数理解析研究所講究録
1514巻 2006年 176-182

多項式行列の行列式の補間による計算II

木村欣司
KINJI KIMURA
JST・立教大学
JAPAN SCIENCE AND TECHNOLOGY AGENCY, FACULTY OF SCIENCE, RIKKYO UNIVERSITY

1 はじめに

A.J. Goldstein, R.L. Graham, A Hadamard-type bound on the coefficient of a determinant of polynomials, SIAM Review 16, 394-395, (1974) に記載されている公式は, 多変数多項式行列の行列式の計算において有用である. その公式の価値を改めて確認することがここでの目的である. その前に, この論文の公式のもととなったHadamard公式についても述べることとする. また, タイトなsupportにおけるNewton補間も多項式行列の行列式を高速に計算するために重要となるのでその詳細についても具体例を用いて丁寧に述べることとする.

2 行列式の評価公式

2.1 整数を要素とする行列の行列式の評価公式

$n \times n$ の行列 A に対して $\det(A)$ の評価は以下のようにおこなう.[4]

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix},$$

より

$$u_1 = (a_{1,1}, \ldots, a_{1,n}), \ldots, u_n = (a_{n,1}, \ldots, a_{n,n}),$$
$$v_1 = (a_{1,1}, \ldots, a_{n,1}), \ldots, v_n = (a_{1,n}, \ldots, a_{n,n}),$$

を定義すると, Hadamardの公式より

$$\det(A) \text{の絶対値} \leq \min(\|u_1\|_2 \|u_2\|_2 \cdots \|u_{n-1}\|_2 \|u_n\|_2, \|v_1\|_2 \|v_2\|_2 \cdots \|v_{n-1}\|_2 \|v_n\|_2) \equiv H,$$

は整数を要素とする行列の行列式を計算するときに重要な役割を果たすことはあらためて述べるまでもないが, その算法はさらに改良されたのでそれについてもここで述べることとする.

2.2 多変数多項式を要素とする行列の行列式の評価公式

多変数多項式の1ノルムは, 係数の絶対値の総和と定義する.

$$\begin{pmatrix} ||a_{1,1}||_1 & \cdots & ||a_{1,n}||_1 \\ \vdots & & \vdots \\ ||a_{n,1}||_1 & \cdots & ||a_{n,n}||_1 \end{pmatrix}$$

としてHadamardの公式を適用する. そのときの値を H_1 とすると

多変数多項式を要素とする行列の行列式の係数の絶対値最大 $\leq H_1$

が成立する. 詳しくは, [1] を参照されたい. この公式の利用価値はきわめて高いと考えここでその利用法を紹介する.

2.2.1 系:固有多項式の係数の絶対値最大の見積もり公式

$$\begin{pmatrix} |a_{1,1}|+|1| & \cdots & |a_{1,n}| \\ \vdots & \ddots & \vdots \\ |a_{n,1}| & \cdots & |a_{n,n}|+|1| \end{pmatrix}$$

としてHadamardの公式を適用する. そのときの値を H_2 とする H_2 は固有多項式の係数の絶対値の上界を与える.

3 整数を要素とする行列式の計算法

行列 A が与えられたとき, b を整数の乱数ベクトルとして適当な連立一次方程式 $Ax = b$ をHensel構成により解く.[5] 解 x を

$$x = \left(\frac{XN_1}{XD_1}, \cdots, \frac{XN_n}{XD_n}\right)^{\mathrm{T}}$$

とするとき, $\Phi = \mathrm{L.C.M.}(XD_1, XD_2, \cdots, XD_n)$ を計算する. 有限体上のLU分解においてfull rankでないとき $\Phi = 1$ とする. このとき, 整数の未知数を Ψ とすると, $\Phi \times \Psi = \det(A)$ が成立する. これからは, Ψ のみ計算することを考える. Hadamardの公式より

$$|\Phi| \times |\Psi| = |\det(A)| \leq H, \quad |\Psi| \leq \frac{H}{|\Phi|} \equiv H_0,$$

より, 上界が計算できる. $(\Phi \bmod p_i) \times (\Psi \bmod p_i) = \det(A) \bmod p_i$ より $\det(A) \bmod p_i$ が計算できると $\Psi \bmod p_i$ が計算できる. 有限体 $\mathbb{Z}/p\mathbb{Z}$ 上においてガウスの消去法を行うと $\det(A) \bmod p_i$ が計算できる. 逆元を計算すれば $\Psi \bmod p_i$ が計算できる. 以下, p_i を変化させて何度もガウスの消去法を繰り返し, 中国剰余定理をもちいて Ψ を合成する. 中国剰余定理の解の正規化条件が $\left[-\frac{\prod p_i - 1}{2}, \frac{\prod p_i - 1}{2}\right]$ であるから, $\frac{\prod p_i - 1}{2}$ が H_0 以上になると正しい Ψ を計算できたことになる.

4 整数を要素とする行列の固有多項式の計算

4.1 方法I

最小多項式の次数が行列サイズに満たない場合にも利用できる算法を紹介する．まず，固有多項式の係数の上界 H_2 がわかっていることを注意する．有限体 $\mathbb{Z}/p\mathbb{Z}$ 上で"ガウスの消去法の拡張"をおこなうと，いかなる整数を要素とする行列も上 Hessenberg 行列に変形できる．ここで，"ガウスの消去法の拡張"による上 Hessenberg 行列への変形は数値計算ではもはや過去の算法であるため老婆心ながらここで述べる．

n を行列サイズとし pivot の成分を $a(k,k)$ とすると

$$\alpha = \frac{a(i,k)}{a(k,k)}$$
$$a(i,j) \leftarrow a(i,j) - \alpha a(k,j) \quad j = k+1, ..., n$$

として消去法をおこなうのがガウスの消去法であるが，この行消去を行ったあと

$$a(m,k) \leftarrow a(m,k) + \alpha a(m,i) \quad m = 1, ..., n$$

として列に対して行を消去したときに用いた量を足しこみ固有値を不変にする算法である．さらに，上 Hessenberg 行列から有限体 $\mathbb{Z}/p\mathbb{Z}$ 上の固有多項式が計算できる．p_i を変化させて何度もガウスの消去法の拡張を繰り返す．中国剰余定理をもちいて固有多項式の係数を合成する．中国剰余定理の解の正規化条件が $\left[-\frac{\Pi p_i - 1}{2}, \frac{\Pi p_i - 1}{2}\right]$ であるから $\frac{\Pi p_i - 1}{2}$ が H_2 以上になると固有多項式を計算できたことになる.[2]

"ガウスの消去法の拡張"を利用して固有多項式を計算する代わりに Danilevsky 法を用いて有限体 $\mathbb{Z}/p\mathbb{Z}$ 上の固有多項式を計算することもできる.[3]

4.2 方法II

最小多項式の次数が行列サイズに一致する場合のみに利用できる算法を紹介する．正確には，一致しない場合にもこの算法を利用することができるがそのときに方法Iと比較するとこの方法のほうが非効率であるためこの方法を利用すべきでない．数値計算の GMRES 法に対応する．v を乱数ベクトルとして $A^k v$ を有限体 $\mathbb{Z}/p\mathbb{Z}$ ではなく整数で計算し

$$\left(\begin{array}{c|c|c|c} v & Av & \cdots & A^{n-1}v \end{array}\right)\begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix} = -A^n v$$

を連立一次方程式の解法で解く．$c_{n-1}, \cdots, c_0$ は固有多項式の係数となる．解があらかじめ整数であるとわかっているとき Hensel 構成の実装は工夫できる．整数から有理数に変換する必要がないのはあきらかであるが，数値計算の残差反復法のアナロジーであることからも明らかなように右辺の残差ベクトルが 0 になった時点で計算を終了してよい．x_j を $[-\frac{p-1}{2}, \frac{p-1}{2}]$ に規格化することにより残差が 0 になる j が存在することが保証されるのである．

4.3 注意

固有多項式の定数項は行列式であるため固有多項式が高速に計算できれば行列式も高速に計算できる. 固有多項式を求める方法 II は, 空間計算量は大きいが高速であるため行列式の計算法としても有力なように思えるがそれは正しくない. Hadamard の公式と有限体上のガウスの消去法を組み合わせた単純な方法で行列式を計算した場合には, 方法 II に実行時間の点で劣る. しかし, ここで紹介した方法を実装したところ固有多項式を求める方法 II に常に実行時間の点でも空間計算量の点でも優れているという結果を得ている. よって, 行列式は行列式のための算法を用いるべきであるということをここで強調しておく.

5 多変数多項式を要素とする行列の行列式の計算法

多変数版の Newton 補間を利用する.

$$A = \begin{pmatrix} x+y+z & xy \\ xyz & 2 \end{pmatrix}$$

が与えられたとき, 単純な計算により

$$\begin{aligned} |A| \;=\; & b_0 + b_1 z + b_2 z^2 + (b_3 + b_4 z + b_5 z^2) y + (b_6 + b_7 z) y^2 + ((b_9 + b_{10} z + b_{11} z^2) + \\ & (b_{12} + b_{13} z + b_{14} z^2) y + (b_{15} + b_{16} z) y^2) x + ((b_{18} + b_{19} z) + (b_{21} + b_{22} z) y + \\ & (b_{24} + b_{25} z) y^2) x^2, \end{aligned} \tag{1}$$

と仮定できる. 変数 x については

$$A \;=\; \begin{pmatrix} x+y+z & xy \\ & \\ xyz & 2 \end{pmatrix} \begin{matrix} 1 \\ + \\ 1 \end{matrix}$$

$$1 \quad + \quad 1$$

2 となる. つぎにすべての上界を計算する

variable	parameter	total degree
x	y, z	2
y	x, z	2
z	x, y	1
x, y	z	4
y, z	x	3
z, x	y	3
x, y, z		5

この表が (1) の根拠である.

supportがこのような複雑な場合, Newton補間はきわめて難しいように思えるがそれは正しくない. Aは, 説明のための例としてあまりにも複雑であるため次の例を使って説明する,

$$B = \begin{pmatrix} x+y & 2 \\ 3 & xy \end{pmatrix}.$$

Bにおいても同様に,

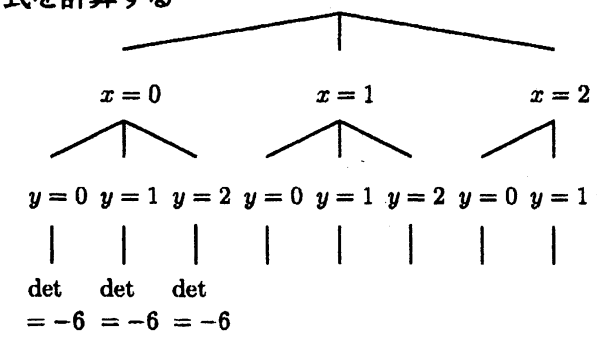
$$\begin{aligned} |B| &= (a_0 + a_1 y + a_2 y(y-1)) + x(a_3 + a_4 y + a_5 y(y-1)) \\ &\quad + x(x-1)(a_6 + a_7 y + a_8 y(y-1)), \quad a_8 = 0, \end{aligned} \tag{2}$$

と仮定する.

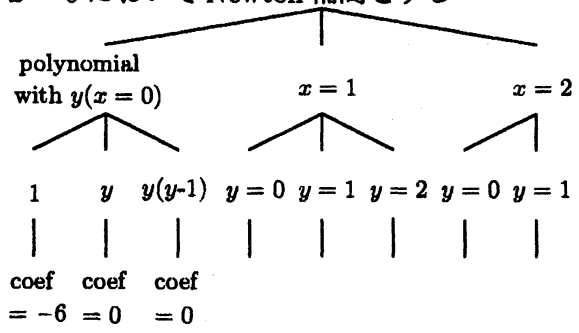
5.1 計算手順

ここでは説明のため$\mathbb{Q}$上で計算するが, 実際のプログラムでは$\mathbb{Z}/p\mathbb{Z}$を利用して計算する. 多変数多項式を要素とする行列式の係数についての上界公式により, 係数についてはすべての計算の後中国剰余定理によって復元される.

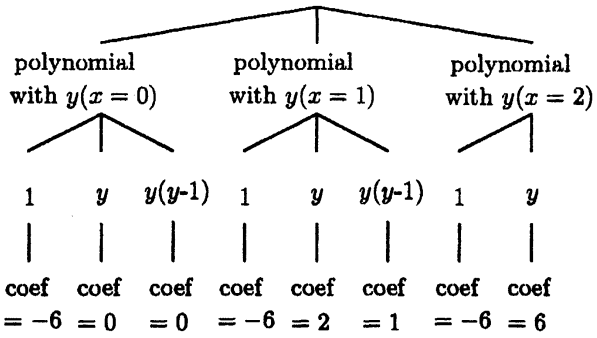
(2)から次の木を作り, $x=0$においてLU分解を利用して$y=0,1,2$のそれぞれの行列式を計算する



$x=0$においてNewton補間をする

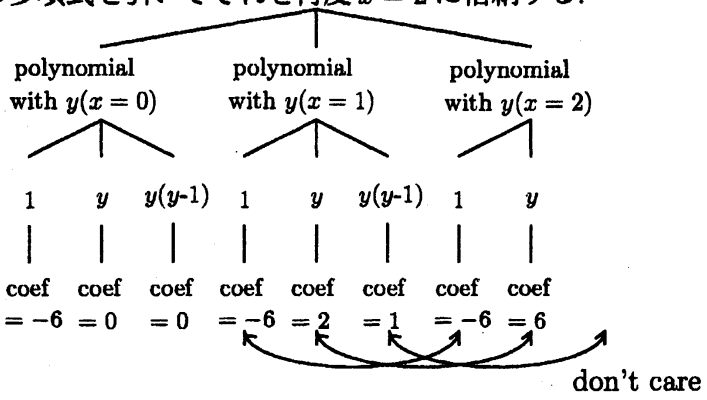


$x=1, x=2$においても同様の計算をおこなう.

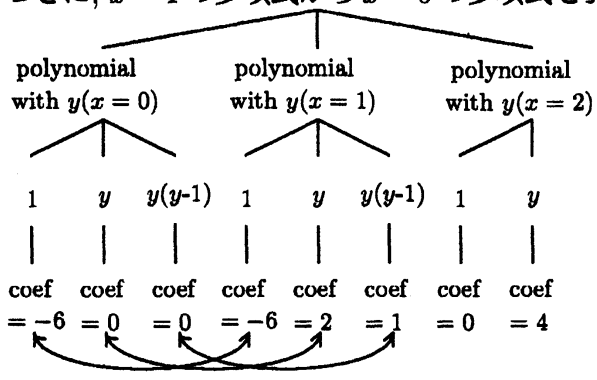


$x=2$ の多項式は正しくない. 正確には $\det(A)|_{x=2} = -6+6y+2y(y-1)$ である. しかし, Newton 補間は逐次補間であるためこのような途中で打ち切ったものを入力としても正しい計算ができるのである.

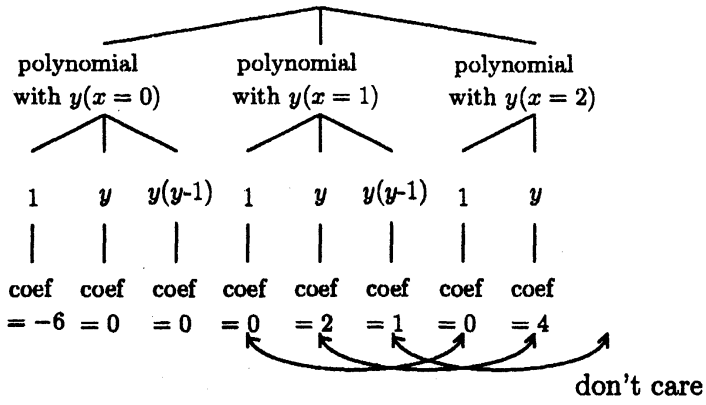
ここからは, 多項式を入力として Newton 補間をする. まず, $x=2$ の多項式から $x=1$ の多項式を引いてそれを再度 $x=2$ に格納する.



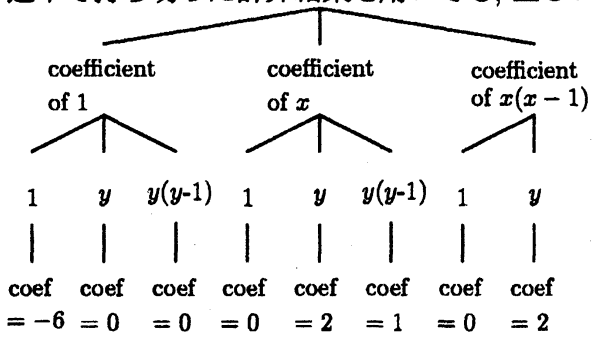
つぎに, $x=1$ の多項式から $x=0$ の多項式を引き, その結果を $x=1$ に格納する.



最後に $x=1$ の多項式から $x=0$ の多項式を引くと多項式における Newton 補間が完成する.



途中で打ち切った計算結果を用いても, 正しい結果が得られることを確認されたい.



6 タイミングデータ

非線形連立代数方程式を解くため multipolynomial resultant を計算する場合, 行列式の計算速度がその実行時間を左右する. 実験環境は, Intel Xeon 2.8GHz, Memory 2GByte として日本数学史の中にあらわれる問題をもちいて Singular と比較したところ, Singular が 13.33 秒を必要とし, ここで紹介した方法が 2.64 秒を必要とした. A.J. Goldstein, R.L. Graham による公式とタイトな support における Newton 補間がもたらした結果である.

参 考 文 献

[1] A.J. Goldstein, R.L. Graham, A Hadamard-type bound on the coefficient of a determinant of polynomials, SIAM Review 16, 394-395, (1974).

[2] S. Lo, M. Monagan, A. Wittkopf, A Modular Algorithm for Computing the Characteristic Polynomial of an Integer Matrix in Maple, http://www.cecm.sfu.ca/CAG/papers/CPpaper.pdf.

[3] 有本卓, 数値解析 (I), コロナ社, 東京, 1997.

[4] 高木貞治, 代数学講義 (改訂新版), 共立出版, 東京, 1965.

[5] 野呂正行, 横山和弘, グレブナー基底の計算 基礎篇, 東京大学出版会, 東京, 2003.