QE for RCF by CAD

富永 直弥

2023 年 7 月 4 日

1 CAD アルゴリズム

CAD とは, ユークリッド空間の分割で, 各分割の上で複数の多項式を符号不変にするものである. Collins により提唱された CAD アルゴリズムについてかく.

定義 1.1. $\mathbb{R}^n$ の有限部分集合族 $\mathfrak{D}$ が,

- 任意の $D \in \mathfrak{D}$ は空でない弧状連結集合,
- 任意の $D_1, D_2 \in \mathfrak{D}$ について, $D_1 \neq D_2$ ならば $D_1 \cup D_2 = \emptyset$,
- $\bigcup_{D \in \mathfrak{D}} D = \mathbb{R}^n$

を満たすとき, $\mathfrak{D}$ を $\mathbb{R}^n$ の分割という.

定義 1.2. $F \subset \mathbb{R}[x_1, \ldots, x_n]$ を有限部分集合とする.
$D \subset \mathbb{R}^n$ が F-符号不変であるとは, 任意の $f \in F$ に対し, f の符号が D 上一定であることと定義する.
さらに. $\mathbb{R}^n$ の分割 $\mathfrak{D}$ が, 任意の $D \in \mathfrak{D}$ に対して, D が F-符号不変となるとき, $\mathfrak{D}$ を $\mathbb{R}^n$ の F-符号不変な分割という.

1.1 描画可能

定義 1.3. $F \subset \mathbb{R}^n[x_1, \ldots, x_n]$ を有限部分集合とする. 空でない弧状連結部分集合 $S \subset \mathbb{R}^{n-1}$ が F-描画可能であるとは,

- 任意の $x \in S$ に対し, F の解の個数, すなわち $\{y \in \mathbb{R} \mid$ ある $f \in F$ に対し $\mathrm{f(x,y)} = 0\}$ の元の個数が一定であり,
- 各 $x \in S$ の F の解を $f_1(x) < f_2(x) < \cdots < f_k(x)$ と書くとき, 各 f_i は S 上の実数値連続関数

であることと定義する.

命題 1.1. $S \subset \mathbb{R}^{n-1}$ を空でない弧状連結部分集合とし, $F \subset \mathbb{R}[x_1, \ldots, x_n]$ を有限部分集合とする. 次の 3 条件を満たすとき, S は F-描画可能である.

- 任意の $f \in F$ に対し, S 上 f の複素数根の数は重複度込みで一定である.
- 任意の $f \in F$ に対し, S 上 f の相異なる複素数根の数は一定である.

- 相異なる任意の $f, g \in F$ に対し, S 上 f, g に共通する複素数根の数は重複度込みで一定である.

この命題を示すために次の二つの補題を用意する.

補題 1.1. $S \subset \mathbb{R}^{n-1}$ を空でない弧状連結部分集合とし, $f_1, f_2 \in \mathbb{R}[x_1, \ldots, x_n]$ が次を満たすとする.

- 各 $i = 1, 2$ に対し, S 上 f_i の重複度込みの複素数根の数は一定.
- 各 $i = 1, 2$ に対し, S 上 f_i の相異なる複素数根の数は一定.
- S 上 f_1, f_2 の重複度込みの複素数共通根の数は一定.

このとき, S 上 f_1, f_2 の相異なる複素数共通根の数は一定.

証明. 方針: $S_k = \{a \in S \mid f_1(a), f_2(a)$ の相異なる複素数共通根が k 個 $\}$ が開集合であることを示す. (多項式の解の, 係数についての連続性から示せる.)

□

補題 1.2. $A \in \mathbb{R}[x_1, \ldots, x_n]$ とし, $S \subset \mathbb{R}^{n-1}$ を弧状連結部分集合とする.

- S 上 A の重複度込みの複素数根の数は一定.
- S 上 A の相異なる複素数根の数は一定.

この時, S は $\{A\}$-描画可能である.

証明. 方針: 次の二つのことを示さなければならない.
1. S 上実根の数は一定.
2. S 上実根は連続である.
いずれも多項式の根の係数に対する連続性から示せる. □

命題 1.1. **の証明.** 補題 1.2. より, 各 $f \in F$ に対して, S は $\{f\}$-描画可能である. よって,S 上の連続関数 $\alpha_{1,f}(a) < \ldots \alpha_{n_f,f}(a)$ を, 各 $a \in S$ で $f(a)(x) \in \mathbb{R}[x]$ の解であるようにとれる.

主張. $f, g \in F$ が, $f \neq g$ であるとする, ある $a \in S$ において $\alpha_{k,f}(a) = \alpha_{l,g}(a)$ であるならば, 任意の $a \in S$ に対して $\alpha_{k,f}(a) = \alpha_{l,g}(a)$ である.

この主張は, S が弧状連結であることと, 補題 1.1. から従う. この主張より, F の解の個数は S 上一定である. よって, 命題が示された. □

系 1.1. $S \subset \mathbb{R}^{n-1}$ を弧状連結部分集合とし, $F \subset \mathbb{R}[x_1, \ldots, x_n]$ を有限部分集合とする. 次が成り立つとき, S は F-描画可能である.

- 任意の $f \in F$ に対し, $\deg(f(a))$ が一定 $(a \in S)$.
- 任意の $f \in F$ に対し, $\deg(\gcd(f(a), \frac{\partial f}{\partial x_n}(a)))$ が一定 $(a \in S)$.
- 任意の $f, g \in F$ に対し, $\deg(\gcd(f(a), g(a)))$ が一定 $(a \in S)$.

よって, F-符号不変な $\mathbb{R}^n$ の分割を与えるには, 系.1.1. の条件を満たすような $\mathbb{R}^{n-1}$ の分割を構成すればよい. 一つ目の条件を満たすような $\mathbb{R}^{n-1}$ の分割を与えるには, 各 $f \in F$ について, x_n 係数が符号不変になるような分割を構成すればよい. しかし, 二つ目と三つ目の条件を満たすような $\mathbb{R}^{n-1}$ の分割を与えるの

は少し難しい. なぜなら, 多項式 $f, g \in \mathbb{R}[x_1, \ldots, x_n]$ について, $a \in \mathbb{R}^{n-1}$ を固定したとき, $\gcd(f,g)(a)$ と $\gcd(f(a), g(a))$ は必ずしも等しくないからである.

よって, 二つ目と三つ目の条件も満たすような $\mathbb{R}^{n-1}$ の分割を与えることができるように次の節で準備をする.

1.2 主部分終結式係数 (Principal Subresultant Coefficient)

定義 1.4. R を可換環とし, $A(x), B(x) \in \mathrm{R}[x]$ を, $\deg A(x) = m, \deg B(x) = n$ とする. ただし, $\deg 0 = 0$ と解釈する.

$j = 0, \ldots, \min\{n, m\}$ に対し, 多項式 $A(x), B(x)$ の j-部分終結式 $S_j(A, B)$ を次のように定義する.

$$A(x) = a_m x^m + \cdots + a_1 x + a_0,$$
$$B(x) = b_n x^n + \cdots + b_1 x + b_0$$

として, $j = 0, \ldots, \min\{n, m\}$ に対し,

$$M_j = \begin{pmatrix} a_m & a_{m-1} & \cdots & a_1 & a_0 & \\ & a_m & \cdots & a_2 & a_1 & a_0 \\ & & \ddots & & & \\ b_n & b_{n-1} & \cdots & b_1 & b_0 & \\ & b_n & \cdots & b_2 & b_1 & b_0 \\ & & \ddots & & & \end{pmatrix} \in \mathrm{M}_{m+n-2j, m+n-j}(\mathrm{R})$$

とする. ここで, 行列の空白部分はすべて 0 であり, また, 行列の上側は $n - j$ 行, 行列の下側は $m - j$ 行である.

また, $j = 0, \ldots, \min\{m, n\}$, $i = 0, \ldots, j$ に対し,

$$M_{j,i} = (M_j \text{ の第 } 1 \text{ 列}, M_j \text{ の第 } 2 \text{ 列}, \ldots, M_j \text{ の第 } m+n-2j-1 \text{ 列}, M_j \text{ の第 } m+n-i-j \text{ 列}) \in \mathrm{M}_{m+n-2j, m+n-2j}(\mathrm{R})$$

とする. $j = 0, \ldots, \min\{n, m\}$ に対し,

$$S_j(A, B) = \sum_{i=0}^{j} \det M_{j,i} \cdot x^i$$

を, 多項式 $A(x), B(x)$ の j-部分終結式 $S_j(A, B)$ という.

この j-部分終結式の先頭項係数を, $\mathrm{psc}_j(A, B)$ とかき, 多項式 $A(x), B(x)$ の j-主部分終結式係数という.

主部分終結式係数は, 多項式 $A(x), B(x)$ の係数, 及び次数に依存して定まる.

注意 1.1. m, n のどちらかが 0 のとき, $S_0(A, B) = 0, \mathrm{psc}_0(A, B) = 0$ とする.

また, $\mathrm{psc}_0(A, B)$ は, 多項式 $A(x), B(x)$ の終結式に一致する.

命題 1.2. R を体とし, $A(x), B(x) \in \mathrm{R}[x] \setminus \{0\}$ とすると, 次が成立する.

$$\deg(\gcd(A, B)) = \min\{j \in \{0, 1, \ldots, \min\{n, m\}\} \mid \mathrm{psc}_j(A, B) \neq 0\}$$

証明. 後で書く. 方針: 部分終結式がユークリッドの互除法で出てくる多項式の列の定数倍になることが分かる.

□

1.3 符号不変な分割の存在と CAD アルゴリズム

定義 1.5. $F \subset \mathbb{R}[x_1, \ldots, x_n]$ を有限部分集合とする. $\mathrm{PROJ}(F) \subset \mathbb{R}[x_1, \ldots, x_{n-1}]$ を, 次のように定める.

まず, $B(F) := \{\mathrm{red}^k(f) \mid f \in F, k = 1, \ldots, \deg(f)\}$ とする. ただし, $\mathrm{red}(f) = f - \mathrm{LT}(f; x_n)$ である. 次に,

$$\begin{aligned}
\mathrm{PROJ}_1(F) &:= \{\mathrm{LC}(f; x_n) \mid f \in B\} \\
\mathrm{PROJ}_2(F) &:= \{\mathrm{psc}_j(f, \frac{\partial f}{\partial x_n}; x_n) \mid f \in B, j = 0, \ldots, \deg(\frac{\partial f}{\partial x_n}; x_n)\} \\
\mathrm{PROJ}_3(F) &:= \{\mathrm{psc}_j(f, g; x_n) \mid f, g \in B, j = 0, \ldots, \min\{\deg(f; x_n), \deg(g; x_n)\}\}
\end{aligned}$$

とし, 以上を用いて

$$\mathrm{PROJ}(F) := \mathrm{PROJ}_1(F) \cup \mathrm{PROJ}_2(F) \cup \mathrm{PROJ}_3(F)$$

と定める.

系 1.2. $F \subset \mathbb{R}[x_1, \ldots, x_n]$ を有限部分集合とし, $S \subset \mathbb{R}^{n-1}$ を弧状連結部分集合とする.

S が $\mathrm{PROJ}(F)$-符号不変ならば, S は F-描画可能である.

証明. 命題 1.1. 及び命題 1.2. から従う. □

定義 1.6. $F \subset \mathbb{R}[x_1, \ldots, x_n]$ を有限部分集合とする. $S \subset \mathbb{R}^{n-1}$ が F-描画可能とする. このとき, S 上の F の解を $f_1(x) < \cdots < f_k(x)$ とし, $f_0(x) := -\infty$, $f_{k+1}(x) := \infty$ とするとき,

$$\begin{aligned}
C_{2i} &:= \{(x, y) \mid x \in S, f_i(x) = y\} \quad i = 1, \ldots, k, \\
C_{2i+1} &:= \{(x, y) \mid x \in S, f_i(x) < y < f_{i+1}(x)\} \quad i = 0, 1, \ldots, k
\end{aligned}$$

とすれば, $\{C_j\}_{j=1}^{2k+1}$ は $S \times \mathbb{R}$ の F-符号不変な分割を与える. この $S \times \mathbb{R}$ の分割 $\{C_j\}_{j=1}^{2k+1}$ を, S の持ち上げといい, $\mathfrak{L}(S)$ と書く.

また, $\mathfrak{D}$ が $\mathbb{R}^{n-1}$ の分割であるとき, $\mathfrak{L}(\mathfrak{D}) := \bigcup_{D \in \mathfrak{D}} \mathfrak{L}(D)$ を $\mathfrak{D}$ の持ち上げという.

以上より, 有限部分集合 $F \subset \mathbb{R}[x_1, \ldots, x_n]$ が与えられたとき, F の符号不変な分割を取得するアルゴリズムは次のように表現される.

Algorithm 1 CAD アルゴリズム

Require: $n \geq 1$: 自然数, $F \subset \mathbb{R}[x_1, \ldots, x_n]$: 有限部分集合

Ensure: $\mathfrak{D}$: $\mathbb{R}^n$ の F-符号不変な分割

1: $\mathfrak{D} \leftarrow \mathrm{PROJ}^{n-1}(F)$-符号不変な $\mathbb{R}^1$ の分割
2: $k \leftarrow 1$
3: **while** $k < n$ **do**
4: $\quad \mathfrak{D} \leftarrow \mathfrak{L}(\mathfrak{D})$: $\mathfrak{D}$ の持ち上げ
5: $\quad k \leftarrow k + 1$
6: **end while**

このアルゴリズムを実際にコンピュータ上に実装するには, $\mathbb{R}^n$ の分割でなく, 分割の各セルから代表元を取得したものを得る.