否めない。その点の改良もいくつかなされている。その一つが、Partial CAD (Collins & Hong, 1991) である。これは、CAD 計算と、quantifier elimination (実際には、evaluation) を同時に進めることで、無駄な計算を省くものである。

### 27.5.2 Simplification

CAD algorithm を通じて、機械的に求められた quantifier free formula は、一般に、非常に大きく

なる。しかし、それらの成分のうちほとんどは、重複していたり、空集合であったりというように、余分なものであることが少なくない。よって、これらの quantifier free formula を simplification しようとする考え方が出てくる。詳細は、Hong (1992) をお読みいただきたい。

### 27.5.3 Comprehensive Gröbner Bases

CAD 以外の方法で、quantifier elimination を、機械的に計算する手法もはちまち出始めており、その一つが Comprehensive Gröbner Bases を用いた方法である。詳しくは、Weispfenning (1994) を参照のこと。

## 27.6 CAD の計算例

多項式、 $f = y^4 - 2y^3 + y^2 - 3x^2y + 2x^4$  を考える。この  $f$  に対し、 $f$ -invariant な cylindrical algebraic decomposition を、Collins (1975) に多少手を加えた方法で計算する。変数順序は  $y > x$  とする。 $f$  は、Fig 1 に表れる零点集合を持つ。 $f$  の零点集合が delineable となるように、 $\mathbf{R}^2$  を cylinder に分割すると、Fig 2. となる。

(Collins (1975) の方法では、 $f$  の augmented projection  $Aproj(f)$  を計算し、その零点集合でもって、cylinder に分割するのだが、この場合、 $Aproj(f)$  は、余分な polynomial を多く含んでいて使いづらい。)

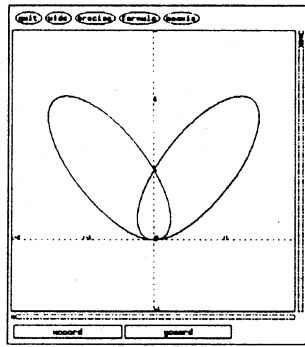


Fig 1.

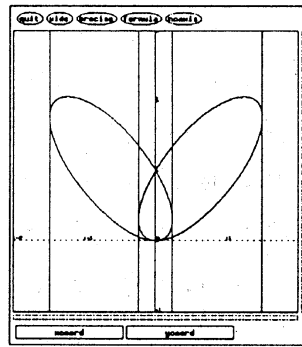


Fig 2.

これらの分割直線の  $x$  座標は、 $res_y(f, f') = 2048x^{12} - 4608x^{10} + 37x^8 + 12x^6 = 0$  で表される。さて、Fig 2 に表れる各 cell を semi-algebraic に表す事が、目標である。そのためにまず、 $f' = 4y^3 - 6y^2 + 2y - 3x^2$  を用意する。Fig 3 は、Fig 2 に  $f' = 0$  を重ねたものである。 $f'$  の零点集合によって、 $f$  の各 cylinder 内の零点集合が、上下に分離できているのが確認できる。この  $f' = 0$  を用いるには、更に、 $f'$  の零点集合を semi-algebraic に表現しなくては行けない。そのために、 $f'' = 12y^2 - 12y + 2$  を用意する。Fig 4 は、 $f'$  と  $f''$  の零点集合を重ね、 $f'$  の零点集合が、delineable になるように、 $\mathbf{R}^2$  を cylinder に分割したものである。 $f''$  の零点集合によって、 $f'$  のそれが、分離で

きている。Fig 4 の各分割直線の  $x$  座標は,  $\text{res}_y(f', f'') = 64(243x^4 - 1) = 0$  で表される。

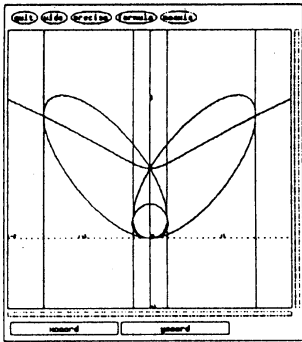


Fig 3.

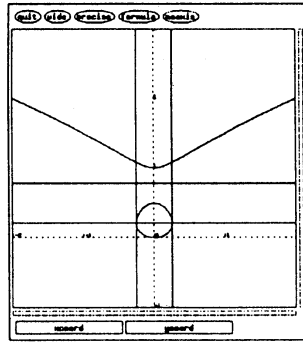


Fig 4.

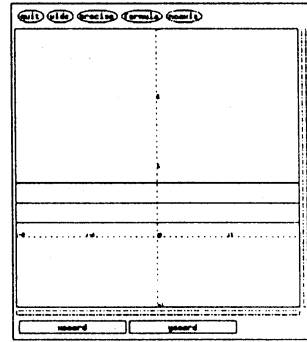


Fig 5.

さて,  $f'' = 12y^2 - 12y + 2$  (既約) の零点集合は,  $\mathbf{R}$  全体で delineable であり, cell の個数は, 5 である。それぞれの cell は,  $f''' = 2y - 1$  を用いて,  $\Phi_1^2, \dots, \Phi_5^2$  と semi-algebraic に書ける。Fig 5 は,  $f'' = 0$  と  $f''' = 0$  を重ねたものである。

$$\begin{aligned} \Phi_1^2 &= \{f'' > 0 \& f''' > 0\}, \Phi_2^2 = \{f'' = 0 \& f''' > 0\}, \Phi_3^2 = \{f'' < 0\}, \\ \Phi_4^2 &= \{f'' = 0 \& f''' < 0\}, \Phi_5^2 = \{f'' > 0 \& f''' < 0\}, \end{aligned}$$

続いて,  $f'$  について, まず,  $243x^4 - 1 = 0$  で表される  $x$  の分割を行う。sturm 法によって,  $\Psi_1^1, \dots, \Psi_5^1$  と表される。  $\Psi_1^1 = \{243x^4 - 1 > 0 \& x > 0\}$ ,  $\Psi_2^1 = \{243x^4 - 1 = 0 \& x > 0\}$ ,  $\Psi_3^1 = \{243x^4 - 1 < 0\}$ ,  $\Psi_4^1 = \{243x^4 - 1 = 0 \& x < 0\}$ ,  $\Psi_5^1 = \{243x^4 - 1 > 0 \& x < 0\}$ 。

これらを用いて,  $f'$  による CAD の各 cell を semi-algebraic に表すと, 次の様に  $\Phi_{i,j}^1, \dots, \Phi_{5,3}^1$  とする。

$$\begin{aligned} \Phi_{1,1}^1 &= \Psi_1^1 \& \{f' > 0\}, \quad \Phi_{1,2}^1 = \Psi_1^1 \& \{f' = 0\}, \quad \Phi_{1,3}^1 = \Psi_1^1 \& \{f' < 0\} \\ \Phi_{2,1}^1 &= \Psi_2^1 \& \{f' > 0\}, \quad \Phi_{2,2}^1 = \Psi_2^1 \& \{f' = 0 \& \Phi_1^2\} \\ \Phi_{2,3}^1 &= \Psi_2^1 \& (\{f' < 0 \& \Phi_1^2\} \vee \{f' < 0 \& \Phi_2^2\} \vee \{f' < 0 \& \Phi_3^2\}) \\ \Phi_{2,4}^1 &= \Psi_2^1 \& \{f' = 0 \& \Phi_4^2\}, \quad \Phi_{2,5}^1 = \Psi_2^1 \& \{f' < 0 \& \Phi_5^2\} \\ \Phi_{3,1}^1 &= \Psi_3^1 \& \{f' > 0 \& \Phi_1^2\}, \quad \Phi_{3,2}^1 = \Psi_3^1 \& \{f' = 0 \& \Phi_1^2\} \\ \Phi_{3,3}^1 &= \Psi_3^1 \& (\{f' < 0 \& \Phi_1^2\} \vee \{f' < 0 \& \Phi_2^2\} \vee \{f' < 0 \& \Phi_3^2\}), \quad \Phi_{3,4}^1 = \Psi_3^1 \& \{f' = 0 \& \Phi_3^2\} \\ \Phi_{3,5}^1 &= \Psi_3^1 \& (\{f' > 0 \& \Phi_3^2\} \vee \{f' > 0 \& \Phi_4^2\} \vee \{f' > 0 \& \Phi_5^2\}) \\ \Phi_{3,4}^1 &= \Psi_3^1 \& \{f' = 0 \& \Phi_5^2\}, \quad \Phi_{3,5}^1 = \Psi_3^1 \& \{f' < 0 \& \Phi_5^2\} \\ \Phi_{4,1}^1 &= \Psi_4^1 \& \{f' > 0\}, \quad \Phi_{4,2}^1 = \Psi_4^1 \& \{f' = 0 \& \Phi_1^2\} \\ \Phi_{4,3}^1 &= \Psi_4^1 \& (\{f' < 0 \& \Phi_1^2\} \vee \{f' < 0 \& \Phi_2^2\} \vee \{f' < 0 \& \Phi_3^2\}) \\ \Phi_{4,4}^1 &= \Psi_4^1 \& \{f' = 0 \& \Phi_4^2\}, \quad \Phi_{4,5}^1 = \Psi_4^1 \& \{f' < 0 \& \Phi_5^2\} \\ \Phi_{5,1}^1 &= \Psi_5^1 \& \{f' > 0\}, \quad \Phi_{5,2}^1 = \Psi_5^1 \& \{f' = 0\}, \quad \Phi_{5,3}^1 = \Psi_5^1 \& \{f' < 0\} \end{aligned}$$

以下, 一例を除き, 大幅に省略するが  $f$  の CAD は, 計  $1+3+5+7+9+5+9+7+5+3+1=55$  個の cell から成り, 各々  $\Phi_{1,1}^0, \Phi_{2,1}^0, \dots, \Phi_{11,1}^0$  と, semi-algebraic に表現できる。これらは, 一変数方程式  $2048x^{12} - 4608x^{10} + 37x^8 + 12x^6 = 0$  で与えられる  $x$  軸の分割  $\Psi_1^0, \dots, \Psi_{11}^0$  及び 上で与えられた

$\Phi_{1,1}^1, \dots, \Phi_{5,3}^1$ , 及び  $f > 0, f = 0, f < 0$  によって表現される. 例えば,  $\Phi_{3,2}^0$  は, 次の様に表現される.

$$\Phi_{3,2}^0 = \Psi_3^0 \& (\{f = 0 \& \Phi_{1,1}^1\} \vee \{f = 0 \& \Phi_{2,1}^1\} \vee \{f = 0 \& \Phi_{3,1}^1\}).$$

## References

- D.S.Arnon, G.E.Collins, S.McCallum. (1984). Cylindrical algebraic decomposition I: The basic algorithm. SIAM J. Comp., 13. 856-877.
- D.S.Arnon, S. McCalum (1892). Cylindrical Algebraic Decomposition by Quantifier Elimination. EUROCAM' 82. LNCS 144. 215-222.
- D.S.Arnon, M. Mignotee. (1988). On methanical quantiier elimination for elementary algebra and geometry. JSC.1988,5 (1,2). 237-260.
- B.Buchberger, G.E.Collins, B. Kutzler (1988). Algebraic Methods for Geometric Reasoning. Ann. Rev. Comput. Sci. 1988, 3. 85-119.
- G.E.Collins. (1975) Quantifier elimination for the elementary theory of real closed fields by cylindrical algebraic decomposition. LNCS., 33. 134-183.
- G.E.Collins and H.Hong. (1991) Partial cylindrical algebraic decomposition for qualtifier elimination. JSC.1991,12(3) 299-328.
- G.E.Collins and J.R.Johnson. (1989) Quantifier elimination and the sign variation method for real root isolation . Proceedings of ISSAC 1989. 264-271.
- G.E.Collins and R.G.K.Loos. (1982). Real zeros of polynomials. Computer Algebra, Computing, Suppl. Springer-Verlag 4, 83-94.
- J.H.Davenport and Y.Siret and E.Tournier. (1988). Computer Algebra (systems and algorithms for algebraic computation). Academic Press.
- H. Hong. (1990). An impurovement of the projection operator in cylindrical algebraic decomposition. Proceedings of ISSAC 1990. 261-264.
- H.Hong. (1992). Simple Solution Formula Construction in Cylindrical Algebraic Decomposition based Quantifier Elimination. Proceedings of ISSAC 1992. 177-188.
- H.Hong. (1993). Qualitfier Elimination for Formulas Constrained by Quadratic Equations. Proceedings of ISSAC 1993. 264-274.
- S.McCallum. (1988). An Improved Projection Operation for Cylindrical Algebraic Decomposition of Three-dimensional Space. JSC. 1988, 5. 141-161.
- V.Weispfenning (1994) A new approach to quantifier elimination for real algebra. preprint.