前処理による Barnett の定理に基づく 近似 GCD 計算の安定化の検討

讃岐 勝

筑波大学　医学医療系臨床医学域
〃　附属病院医療情報経営戦略部
〃　学術情報メディアセンター

〃　医学医療系 トランスボーダー医学研究センター

19 – 21 Dec., 2022
RIMS 2022

本日の話：近似 GCD の計算のための前処理

- Barnett の定理のサーベイ
- Barnett の定理
  - Bezout 行列から生成される線形方程式から近似 GCD を計算
- 前処理を検討
  - 条件数の算出
  - 収束性の条件 (優対角行列)：算法に依存

モチベーション:多変数の近似 GCD

入力 F, G ⇒ 話題 2: 入力を操作

⇒ Bezout 行列 ⇒ 話題 1: 部分 Bezout 行列

⇒ 1 変数近似 GCD の計算 ⇒ Lifting 法 ⇒ 多変変数近似 GCD

Barnett の定理＝ Bezout 行列を利用した GCD 計算法

- Companion 行列による線形方程式 (Barnett, 1969, 1971)
- Bezout 行列，Bezout-Hankel 行列による線形方程式
  (Diaz-Toca&G.Vega 1992)
- 高速 LU 分解 (Bini-Boito 2007)
- 多変数への拡張のため直接法による計算 (2009)
- 修正 Newton 法, 最適化手法 (Zhi，池-照井など)
  - SNTLN 法
  - GPGCD 法
- 条件数に関すること
  - 次数の見積もり (2015–)
  - 本日：両条件化の検討・条件数の改善
- 本日:反復法 (Gauss-Seidel 法、Jacobi 法) による方法・視点

記号 (1)

- **入力：** $F, G, F_1, \ldots, F_m \in \mathbb{F}[x]$ **または** $\mathbb{F}[x, u_1, \ldots, u_\ell]$

$$\begin{aligned} F(x) &= f_n x^n + \ldots + f_0 = C\tilde{F} + \Delta_F \\ G(x) &= g_n x^n + \ldots + g_0 = C\tilde{G} + \Delta_G \end{aligned}$$

- **出力：** $C = \gcd(F, G)$ with $k = \deg(C)$

- Bezout **行列を構成するため**

$$\frac{F(x)G(y) - F(y)G(x)}{x - y} = \sum_{0 \le i,j < n} b_{i,j} x^{i-1} y^{j-1}$$

記号 (2):Bezout 行列

- Bezout 行列 $\mathrm{Bez}(F,G) = (b_{i,j})_{1\le i,j\le n} \in \mathbb{F}^{n\times n}$

$$
\begin{aligned}
\mathrm{Bez}(F,G) &= \left(\begin{array}{ccc||ccc}
b_{1,1} & \cdots & b_{1,k} & b_{1,k+1} & \cdots & b_{1,n} \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
b_{k,1} & \cdots & b_{k,k} & b_{1,k+1} & \cdots & b_{k,n} \\
\hline\hline
b_{k+1,1} & \cdots & b_{k+1,k} & b_{k+1,k+1} & \cdots & b_{k+1,n} \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
b_{n,1} & \cdots & b_{n,k} & b_{n,k+1} & \cdots & b_{n,n}
\end{array}\right) \\
&= \left(\begin{array}{ccc||ccc}
\boldsymbol{b}_1 & \cdots & \boldsymbol{b}_k & \boldsymbol{b}_{k+1} & \cdots & \boldsymbol{b}_n
\end{array}\right) \\
&= \left(\begin{array}{ccc||c}
\boldsymbol{b}_1 & \cdots & \boldsymbol{b}_k & \mathrm{Bez}_{n-k}(F,G)
\end{array}\right) \\
&= \left(\begin{array}{ccc||c}
* & \cdots & * & * \\
\hline\hline
\tilde{\boldsymbol{b}}_1 & \cdots & \tilde{\boldsymbol{b}}_k & \tilde{\mathrm{Bez}}_k(F,G)
\end{array}\right)
\end{aligned}
$$

  - $\boldsymbol{b}_{k+1},\ldots,\boldsymbol{b}_n$ は一次独立
  - $\boldsymbol{b}_i = \mathrm{span}_{\mathbb{F}}(\boldsymbol{b}_{k+1},\ldots,\boldsymbol{b}_n)$

算法の復習：Bezout 行列による GCD 計算

- **入力：** $F(x), G(x) \in \mathbb{F}[x]$ with $n = \deg(F) \geq \deg(G)$
- **算法：**
  1. Bezout **行列** $\mathrm{Bez}(F,G) = (b_{i,j})_{1 \leq i,j \leq n} \in \mathbb{F}^{n \times n}$ **を構成**

$$
\begin{aligned}
\mathrm{Bez}(F,G) &= \left(\begin{array}{ccc||ccc}
b_{1,1} & \cdots & b_{1,k} & b_{1,k+1} & \cdots & b_{1,n} \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
\hline\hline
b_{k+1,1} & \cdots & b_{k+1,k} & b_{k+11,k+1} & \cdots & b_{k+1,n} \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
b_{n,1} & \cdots & b_{n,k} & b_{n,k+1} & \cdots & b_{n,n}
\end{array}\right) \\
&= \left(\begin{array}{ccc||c}
\boldsymbol{b}_1 & \cdots & \boldsymbol{b}_k & \mathrm{Bez}_{n-k}(F,G)
\end{array}\right) \\
&= \left(\begin{array}{ccc||c}
* & \cdots & * & * \\
\hline\hline
\tilde{\boldsymbol{b}}_1 & \cdots & \tilde{\boldsymbol{b}}_k & \tilde{\mathrm{Bez}}_k(F,G)
\end{array}\right)
\end{aligned}
$$

  2. **線形方程式系を解く**

$$\mathrm{Bez}_{n-k}(F,G)\boldsymbol{x} = \boldsymbol{b}_i \text{ for } 1 \leq i \leq k$$

  3. **解が** GCD **の係数**

算法の復習：Bezout 行列による GCD 計算

- **入力：** $F(x), G(x) \in \mathbb{F}[x]$ with $n = \deg(F) \geq \deg(G)$
- **算法：**
  1. Bezout **行列** $\mathrm{Bez}(F,G) = (b_{i,j})_{1 \leq i,j \leq n} \in \mathbb{F}^{n \times n}$ **を構成**

$$\mathrm{Bez}(F,G) \quad = \quad \left(\begin{array}{ccc|c} \boldsymbol{b}_1 & \cdots & \boldsymbol{b}_k & \mathrm{Bez}_{n-k}(F,G) \end{array} \right)$$

  2. **線形方程式系を解く**

$$\mathrm{Bez}_{n-k}(F,G)\boldsymbol{x} = \boldsymbol{b}_i \text{ for } 1 \leq i \leq k$$

  3. **解が GCD の係数：** $\mathrm{Bez}_{n-k}(F,G)\boldsymbol{x} = \boldsymbol{b}_i$ **の解**

$$\boldsymbol{x} = \boldsymbol{c}_i = \begin{pmatrix} c_{i,1} \\ c_{i,2} \\ \vdots \\ c_{i,n-k} \end{pmatrix}$$

の $c_{i,1}$ **は GCD の** x^{i-1} **の係数：**

$$C(x) = x^k + \sum_{i=1}^{k} c_{i,1} x^{i-1}$$

Barnett の定理における研究のポイント

- 線型方程式をいかに解くか？
  - LU 分解・高速演算
  - 最適化法
  - その他
- いつ悪条件になるのか？
- 多変数への拡張

前処理をしようとする人は多分だれもいない．

今日の話：近似 GCD 計算の安定化

問題

- 入力：$F, G \in \mathbb{F}[x]$ または $\mathbb{F}[x, u_1, \ldots, u_\ell]$
- 近似 GCD を求めるため，あるアルゴリズムを実行するときに精度良く (安定して) 結果を返したい

アルゴリズム_A ⇒ refinement_A

アルゴリズム_B ⇒ refinement_B

本講演では次を考えたい

前処理_* ⇒ アルゴリズム_A' ⇒ refinement_A'

前処理:条件数の改善_+ ⇒ アルゴリズム_B' ⇒

個人的な興味は、多変数の近似 GCD (1 変数の拡張)

条件数? ⇒ 前処理_+ ⇒ アルゴリズム_B' ⇒ 多変数に拡張

今日の話：近似 GCD 計算の安定化

問題

- 入力：$F, G \in \mathbb{F}[x]$ または $\mathbb{F}[x, u_1, \ldots, u_\ell]$
- 近似 GCD を求めるため，あるアルゴリズムを実行するときに精度良く (安定して) 結果を返したい

アルゴリズム_A ⇒ refinement_A

アルゴリズム_B ⇒ refinement_B

本講演では次を考えたい

前処理_* ⇒ アルゴリズム_A' ⇒ refinement_A'

前処理:条件数の改善_+ ⇒ アルゴリズム_B' ⇒

個人的な興味は、多変数の近似 GCD (1 変数の拡張)

条件数? ⇒ 前処理_+ ⇒ アルゴリズム_B' ⇒ 多変数に拡張

今日の話：近似 GCD 計算の安定化

問題

- 入力：$F, G \in \mathbb{F}[x]$ または $\mathbb{F}[x, u_1, \ldots, u_\ell]$
- 近似 GCD を求めるため，あるアルゴリズムを実行するときに精度良く (安定して) 結果を返したい

アルゴリズム_A ⇒ refinement_A

アルゴリズム_B ⇒ refinement_B

本講演では次を考えたい

前処理_* ⇒ アルゴリズム_A' ⇒ refinement_A'

前処理:条件数の改善_+ ⇒ アルゴリズム_B' ⇒

個人的な興味は、多変数の近似 GCD (1 変数の拡張)

条件数? ⇒ 前処理_+ ⇒ アルゴリズム_B' ⇒ 多変数に拡張

アルゴリズムによって考慮することは違うけど

例：線型方程式

$$\mathcal{A}\boldsymbol{x} = \boldsymbol{b}$$

- 直接法

$$\boldsymbol{x} = \mathcal{A}^{-1}\boldsymbol{b}$$

  - 計算の安定性：条件数に依存する
  - 修正 GKO 法 (高速 LU 分解)
- 反復法

$$\boldsymbol{x}^{(i+1)} = \mathcal{M}_1\boldsymbol{x}^{(i)} + \boldsymbol{r}^{(i)}$$

  - Gauss-Saidel 法, Jacobi 法，SOR 法：行列が優対角か否か
  - Krylov 部分空間法-based：
- 最適化法
  - 不動点定理に基づく (基本，null-space を計算する)

- 算法に依存する改良もあるが，条件数の改善は算法によらず有効

トピック１：
生成したBezout行列を細かく分解

- 算法：
  1. Bezout 行列 $\mathrm{Bez}(F,G) = (b_{i,j})_{1\le i,j\le n} \in \mathbb{F}^{n\times n}$ を構成

$$\begin{aligned}\mathrm{Bez}(F,G) &= \left(\begin{array}{ccc||c} \boldsymbol{b}_1 & \cdots & \boldsymbol{b}_k & \mathrm{Bez}_{n-k}(F,G) \end{array}\right) \\ &= \left(\begin{array}{ccc||c} * & \cdots & * & * \\ \hline \tilde{\boldsymbol{b}}_1 & \cdots & \tilde{\boldsymbol{b}}_k & \tilde{\mathrm{Bez}}_k(F,G) \end{array}\right)\end{aligned}$$

  2. 線形方程式系を解く&係数を取り出す

$$\mathrm{Bez}_{n-k}(F,G)\boldsymbol{x} = \boldsymbol{b}_i \text{ for } 1 \le i \le k$$

1. $\mathrm{Bez}_{n-k}(F,G) \in \mathbb{F}^{n\times(n-k)}$ なので、k 行余分に行を含んでいる．
   - 讃岐 2009 では、下の $(n-k)\times(n-k)$ 行列 $\tilde{\mathrm{Bez}}_k(F,G)$ を利用した
     - $\tilde{\mathrm{Bez}}_k(F,G)$ は対称行列
     - $\tilde{\mathrm{Bez}}_k(F,G)$ の悪条件性について
   - 他の方法では、余分な行を含んだ状態でアルゴリズムを適応

$\gamma = |\mathrm{lc}(\gcd(F,G))|/||\gcd(F,G)||$ とするとき

1. 行列に関して

$$\begin{pmatrix} O(1) & \cdots & O(1) & O(\gamma) \\ \vdots & \ddots & \vdots & \vdots \\ O(1) & \cdots & O(1) & O(\gamma) \\ O(\gamma) & \cdots & O(\gamma) & O(\gamma^2) \end{pmatrix} \propto \mathrm{Bez}(F,G)$$

2. 条件数に関して、$1/\gamma^k \propto \mathrm{cond}_2(\tilde{\mathrm{Bez}}_k(F,G))$
3. 解に関して

$$\begin{pmatrix} 1/\gamma \\ 1/\gamma^2 \\ \vdots \\ 1/\gamma^{n-k} \end{pmatrix} \propto \boldsymbol{x}$$

結局のところ，主係数に激しく依存する

- 条件数が大きい：線型方程式の精度が悪い，収束が遅い

条件数の改善 1 (効くかも)：

例 1

$$C(x) = (0.1x - 1)(x + 0.5)$$
$$F(x) = C(x)(x^3 + 4x - 1), \quad G(x) = C(x)(x^3 - 4x^2 + 1)$$

の Bezout 行列は次の通り

$$\mathcal{B}^{(1)}_{\text{before}} = \left(\begin{array}{ccc|cc} -1.0 & -0.900 & 1.6000 & -1.1500 & 0.1000 \\ -0.900 & -4.3100 & -4.7100 & 0.6150 & -0.0100 \\ \hline 1.6000 & -4.7100 & -12.0450 & 7.2500 & -0.6000 \\ -1.1500 & 0.6150 & 7.2500 & 2.6700 & -0.340 \\ 0.1000 & -0.0100 & -0.6000 & -0.340 & 0.040 \end{array}\right)$$

- $F(x) \to F(1/x) \times x^{\deg(F)}$
- $G(x) \to G(1/x) \times x^{\deg(G)}$

なる変換を施す (Bezout 行列がひっくり返るだけ)

$$\mathcal{B}^{(1)}_{\text{after}} = \left(\begin{array}{cc|ccc} -0.040 & 0.340 & 0.6000 & 0.0100 & -0.1000 \\ 0.340 & -2.6700 & -7.2500 & -0.6150 & 1.1500 \\ \hline 0.6000 & -7.2500 & 12.0450 & 4.7100 & -1.6000 \\ 0.0100 & -0.6150 & 4.7100 & 4.3100 & 0.900 \\ -0.1000 & 1.1500 & -1.6000 & 0.900 & 1.0 \end{array}\right)$$

.

${\mathcal{B}^{(1)}_{*}}_{3..5,3..5}$ の条件数

- $6.32 \times 10^6 \to 235.$ と大幅現象

効かない変換

- $x \to ax$ with $|a| > 1$

例 1:繰り返し

$$C(x) = (0.1x - 1)(x + 0.5)$$
$$F(x) = C(x)(x^3 + 4x - 1), \quad G(x) = C(x)(x^3 - 4x^2 + 1)$$

条件数は 6.32×10^6 **から**

- $a = 2$: $\to 6.42 \times 10^5$
- $a = 5$: $\to 1.16 \times 10^5$ **(行列表示)**
- $a = 10$:$\to 7.02 \times 10^4$

$$\left(\begin{array}{cc|ccc} -5.0 & -22.500 & 200.0 & -718.7500 & 312.5000 \\ -22.500 & -538.7500 & -2943.7500 & 1921.8750 & -156.2500 \\ \hline 200.0 & -2943.7500 & -37640.6250 & 113281.2500 & -46875.0 \\ -718.7500 & 1921.8750 & 113281.2500 & 208593.7500 & -132812.500 \\ 312.5000 & -156.2500 & -46875.0 & -132812.500 & 78125.0 \end{array}\right)$$

条件数の改善 2 (効果あり)

例 2

$$C(x) = 1/5.0x^2 - x + 1$$
$$F(x) = C(x)(x^3 + 4x^2 + 3x - 1), \quad G(x) = C(x)(x^3 - 4x^2 + 1)$$

$$\mathcal{B}^{(2)} = \left(\begin{array}{ccc|cc} -3.0 & 3.0 & & -2.60 & 2.0 & -0.400 \\ 3.0 & -17.0 & & 19.60 & -7.800 & 1.0 \\ -2.600 & 19.60 & & -12.92 & -1.200 & 0.9200 \\ 2.0 & -7.800 & & -1.200 & 6.2400 & -1.480 \\ -0.400 & 1.0 & & 0.9200 & -1.480 & 0.3200 \end{array}\right)$$

$\mathrm{cond}(\mathcal{B}^{(2)}_{345,3..5}) = 5.95 \times 10^4$ だが，主係数が小さそうな時は上の行から

- $\mathrm{cond}(\mathcal{B}^{(2)}_{123,3..5}) = 1.43 \times 10^3$
- $\mathrm{cond}(\mathcal{B}^{(2)}_{124,3..5}) = 1.23 \times 10^3$
- $\mathrm{cond}(\mathcal{B}^{(2)}_{125,3..5}) = 1.81 \times 10^3$
- $\mathrm{cond}(\mathcal{B}^{(2)}_{135,3..5}) = 1.18 \times 10^3$
- $\mathrm{cond}(\mathcal{B}^{(2)}_{234,3..5}) = 4.50 \times 10^3$
- $\mathrm{cond}(\mathcal{B}^{(2)}_{235,3..5}) = 8.80 \times 10^3$

条件数の改善 3 (少し手間をかける：効果的面)：

- k が小さい場合に，選択できる行が少ない
  $\Rightarrow$ 行列のサイズを増やす

$F(x) \to F'(x) = (ax+1)F(x)$ and $G(x) \to G'(x) = (bx+1)G(x)$

1. $a \neq 0$ and $b = 0$ のとき
   $\mathrm{Bez}(F', G') \in \mathbb{F}^{(n+1)\times(n+1)}$ and $\mathrm{Bez}_{n-k}(F', G') \in \mathbb{F}^{(n-k+1)\times(n-k+1)}$
2. $a \neq b$ and $a, b \neq 0$ のとき
   $\mathrm{Bez}(F', G') \in \mathbb{F}^{(n+2)\times(n+2)}$ and $\mathrm{Bez}_{n-k}(F', G') \in \mathbb{F}^{(n+1)\times(n-k+1)}$
3. $a = b$ and $a, b \neq 0$ のとき
   $\mathrm{Bez}(F', G') \in \mathbb{F}^{(n+2)\times(n+2)}$ and $\mathrm{Bez}_{n-k-1}(F', G') \in \mathbb{F}^{(n+2)\times(n-k)}$

$$\mathrm{Bez}(F, G) = \left(\begin{array}{ccc|c} \boldsymbol{b}_1 & \cdots & \boldsymbol{b}_k & \mathrm{Bez}_{n-k}(F, G) \end{array} \right)$$

$\Downarrow$

どれが有効か？

条件数の改善 3 (少し手間をかける：効果的面)：

- k が小さい場合に，選択できる行が少ない
  $\Rightarrow$ 行列のサイズを増やす

$F(x) \to F'(x) = (ax+1)F(x)$ and $G(x) \to G'(x) = (bx+1)G(x)$

1. $a \neq 0$ and $b = 0$ のとき
   $\mathrm{Bez}(F', G') \in \mathbb{F}^{(n+1)\times(n+1)}$ and $\mathrm{Bez}_{n-k}(F', G') \in \mathbb{F}^{(n-k+1)\times(n-k+1)}$
2. $a \neq b$ and $a, b \neq 0$ のとき
   $\mathrm{Bez}(F', G') \in \mathbb{F}^{(n+2)\times(n+2)}$ and $\mathrm{Bez}_{n-k}(F', G') \in \mathbb{F}^{(n+1)\times(n-k+1)}$
3. $a = b$ and $a, b \neq 0$ のとき
   $\mathrm{Bez}(F', G') \in \mathbb{F}^{(n+2)\times(n+2)}$ and $\mathrm{Bez}_{n-k-1}(F', G') \in \mathbb{F}^{(n+2)\times(n-k)}$

$$\mathrm{Bez}(F, G) = \left(\begin{array}{ccc|c} \boldsymbol{b}_1 & \cdots & \boldsymbol{b}_k & \mathrm{Bez}_{n-k}(F, G) \end{array} \right)$$

$\Downarrow$

どれが有効か？

$F(x) \to F'(x) = (ax+1)F(x)$ and $G(x) \to G'(x) = (bx+1)G(x)$

1. $a \neq 0$ and $b = 0$ のとき
   $\mathrm{Bez}(F', G') \in \mathbb{F}^{(n+1)\times(n+1)}$ and $\mathrm{Bez}_{n-k}(F', G') \in \mathbb{F}^{(n-k+1)\times(n-k+1)}$

   $\Rightarrow$ 変形していない共通因子の影響を受ける (効果なし)

2. $a \neq b$ and $a, b \neq 0$ のとき
   $\mathrm{Bez}(F', G') \in \mathbb{F}^{(n+2)\times(n+2)}$ and $\mathrm{Bez}_{n-k}(F', G') \in \mathbb{F}^{(n+1)\times(n-k+1)}$

   $\Rightarrow$ 変形していない共通因子の影響を受ける (効果なし)

3. $a = b$ and $a, b \neq 0$ のとき
   $\mathrm{Bez}(F', G') \in \mathbb{F}^{(n+2)\times(n+2)}$ and $\mathrm{Bez}_{n-k-1}(F', G') \in \mathbb{F}^{(n+2)\times(n-k)}$

   $\Rightarrow$ 共通因子が変わる (効果あり)
   $\Rightarrow$ 選択可能な行が 2 行増える (線型方程式の個数は 1 つ増える)

例 2:再び

$$C(x) = 1/5.0x^2 - x + 1$$
$$F(x) = C(x)(x^3 + 4x^2 + 3x - 1), \quad G(x) = C(x)(x^3 - 4x^2 + 1)$$

$F(x) \to F'(x) = (10x + 1)F(x)$ and $G(x) \to G'(x) = (10x + 1)G(x)$

- $\mathrm{cond}(\mathcal{B}^{(2)}_{456,4..6}) = 5.43 \times 10^4$
- $\mathrm{cond}(\mathcal{B}^{(2)}_{123,4..6}) = 1.46 \times 10^5$
- $\mathrm{cond}(\mathcal{B}^{(2)}_{124,4..6}) = 8.91 \times 10^3$
- $\mathrm{cond}(\mathcal{B}^{(2)}_{125,4..6}) = 9.61 \times 10^2$
- $\mathrm{cond}(\mathcal{B}^{(2)}_{126,4..6}) = 2.07 \times 10^2$
- $\mathrm{cond}(\mathcal{B}^{(2)}_{234,4..6}) = 1.27 \times 10^3$
- $\mathrm{cond}(\mathcal{B}^{(2)}_{235,4..6}) = 1.03 \times 10^3$
- $\mathrm{cond}(\mathcal{B}^{(2)}_{135,4..6}) = 9.01 \times 10^3$
- $\mathrm{cond}(\mathcal{B}^{(2)}_{156,4..6}) = 3.17 \times 10^3$

- **選択する基準は，低次と高次を組み合わせた．**

トピック2：
生成されるBezout行列を前処理で変化させると・・・

ここで扱うのは、線型方程式を解くための古典的な反復法 [1]

- Gauss-Seidel 法，SOR 法 [2]
- Jacobi 法 [3]

---

[1] Krylov 部分空間法に比べて早いわけではない

[2] 逐次過緩和法, successive overrelaxation method．Gauss-Seidel 法に加速パラメータを入れたもの

[3] 並列化可能．多変数への拡張の時に k 倍の高速化

Gauss-Seidel 法と Jacobi 法

$\mathcal{A} = (\mathcal{L} + \mathcal{D} + \mathcal{U})$ と分解したとき，次の反復式で $\mathcal{A}\boldsymbol{x} = \boldsymbol{b}$ を計算

Gauss-Seidel 法

$$(\mathcal{L} + \mathcal{D})\boldsymbol{x}^{(t+1)} = \boldsymbol{b} - \mathcal{U}\boldsymbol{x}^{(t)}$$

であり，各成分は次で計算可能．

$$x_i^{(t+1)} = \frac{1}{a_{i,i}}\left(b_i - \sum_{j=1}^{i-1} a_{i,j}x_j^{(t+1)} - \sum_{j=i+1}^{n} a_{i,j}x_j^{(t)}\right)$$

Jacobi 法

$$\mathcal{D}\boldsymbol{x}^{(t+1)} = \boldsymbol{b} - (\mathcal{L} + \mathcal{U})\boldsymbol{x}^{(t)}$$

であり，各成分は次で計算可能 (並列化可能)．

$$x_i^{(t+1)} = \frac{1}{a_{i,i}}\left(b_i - \sum_{j\neq j} a_{i,j}x_j^{(t)}\right)$$

Gauss-Seidel 法と Jacobi 法の収束条件

収束するための十分条件

- 行列 $\mathcal{A} = (a_{i,j})$ が (狭義) 優対角行列 $\Leftrightarrow$

$$|a_{i,i}| > \sum_{j \neq i} |a_{i,j}| \text{ for } 1 \leq i \leq n$$

数値計算においては

- 行列 A を (狭義) 優対角にする変換はたくさん研究されている.

多項式の積・係数から構成される Bezout 行列においては

- Bezout 行列の性質上，$\mathrm{Bez}(F, G)$ が優対角な行列になっていることはまれ.
- 前処理がほぼ 100%必要
- 数値計算における前処理は好ましくない (構造を壊す可能性あり)

Gauss-Seidel 法と Jacobi 法の収束条件

収束するための十分条件

- 行列 $\mathcal{A} = (a_{i,j})$ が (狭義) 優対角行列 $\Leftrightarrow$

$$|a_{i,i}| > \sum_{j \neq i} |a_{i,j}| \text{ for } 1 \leq i \leq n$$

数値計算においては

- 行列 A を (狭義) 優対角にする変換はたくさん研究されている.

多項式の積・係数から構成される Bezout 行列においては

- Bezout 行列の性質上，$\mathrm{Bez}(F, G)$ が優対角な行列になっていることはまれ.
- 前処理がほぼ 100%必要
- 数値計算における前処理は好ましくない (構造を壊す可能性あり)

Gauss-Seidel 法と Jacobi 法の収束条件

収束するための十分条件

- 行列 $\mathcal{A} = (a_{i,j})$ が (狭義) 優対角行列 $\Leftrightarrow$

$$|a_{i,i}| > \sum_{j \neq i} |a_{i,j}| \text{ for } 1 \leq i \leq n$$

数値計算においては

- 行列 A を (狭義) 優対角にする変換はたくさん研究されている.

多項式の積・係数から構成される Bezout 行列においては

- Bezout 行列の性質上，$\mathrm{Bez}(F, G)$ が優対角な行列になっていることはまれ.
- 前処理がほぼ 100%必要
- 数値計算における前処理は好ましくない (構造を壊す可能性あり)

例：主係数は微小でないように変換しておく

$$
\begin{aligned}
F(x) &= (\underline{2x^2} - x + 1)(x^3 + 4x - 1) \\
G(x) &= (\underline{2x^2} - x + 1)(x^3 - 4x^2 + 1)
\end{aligned}
$$

$$
\mathrm{Bez}(F,G) = \left(\begin{array}{ccc||cc}
-4 & 8 & & -14 & 10 & -4 \\
8 & -30 & & 44 & -50 & 12 \\
\hline\hline
-14 & 44 & & -62 & 64 & -8 \\
10 & -50 & & 64 & -84 & 8 \\
-4 & 12 & & -8 & 8 & 16
\end{array}\right)
$$

次の性質がある[4].

性質

1. $\mathrm{Bez}(aF,G) = a\mathrm{Bez}(F,G)$ with $a \in F$
2. $\mathrm{Bez}(F,G) = \mathrm{Bez}(F+aG,G) = \mathrm{Bez}(F+aG,G+bF)$ with $a,b \in F$

[4]前処理として使えない変換である

$(F, G) \to (a(x)F(x), b(x)G(x))$ を検討

例の改変 1：$a(x) \neq b(x)$ and $b(x) = 1$

$$
\begin{aligned}
F(x) &= (a_1 x - a_0)(2x^2 - x + 1)(x^3 + 4x - 1) \\
G(x) &= (2x^2 - x + 1)(x^3 - 4x^2 + 1))
\end{aligned}
$$

$$
\left(\begin{array}{cc||ccc}
4a_0 + a_1 & -8a_0 - 5a_1 & 14a_0 + 6a_1 & -10a_0 - 9a_1 & 4a_0 + a_1 & -2a_1 \\
-8a_0 - 5a_1 & 30a_0 + 13a_1 & -44a_0 - 20a_1 & 50a_0 + 19a_1 & -12a_0 - 5a_1 & 2a_1 \\
\hline
14a_0 + 6a_1 & -44a_0 - 20a_1 & 62a_0 + 32a_1 & -64a_0 - 32a_1 & 8a_0 + 10a_1 & 4a_1 \\
-10a_0 - 9a_1 & 50a_0 + 19a_1 & -64a_0 - 32a_1 & 84a_0 + 19a_1 & -8a_0 - 3a_1 & -10a_1 \\
4a_0 + a_1 & -12a_0 - 5a_1 & 8a_0 + 10a_1 & -8a_0 - 3a_1 & -16a_0 - a_1 & 18a_1 \\
-2a_1 & 2a_1 & 4a_1 & -10a_1 & 18a_1 & -4a_1
\end{array}\right)
$$

- 傾向：次数の大きな多項式の情報に置き換わりがち．$(a_1 x - a_0)$ に引っ張られる．
- 優対角行列にするのは難しそう．

$(F, G) \to (a(x)F(x), b(x)G(x))$ を検討

例の改変 2：$a(x) \neq b(x)$

$$
\begin{aligned}
F(x) &= (3x-2)(2x^2-x+1)(x^3+4x-1) \\
G(x) &= (4x-10)(2x^2-x+1)(x^3-4x^2+1))
\end{aligned}
$$

$$
\left(\begin{array}{cc||cccc}
-102 & 302 & -476 & 510 & -182 & 76 \\
302 & -1062 & 1768 & -2018 & 902 & -188 \\
\hline\hline
-476 & 1768 & -3008 & 3408 & -1588 & 120 \\
510 & -2018 & 3408 & -3866 & 1730 & 60 \\
-182 & 902 & -1588 & 1730 & -794 & -428 \\
76 & -188 & 120 & 60 & -428 & 280
\end{array}\right)
$$

- あまり，よいことはなさそう

例の改変 3：$a(x) = b(x)$

$$
\begin{aligned}
F(x) &= (100x - 2)(2x^2 - x + 1)(x^3 + 4x - 1) \\
G(x) &= (100x - 2)(2x^2 - x + 1)(x^3 - 4x^2 + 1))
\end{aligned}
$$

$$
\left(\begin{array}{ccc||ccc}
-12 & 612 & -632 & 1608 & -416 & 800 \\
612 & -31268 & 35100 & -85532 & 27440 & -42000 \\
-632 & 35100 & -180128 & 263132 & -338592 & 99600 \\
\hline
1608 & -85532 & 263132 & -333440 & 341584 & 20800 \\
-416 & 27440 & -338592 & 341584 & -598272 & -46400 \\
800 & -42000 & 99600 & 20800 & -46400 & 320000
\end{array}\right)
$$

- 線型方程式に利用する行列サイズは変わらないが，解く方程式の本数が増える．
- 状況は良さそう？

例の改変 3：$a(x) = b(x)$

$$
\begin{aligned}
F(x) &= (200x - 2)(2x^2 - x + 1)(x^3 + 4x - 1) \\
G(x) &= (200x - 2)(2x^2 - x + 1)(x^3 - 4x^2 + 1))
\end{aligned}
$$

$$
\left(\begin{array}{ccc||ccc}
-12 & 1212 & -1232 & 3208 & -816 & 1600 \\
1212 & -122468 & 130100 & -330932 & 94840 & -164000 \\
-1232 & 130100 & -700128 & 1026132 & -1337192 & 399200 \\
\hline
3208 & -330932 & 1026132 & -1306640 & 1343184 & 81600 \\
-816 & 94840 & -1337192 & 1343184 & -2396672 & -172800 \\
1600 & -164000 & 399200 & 81600 & -172800 & 1280000
\end{array}\right)
$$

例の改変 3：$a(x) = b(x)$

$$
\begin{aligned}
F(x) &= (x-2)(2x^2 - x + 1)(x^3 + 4x - 1) \\
G(x) &= (x-2)(2x^2 - x + 1)(x^3 - 4x^2 + 1))
\end{aligned}
$$

$$
\left(\begin{array}{ccc||ccc}
-12 & 18 & -38 & 24 & -20 & 8 \\
18 & -83 & 153 & -194 & 116 & -24 \\
-38 & 153 & -245 & 287 & -111 & 6 \\
\hline
24 & -194 & 287 & -404 & 133 & 10 \\
-20 & 116 & -111 & 133 & 84 & -68 \\
8 & -24 & 6 & 10 & -68 & 32
\end{array}\right)
$$

例の改変 3：$a(x) = b(x)$

$$
\begin{aligned}
F(x) &= (10x - 2)(2x^2 - x + 1)(x^3 + 4x - 1) \\
G(x) &= (10x - 2)(2x^2 - x + 1)(x^3 - 4x^2 + 1))
\end{aligned}
$$

$$
\left[\begin{array}{ccc||ccc}
-12 & 72 & -92 & 168 & -56 & 80 \\
72 & -488 & 900 & -1472 & 980 & -600 \\
-92 & 900 & -2828 & 3932 & -4152 & 960 \\
\hline
168 & -1472 & 3932 & -4760 & 4444 & 280 \\
-56 & 980 & -4152 & 4444 & -5712 & -1040 \\
80 & -600 & 960 & 280 & -1040 & 3200
\end{array}\right]
$$

- (対称) 優対角行列になった
- 大きすぎるのは良くないけど，少し傾斜をつけるのは有効

結局，どうすればよい？

- 理論的に考察

なぜ，優対角になりづらいのか？

- Bezout 行列が多項式の積の係数から構成される行列のため

$$\begin{aligned}\frac{F(x)G(y) - F(y)G(x)}{x - y} &= \sum b_{i,j} x^{i-1} y^{j-1} \\ &= \sum (f_* g_* - f_* g_*) x^{i-1} y_{j-1}\end{aligned}$$

- 中次くらいのところは，係数が大きくなる傾向がある．

$(F, G) \to (a(x)F(x), b(x)G(x))$ を検討

例の改変 3：$a(x) = b(x)$

$$
\begin{aligned}
F(x) &= (ax-1)(2x^2-x+1)(x^3+4x-1) \\
G(x) &= (ax-1)(2x^2-x+1)(x^3-4x^2+1))
\end{aligned}
$$

$$
\left(\begin{array}{ccc||ccc}
-3 & 3a+3 & -3a-8 & 8a+2 & -2a-4 & 4a \\
3a+3 & -3a^2-6a-17 & 3a^2+25a+25 & -8a^2-27a-33 & 2a^2+37a+10 & -4a^2-10a \\
-3a-8 & 3a^2+25a+25 & -17a^2-50a-32 & 25a^2+65a+33 & -33a^2-43a+2 & 10a^2-2a \\
\hline
8a+2 & -8a^2-27a-33 & 25a^2+65a+33 & -32a^2-66a-60 & 33a^2+58a-4 & 2a^2+4a \\
-2a-4 & 2a^2+37a+10 & -33a^2-43a+2 & 33a^2+58a-4 & -60a^2+8a+32 & -4a^2-32a \\
4a & -4a^2-10a & 10a^2-2a & 2a^2+4a & -4a^2-32a & 32a^2
\end{array}\right)
$$

- 変数 a の制約付き問題 (a の次数 $= 2$)
- $|a| > 1$

残る問題

- すべて，優対角に変換可能か？
- $(ax-1)$ で十分か？
- (ax^2+bx-1) を使うと？制約付き問題が難しくなる．

例の改変 3：$a(x) = b(x)$

$$
\begin{aligned}
F(x) &= (ax-1)(2x^2 - x + 1)(x^3 + 4x - 1) \\
G(x) &= (ax-1)(2x^2 - x + 1)(x^3 - 4x^2 + 1))
\end{aligned}
$$

$$
\left(\begin{array}{ccc||ccc}
-3 & 3a+3 & -3a-8 & 8a+2 & -2a-4 & 4a \\
3a+3 & -3a^2-6a-17 & 3a^2+25a+25 & -8a^2-27a-33 & 2a^2+37a+10 & -4a^2-10a \\
-3a-8 & 3a^2+25a+25 & -17a^2-50a-32 & 25a^2+65a+33 & -33a^2-43a+2 & 10a^2-2a \\
\hline
8a+2 & -8a^2-27a-33 & 25a^2+65a+33 & -32a^2-66a-60 & 33a^2+58a-4 & 2a^2+4a \\
-2a-4 & 2a^2+37a+10 & -33a^2-43a+2 & 33a^2+58a-4 & -60a^2+8a+32 & -4a^2-32a \\
4a & -4a^2-10a & 10a^2-2a & 2a^2+4a & -4a^2-32a & 32a^2
\end{array}\right)
$$

- 変数 a の制約付き問題 (a の次数 $= 2$)
- $|a| > 1$

残る問題

- すべて，優対角に変換可能か？
- $(ax-1)$ で十分か？
- $(ax^2 + bx - 1)$ を使うと？制約付き問題が難しくなる．

(狭義) 優対角であると・・・

- 実対称優対角行列は半正定値
  $\Rightarrow$ コレスキー分解が使える [5]

$$\mathrm{Bez}_{n-k}(F, G) = LL^T$$

[5] 計算量 $O(n^2)$

ゴール：Bezout 行列による多変数 GCD 計算

- 入力：$F(x), G(x) \in \mathbb{F}[x, u_1, \ldots, u_\ell]$ with $n = \deg(F) \geq \deg(G)$
- 算法：
  1. Bezout 行列 $\mathrm{Bez}(F, G) = (b_{i,j})_{1 \leq i,j \leq n} \in \mathbb{F}[\boldsymbol{u}]^{n \times n}$ を構成

$$\mathrm{Bez}(F, G) \quad = \quad \left(\begin{array}{ccc||c} * & * & * & * \\ \boldsymbol{b}_1 & \cdots & \boldsymbol{b}_k & \mathcal{B} \end{array} \right)$$

  2. 線形方程式系を解く

$$\boldsymbol{x} = {\mathcal{B}^{(0)}}^{-1} \boldsymbol{b}_i \text{ for } 1 \leq i \leq k$$

  3. リフティング
     $\mathcal{B}\boldsymbol{x} = \boldsymbol{b}$ を
     $(\mathcal{B}^{(0)} + \delta\mathcal{B}^{(1)} + (\text{高次}))(\boldsymbol{x}^{(0)} + \delta\boldsymbol{x}^{(1)} + (\text{高次})) = \boldsymbol{b}^{(0)} + \delta\boldsymbol{b}^{(1)} + (\text{高次})$
     と分解して，全次数 1 の斉次項をあつめる．

$$\begin{aligned} \mathcal{B}^{(0)}\delta\boldsymbol{x}^{(w)} + \delta\mathcal{B}^{(w)}\boldsymbol{x}^{(w-1)} &= \delta\boldsymbol{b}^{(2)} \\ \mathcal{B}^{(0)}\delta\boldsymbol{x}^{(w)} &= \delta\boldsymbol{b}^{(w)} - \delta\mathcal{B}^{(1)}\boldsymbol{x}^{(w-1)} - \ldots - \delta\mathcal{B}^{(w)}\boldsymbol{x}^{(0)} \end{aligned}$$

- 精度のよい逆行列計算が必要！