数理解析研究所講究録 1381 巻 2004 年 168-181

Interpolation solves open questions in discrete integrable system

神戸大学自然科学研究科 木村欣司 (Kinji Kimura)
Graduate School of Science and Technology,
Kobe University

1 Introduction

多項式補間を用いて 2 つの問題を解く. 多項式補間には, (i) 陽関数補間と (ii) 陰関数補間がある. (i) 陽関数補間は, Lagrange 補間や Newton 補間という代表的な算法が知られており工学において重要であることは, 言うまでもない. 一方, (ii) 陰関数補間に触れている教科書は少ない. 現状では, その算法は Gauss の消去法に帰着するため計算量の観点からあまり利用されることはないようである.

しかし, discrete integrable system を解くという立場からはどちらの算法も重要であり筆者にとっては両方とも興味深い対象である.

紙面の関係で (i) 陽関数補間についての話題は, その算法が discrete integrable system を解くためにどのように利用されるのか記述することを控える. また, この講演後の研究でこの話題について大きな進展があった. その進展とは, これから紹介する算法に付随する欠点をいかに克服するかという立場から生まれたものである. ここでは, あえて欠点を含む算法を紹介し次の講究録 「Computer Algebra-Design of Algorithms, Implementation and Applications」 においてその困難を克服する算法を紹介することとする.

2 陰関数補間によって解く

discrete integrable system は, 近年注目を集めている. 差分方程式によって力学系を記述する試みは新しくはないが, 解析関数によってその解を記述できるもしくは高い対称性をもつ差分方程式を研究することは最近活発におこなわれるようになった.

ここでは, 古典可積分系の代表例といえる Lagrange のコマの運動を記述する差分方程式を陰関数補間つかって解くことを試みる.

2.1 保存量を自動的に求める

n 階の差分方程式は, n 次元の点の運動を記述していると思える. 差分方程式の解がわかるということは, その差分方程式がどのような解空間のなかの点の運動を記述しているかを理解できるということと思える. 一般の差分方程式の解空間は, カオスをみれば明らかなようにその細部までわかることは極めて難しい. しかし, discrete integrable system にはその解空間が有理式によって具体的に表示できるものが存在する. この解空間の表示とは, 初期値空間という意味ではなく単に保存量のことである. Lagrange のコマの運動を記述する差分方程式においては, もしその保存量をもとめることができれば容易に解を求めることができる. それを自動的におこなう算法を紹介したい. もちろん, 陰関数多項式補間を用いるわけである.

一般の差分方程式を設定して記述することもできるが詳しい説明をおこなう目的で例を用いてその算法を紹介する. 陰関数多項式補間は現状では Gauss の消去法に帰着されるためその計算量を

低減する抜本的なアイディアはほとんど期待されない.

しかし, 多項式の support を決めるすなわち係数が 0 でない項を見積もるという目的で Gauss の消去法をおこなうのであれば行列要素が有理数ならば $\mathbf{F}_p$ に射影した空間において計算をすることは有効な手段である.

例として, 次の差分方程式の保存量をもとめる.

$$u_{n+1} = \frac{\alpha u_n + 1}{u_n u_{n-1}}. \tag{1}$$

次の算法によって保存量をもとめる.

1. Fix, a prime number p and $\alpha, u_0, u_1 \in \mathbf{F}_p$, where $\mathbf{F}_p$ is the finite prime field of order p.

2. Assume that an invariant curve is of the following form:

$$\begin{aligned} &a_0(u_n)^2(u_{n+1})^2 + a_1(u_n)^2 u_{n+1} + a_2 u_n (u_{n+1})^2 + a_3(u_n)^2 + a_4(u_{n+1})^2 \\ &+a_5 u_n u_{n+1} + a_6 u_n + a_7 u_{n+1} + a_8 = 0. \end{aligned} \tag{2}$$

   If the mapping has time-reversibility (invariance of equatinos by the transformation $n+1 \to n-1$), $a_1 = a_2, a_3 = a_4$ and $a_6 = a_7$

3. Calculate u_2, u_3, u_4, u_5, u_6 in $\mathbf{F}_p$ by using the eq. (1).
   If some u_i is equal to 0 in $\mathbf{F}_p$, exchange p and go back to 1.

4. Solve the following simultaneous linear eqations for $a_0, a_1, a_3, a_5, a_6, a_8$ in $\mathbf{F}_p$,

$$\begin{aligned} &a_0 u_0^2 u_1^2 + a_1 u_0 u_1 (u_0 + u_1) + a_3(u_0^2 + u_1^2) + a_5 u_0 u_1 + a_6(u_0 + u_1) + a_8 = 0, \\ &a_0 u_1^2 u_2^2 + a_1 u_1 u_2 (u_1 + u_2) + a_3(u_1^2 + u_2^2) + a_5 u_1 u_2 + a_6(u_1 + u_2) + a_8 = 0, \\ &\cdots \\ &a_0 u_5^2 u_6^2 + a_1 u_5 u_6 (u_5 + u_6) + a_3(u_5^2 + u_6^2) + a_5 u_5 u_6 + a_6(u_5 + u_6) + a_8 = 0. \end{aligned}$$

   If the rank is equal to the number of simultaneous linear equations, increase the degree of the invariant cureve and go back to 2.
   If $(p, \alpha, u_0, u_1) = (31991, 7, 2, 5)$ in the case of eq.(1), the solution of the eqs. (3)-(3) is $(a_0, a_1, a_3, a_5, a_6, a_8) = (0, 1, 0, -12, 7, 1)$ under scaling. If $(p, \alpha, u_0, u_1) = (32003, 7, 2, 5)$, the solution of the eqs. (3)-(3) is $(a_0, a_1, a_3, a_5, a_6, a_8) = (0, 1, 0, -12, 7, 1)$ under scaling.

5. By the Chinese remainder theorem, we guess that $a_0 = a_3 = 0$ and $a_1 = a_8 = 1$ in the solution over $\mathbf{Q}$. Furthermore, we guess that a_5 and a_6 only depend on the parameter α and initial conditions. Therefore, a_5 and a_6 are conserved quantities in $\mathbf{Q}$,

$$u_n u_{n+1}(u_n + u_{n+1}) + H_1 u_n u_{n+1} + H_2(u_n + u_{n+1}) + 1 = 0, \tag{3}$$

   where H_1, H_2 will be conserved quantities.

   If $n \to n-1$,

$$u_{n-1} u_n (u_{n-1} + u_n) + H_1 u_{n-1} u_n + H_2(u_{n-1} + u_n) + 1 = 0. \tag{4}$$

6. Solve the eqs. (3) and (4) for H_1, H_2 in $\mathbf{Q}$,

$$H_1 = \frac{-u_n^3 - u_n^2 u_{n-1} - u_n^2 u_{n+1} - u_{n-1}u_n u_{n+1} + 1}{u_n^2}, \tag{5}$$

$$H_2 = \frac{u_{n-1}u_n u_{n+1} - 1}{u_n}. \tag{6}$$

7. Using the eq.(1), we eliminate u_{n-1} in eqs. (5)-(6) over $\mathbf{Q}$,

$$H_1 = -\frac{u_{n-1}u_n(u_{n-1} + u_n) + \alpha(u_{n-1} + u_n) + 1}{u_{n-1}u_n}, \tag{7}$$

$$H_2 = \alpha. \tag{8}$$

8. Using the eq.(1), we can check H_1 is the conserved quantity in $\mathbf{Q}$.

ここでは, Support を決める目的で $\mathbf{F}_p$ をもちいたが中国剰余定理によって $\mathbf{Q}$ 上の真の解を求めることもできる. 詳しくは, [4] を参照されたい. 陰関数補間のための行列の Rank が 2 以上落ちた場合, 複数の代数曲面を得られる. もちろん従属なものを含んでいる. そのとき, 最小の生成元をもとめることは代数幾何学の未解決問題である. 現在のわれわれにできることは, グレブナ基底をもちいてすこしでもその従属なものを取り除くことである. 差分方程式が連立系の場合, 最後の check は保存量を差分方程式系のグレブナ基底によって正規簡約したものが 0 となることを確かめることに置き換わる.

2.2 Lagrange のコマの差分化

2.2.1 可積分なコマの微分方程式

$$\begin{aligned}
I_1\frac{d\omega_1}{dt} &= (I_2 - I_3)\omega_2\omega_3 + z_0\gamma_2 - y_0\gamma_3,\\
I_2\frac{d\omega_2}{dt} &= (I_3 - I_1)\omega_3\omega_1 + x_0\gamma_3 - z_0\gamma_1,\\
I_3\frac{d\omega_3}{dt} &= (I_1 - I_2)\omega_1\omega_2 + y_0\gamma_1 - x_0\gamma_2,\\
\frac{d\gamma_1}{dt} &= \omega_3\gamma_2 - \omega_2\gamma_3,\\
\frac{d\gamma_2}{dt} &= \omega_1\gamma_3 - \omega_3\gamma_1,\\
\frac{d\gamma_3}{dt} &= \omega_2\gamma_1 - \omega_1\gamma_2
\end{aligned}$$

可積分となる十分条件は, (Euler の場合)$x_0 = y_0 = z_0 = 0$ (Lagrange の場合)$A = B, x_0 = y_0 = 0$ (Kovalevskaya の場合)$A = B = 2C, z_0 = 0$. 以下, Lagrange の場合のみあつかう.

2.2.2 Lagrange のコマの保存量

1. 全エネルギー $H_1 = \frac{1}{2}(A\omega_1^2 + A\omega_2^2 + C\omega_3^2) + z_0\gamma_3$

2. 角運動量 $H_2 = A\omega_1\gamma_1 + A\omega_2\gamma_2 + C\omega_3\gamma_3$

3. 単位ベクトル $H_3 = \gamma_1^2 + \gamma_2^2 + \gamma_3^2$

4. 4番目の積分 $H_4 = C\omega_3$

Lagrange のコマの方程式は発散が 0 となるベクトル場を定めるので,M=1 を Jacobi の最終乗式としてもつ. よって 4 つの積分の存在が系を求積可能にする.

2.2.3 双線形形式による差分化

$$\omega_1 = \frac{g_1}{f}, \omega_2 = \frac{g_2}{f}, \omega_3 = \frac{g_3}{f}, \gamma_1 = \frac{g_4}{f}, \gamma_2 = \frac{g_5}{f}, \gamma_3 = \frac{g_6}{f}$$

変数変換すると

$$\begin{aligned}
I_1 D_t g_1 \cdot f &= (I_1 - I_3) g_2 g_3 + z_0 g_5 f, && (9)\\
I_1 D_t g_2 \cdot f &= (I_3 - I_1) g_3 g_1 - z_0 g_4 f, && (10)\\
I_3 D_t g_3 \cdot f &= 0, && (11)\\
D_t g_4 \cdot f &= g_3 g_5 - g_2 g_6, && (12)\\
D_t g_5 \cdot f &= g_1 g_6 - g_3 g_4, && (13)\\
D_t g_6 \cdot f &= g_2 g_4 - g_1 g_5. && (14)
\end{aligned}$$

ここで, D_t とは広田双線形演算子である

$$D_t g \cdot f = g_x f - g f_x.$$

射影座標の性質から,h を任意関数として

$$g_i \to h(t) g_i, f \to h(t) f$$

の変換のもとで (9)-(14) は不変である.

双線形方程式 (9)-(14) を差分化する. $f^{t+1} = f(t+\delta)$ として,

$$\begin{aligned}
I_1(g_1^{t+1} f^t - g_1^t f^{t+1})/\delta &= (I_1 - I_3)(g_2^{t+1} g_3^t + g_2^t g_3^{t+1})/2 + z_0(g_5^{t+1} f^t + f^{t+1} g_5^t)/2,\\
I_1(g_2^{t+1} f^t - g_2^t f^{t+1})/\delta &= (I_3 - I_1)(g_3^{t+1} g_1^t + g_3^t g_1^{t+1})/2 - z_0(g_4^{t+1} f^t + f^{t+1} g_4^t)/2,\\
I_3(g_3^{t+1} f^t - g_3^t f^{t+1})/\delta &= 0,\\
(g_4^{t+1} f^t - g_4^t f^{t+1})/\delta &= (g_3^{t+1} g_5^t + g_3^t g_5^{t+1})/2 - (g_2^{t+1} g_6^t + g_2^t g_6^{t+1})/2,\\
(g_5^{t+1} f^t - g_5^t f^{t+1})/\delta &= (g_1^{t+1} g_6^t + g_1^t g_6^{t+1})/2 - (g_3^{t+1} g_4^t + g_3^t g_4^{t+1})/2,\\
(g_6^{t+1} f^t - g_6^t f^{t+1})/\delta &= (g_2^{t+1} g_4^t + g_2^t g_4^{t+1})/2 - (g_1^{t+1} g_5^t + g_1^t g_5^{t+1})/2
\end{aligned}$$

とすれば, $\delta \to 0$ で微分方程式の双線形形式を復元する.

さらに, h^t を任意関数として

$$g_i^t \to h^t g_i^t, f^t \to h^t f^t$$

の変換のもとで方程式 (15)-(15) は不変である.

従属変数変換,

$$\omega_1 = \frac{g_1^t}{f^t}, \omega_2 = \frac{g_2^t}{f^t}, \omega_3 = \frac{g_3^t}{f^t}, \gamma_1 = \frac{g_4^t}{f^t}, \gamma_2 = \frac{g_5^t}{f^t}, \gamma_3 = \frac{g_6^t}{f^t}$$

により, Lagrange のコマを記述する差分方程式

$$\begin{aligned}
I_1(\omega_1^{t+1} - \omega_1^t)/\delta &= (I_1 - I_3)(\omega_2^{t+1}\omega_3^t + \omega_2^t\omega_3^{t+1})/2 + z_0(\gamma_2^{t+1} + \gamma_2^t)/2, \\
I_1(\omega_2^{t+1} - \omega_2^t)/\delta &= (I_3 - I_1)(\omega_3^{t+1}\omega_1^t + \omega_3^t\omega_1^{t+1})/2 - z_0(\gamma_1^{t+1} + \gamma_1^t)/2, \\
I_3(\omega_3^{t+1} - \omega_3^t)/\delta &= 0 \\
(\gamma_1^{t+1} - \gamma_1^t)/\delta &= (\omega_3^{t+1}\gamma_2^t + \omega_3^t\gamma_2^{t+1})/2 - (\omega_2^{t+1}\gamma_3^t + \omega_2^t\gamma_3^{t+1})/2, \\
(\gamma_2^{t+1} - \gamma_2^t)/\delta &= (\omega_1^{t+1}\gamma_3^t + \omega_1^t\gamma_3^{t+1})/2 - (\omega_3^{t+1}\gamma_1^t + \omega_3^t\gamma_1^{t+1})/2, \\
(\gamma_3^{t+1} - \gamma_3^t)/\delta &= (\omega_2^{t+1}\gamma_1^t + \omega_2^t\gamma_1^{t+1})/2 - (\omega_1^{t+1}\gamma_2^t + \omega_1^t\gamma_2^{t+1})/2
\end{aligned}$$

を得る.

$$\omega_i^t \to \frac{2}{\delta}\omega_i^t, \quad c = \omega_3^t \quad a = \frac{c(I_1 - I_3)}{I_1}, \quad z = \frac{z_0\delta^2}{4I_1},$$

により,

$$\omega_1^{t+1} - \omega_1^t = a(\omega_2^{t+1} + \omega_2^t) + z(\gamma_2^{t+1} + \gamma_2^t), \tag{15}$$

$$\omega_2^{t+1} - \omega_2^t = -a(\omega_1^t + \omega_1^{t+1}) - z(\gamma_1^{t+1} + \gamma_1^t), \tag{16}$$

$$\gamma_1^{t+1} - \gamma_1^t = c(\gamma_2^t + \gamma_2^{t+1}) - (\omega_2^{t+1}\gamma_3^t + \omega_2^t\gamma_3^{t+1}), \tag{17}$$

$$\gamma_2^{t+1} - \gamma_2^t = (\omega_1^{t+1}\gamma_3^t + \omega_1^t\gamma_3^{t+1}) - c(\gamma_1^t + \gamma_1^{t+1}), \tag{18}$$

$$\gamma_3^{t+1} - \gamma_3^t = (\omega_2^{t+1}\gamma_1^t + \omega_2^t\gamma_1^{t+1}) - (\omega_1^{t+1}\gamma_2^t + \omega_1^t\gamma_2^{t+1}). \tag{19}$$

行列による表示,

$$\begin{pmatrix} 1 & -a & 0 & -z & 0 \\ a & 1 & z & 0 & 0 \\ 0 & \gamma_3^t & 1 & -c & \omega_2^t \\ -\gamma_3^t & 0 & c & 1 & -\omega_1^t \\ \gamma_2^t & -\gamma_1^t & -\omega_2^t & \omega_1^t & 1 \end{pmatrix} \begin{pmatrix} \omega_1^{t+1} \\ \omega_2^{t+1} \\ \gamma_1^{t+1} \\ \gamma_2^{t+1} \\ \gamma_3^{t+1} \end{pmatrix} = \begin{pmatrix} \omega_1^t + a\omega_2^t + z\gamma_2^t \\ -a\omega_1^t + \gamma_2^t - z\gamma_1^t \\ \gamma_1^t + c\gamma_2^t \\ -c\gamma_1^t + \gamma_2^t \\ \gamma_3^t \end{pmatrix}, \tag{20}$$

$$\begin{pmatrix} 1 & a & 0 & z & 0 \\ -a & 1 & -z & 0 & 0 \\ 0 & -\gamma_3^t & 1 & c & -\omega_2^t \\ \gamma_3^t & 0 & -c & 1 & \omega_1^t \\ -\gamma_2^t & \gamma_1^t & \omega_2^t & -\omega_1^t & 1 \end{pmatrix} \begin{pmatrix} \omega_1^{t-1} \\ \omega_2^{t-1} \\ \gamma_1^{t-1} \\ \gamma_2^{t-1} \\ \gamma_3^{t-1} \end{pmatrix} = \begin{pmatrix} \omega_1^t - a\omega_2^t - z\gamma_2^t \\ a\omega_1^t + \gamma_2^t + z\gamma_1^t \\ \gamma_1^t - c\gamma_2^t \\ c\gamma_1^t + \gamma_2^t \\ \gamma_3^t \end{pmatrix}. \tag{21}$$

2.3 Lagrange のコマの差分方程式の保存量

$c = \omega_3^t$ としたので 3 つの保存量を求めることができれば解を保存量による求積操作によって求めることができる.

式 (3) に対応する代数曲面は,

1. 全エネルギー

$$H_1^0 = (\omega_1^t)^2 + (\omega_2^t)^2 - H_1^1\gamma_3^t - H_1^2(\gamma_3^t)^2 \tag{22}$$

2. 角運動量

$$H_2^0 = (\omega_1^t\gamma_1^t + \omega_2^t\gamma_2^t) - H_2^1\gamma_3^t - H_2^2(\gamma_3^t)^2 \tag{23}$$

3. 単位ベクトル

$$H_3^0 = (\gamma_1^t)^2 + (\gamma_2^t)^2 - H_3^1\gamma_3^t - H_3^2(\gamma_3^t)^2 \tag{24}$$

となる.

$H_1^0, H_1^1, H_1^2, H_2^0, H_2^1, H_2^2, H_3^0, H_3^1, H_3^2$ すべてが保存量となるわけだが, 従属であり本質的に独立なものは 3 つである.

$H_1^0, H_1^1, H_1^2, H_2^0, H_2^1, H_2^2, H_3^0, H_3^1, H_3^2$ の具体系を得るには以下の手順をとる.

式 (24) より,

$$H_3^0 = (\gamma_1^{t+1})^2 + (\gamma_2^{t+1})^2 - H_3^1\gamma_3^{t+1} - H_3^2(\gamma_3^{t+1})^2, \tag{25}$$

$$H_3^0 = (\gamma_1^t)^2 + (\gamma_2^t)^2 - H_3^1\gamma_3^t - H_3^2(\gamma_3^t)^2, \tag{26}$$

$$H_3^0 = (\gamma_1^{t-1})^2 + (\gamma_2^{t-1})^2 - H_3^1\gamma_3^{t-1} - H_3^2(\gamma_3^{t-1})^2. \tag{27}$$

式 (25)-(27) を H_3^0, H_3^1, H_3^2 について解く,

$$\begin{aligned} H_3^2 = {} & ((\gamma_3^{t+1} - \gamma_3^t)((\gamma_1^{t-1})^2 + (\gamma_2^{t-1})^2) - (\gamma_3^{t-1} - \gamma_3^t)((\gamma_1^{t+1})^2 + (\gamma_2^{t+1})^2) + \\ & (\gamma_3^{t-1} - \gamma_3^{t+1})((\gamma_1^t)^2 + (\gamma_2^t)^2))/((\gamma_3^{t-1} - \gamma_3^{t+1})(\gamma_3^{t-1} - \gamma_3^t)(\gamma_3^{t+1} - \gamma_3^t)). \end{aligned} \tag{28}$$

式 (20)(21) をもちいて式 (28) から $\gamma_1^{t+1}, \gamma_2^{t+1}, \gamma_3^{t+1}, \gamma_1^{t-1}, \gamma_2^{t-1}, \gamma_3^{t-1}$ を消去する,

$$H_3^2 = h_3^2(\omega_1^t, \omega_2^t, \gamma_1^t, \gamma_2^t, \gamma_3^t, a, c, z). \tag{29}$$

式 (29) が保存量であることを証明するには, 式 (15)-(19) のグレブナ基底を計算しそれによって式 (29) の正規簡約したものが 0 となることを確かめればよい.

本質的に独立なものは 3 つであり残りが従属であることは, 具体的に従属関係を計算することで確かめる.

$$H_1^1 = \frac{2z(1+ac)}{1+a^2}H_3^2 \tag{30}$$

$$H_1^2 = \frac{z^2}{1+a^2}H_3^2 \tag{31}$$

$$H_2^2 = \frac{-az}{1+a^2}H_3^2 \tag{32}$$

$$H_2^0 = \frac{2(a^2c^2-1)H_3^2 + z(1-ac)H_3^1 - 2a^2H_1^0 - 2(1+a^2)}{2az} \tag{33}$$

$$H_2^1 = \frac{2(1+ac-a^2-ca^3)H_3^2 - z(1+a^2)H_3^1 + 2(1+a^2)}{2a(q+a^2)} \tag{34}$$

$$\begin{aligned} H_3^0 = {} & (-4(1+a^2)(ac+1)(ac-1)(H_3^2)^2 + 4a^2(1+a^2)H_1^0H_3^2 - 4z(1+a^2)H_3^1H_3^2 \\ & -4(a^2c^2-a^2-2)(1+a^2)H_3^2 + 4a^2(1+a^2)H_1^0 + z^2(1+a^2)(H_3^1)^2 \\ & -4z(1+a^2)H_3^1 + 4(1+a^2)^2)/(4a^2z^2H_3^2) \end{aligned} \tag{35}$$

H_3^2, H_0^1, H_3^1 が独立であることは, Jacobi 行列の rank を調べることで確かめられる.
この保存量をもちいて求積できるわけであるが、詳しくは [1] を参照されたい.

3 陽関数補間によって解く

discrete integrable system の研究において, しばしば行列式を計算したいという要求がおこる.
しかし, その行列式の要素は discrete integrable system の研究においてはもはや数値でなく多変数多項式ないし有理式である. 多変数多項式ないしは有理式を要素とする行列式の計算は, サイズが小さい場合においてもその扱いは極めて難しい.
ここでは, その行列式を $\mathbf{F}_p$ 上の Lagrange 補間によって計算する算法を導入する.

3.1 有理式を要素とする行列式から多項式を要素とする行列式へ

$$A = \begin{vmatrix} \frac{f}{a} & \frac{f(f-1)}{a(b-1)} & \frac{fh}{a(c+5)} \\ \frac{(g+f-4)(g+1)}{c} & \frac{(g+1)g}{a} & \frac{g^2-1}{c^2} \\ \frac{c}{g} & \frac{b^2}{f-b} & \frac{a+b+h}{c-2} \end{vmatrix}$$

すべての行で分子で g.c.d, 分母で l.c.m. をとって変形する.

$$A' = \begin{vmatrix} (b-1)(c-5) & (c+5)(f-1) & (b-1)h \\ ac(g+f-4) & c^2g & a(g-1) \\ c(f-b)(c-2) & gb^2(c-2) & g(f-b)(a+b+h) \end{vmatrix}$$

l.c.m. をかけた合わせて割る.
g.c.d. をかけ合わせてさらに掛ける.

$$\det(A) = \frac{f(g+1)}{a^2c^2g(b-1)(c+5)(f-b)(c-2)}\det(A')$$

数式処理では, $\det(A)$ を計算することは $\det(A')$ を計算することにかわる. よって, 多項式を要素とする行列式のみを対象とすればよい.

3.2 整数を要素とする行列式の計算法

例として, 我々は次の行列式を計算する,

$$A = \begin{vmatrix} 3 & 1 \\ 2 & 4 \end{vmatrix}.$$

2 つの $\mathbf{F}_p$ において計算すると,

$$A \mod 3 = 1,$$
$$A \mod 5 = 0.$$

中国剰余定理と正規化

$$A \mod p \in \left[-\frac{p-1}{2}, \frac{p-1}{2}\right]$$

によって,

$$A \mod 15 = -5,$$

を得るがこれは正しい A の値ではない.

正しい値を得るために, Hadamard の公式をつかう.

$$\begin{aligned} u_1 &= (m_{1,1}, m_{1,2}, ..., m_{1,n-1}, m_{1,n}) \\ &... \\ u_n &= (m_{n,1}, m_{n,2}, ..., m_{n,n-1}, m_{n,n}) \\ v_1 &= (m_{1,1}, m_{2,1}, ..., m_{n-1,1}, m_{n,1}) \\ &... \\ v_n &= (m_{1,n}, m_{2,n}, ..., m_{n-1,n}, m_{n,n}), \end{aligned}$$

を,

$$M = \begin{vmatrix} m_{1,1} & m_{1,2} & ... & m_{1,n-1} & m_{1,n} \\ m_{2,1} & m_{2,2} & ... & m_{2,n-1} & m_{2,n} \\ ... & ... & ... & ... & ... \\ m_{n-1,1} & m_{n-1,2} & ... & m_{n-1,n-1} & m_{n-1,n} \\ m_{n,1} & m_{n,2} & ... & m_{n,n-1} & m_{n,n} \end{vmatrix},$$

より定義すると, Hadamard の公式より

$$\mathrm{abs}(M) \leq \min(\|u_1\|_2 \|u_2\|_2 ... \|u_{n-1}\|_2 \|u_n\|_2, \|v_1\|_2 \|v_2\|_2 ... \|v_{n-1}\|_2 \|v_n\|_2) = H.$$

A を評価できる. 実際に A に適用すると,

$$\mathrm{abs}(M) = 10 \leq \min(\sqrt{10}\sqrt{20}, \sqrt{13}\sqrt{17}) = 14.142...$$

となる.

α を

$$\alpha' \notin \left[-\frac{p-1}{2}, \frac{p-1}{2}\right],$$

とすると,

$$\left(\frac{p-1}{2}\right)^2 < (\alpha')^2.$$

である.

一方, p が

$$H^2 \leq \left(\frac{p-1}{2}\right)^2,$$

をみたすならば

$$\mathrm{abs}(A)^2 \leq H^2 \leq \left(\frac{p-1}{2}\right)^2 < (\alpha')^2.$$

が成立する.

すなわち,

$$H^2 \leq \left(\frac{p-1}{2}\right)^2,$$

は, 中国剰余定理による値が真の Z での値であることを保証する.

行列式 A では, p が 15 であるから

$$200 = H^2 \leq \left(\frac{p-1}{2}\right)^2 = 49,$$

保証されない.

3 つの $\mathbf{F}_p$ において計算すると,

$$\begin{aligned} A \mod 3 &= 1, \\ A \mod 5 &= 0, \\ A \mod 7 &= 3, \end{aligned}$$

であり, p は 105 であるから

$$200 = H^2 \leq \left(\frac{p-1}{2}\right)^2 = 2704$$

中国剰余定理の値が真の値であることを保証し

$$A \mod 105 = 10,$$

A=10 という Z における真の値を得る.

一見見事な解法であるが, 今日のめざましい多倍長数の扱いに関する研究 (GNU gmp) によってこの算法はもはや過去ものである.

多倍長数による Z 上の行列式の算法は, fraction free Gaussian elimination をもちいる.

3.3 fraction free Gaussian elimination

Gauss の消去法は, Z を要素とする行列式の計算が途中で Q 上の計算になるため使えない. この問題を解決するのが fraction free Gaussian elimination である.

fraction free Gaussian elimination とは, Hirota bilinear form による Gauss の消去法のことである.

$N \times N$ の行列 A

$$A = \begin{pmatrix} \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & a^k_{k-1,k-1} & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & a^k_{k,k} & \cdot & a^k_{k,j} & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & a^k_{i,k} & \cdot & a^k_{i,j} & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix}$$

に対して, 次の差分方程式

$$\text{Fraction-free Gauss} \quad a_{i,j}^{k+1} \leftarrow \frac{a_{i,j}^{k} a_{k,k}^{k} - a_{i,k}^{k} a_{k,j}^{k}}{a_{k-1,k-1}^{k-1}} \tag{36}$$

を適用する. $A_{N,N}^{N}$ が行列式を与える.
$a_{i,j}^{k} a_{k,k}^{k} - a_{i,k}^{k} a_{k,j}^{k}$ は必ず $a_{k-1,k-1}^{k-1}$ で割り切れる. その理由は, 式 (36) が分母を左辺に移項すれば Hirota bilinear form(Jacobi の恒等式) であるからである.

この算法は, 要素が整数の行列式に限らず多変数多項式の場合にも今日多くの数式処理ソフトでもちいられている.

3.4 $\mathbf{F}_p$ 上の Lagrange 補間

Lagrange 補間または Vandermonde 行列の連立一次方程式は,

$$\begin{pmatrix} 1 & s_0 & (s_0)^2 & \cdot & \cdot & (s_0)^{N-1} & (s_0)^N \\ 1 & s_1 & (s_1)^2 & \cdot & \cdot & (s_1)^{N-1} & (s_1)^N \\ 1 & s_2 & (s_2)^2 & \cdot & \cdot & (s_2)^{N-1} & (s_2)^N \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & s_{N-1} & (s_{N-1})^2 & \cdot & \cdot & (s_{N-1})^{N-1} & (s_{N-1})^N \\ 1 & s_N & (s_N)^2 & \cdot & \cdot & (s_N)^{N-1} & (s_N)^N \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ \cdot \\ \cdot \\ x_{N-1} \\ x_N \end{pmatrix} = \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ \cdot \\ \cdot \\ b_{N-1} \\ b_N \end{pmatrix} \tag{37}$$

$\mathbf{F}_p$ 上においても Non-sigular でありオーダー n^2 で解を得ることができる. 算法は, [3] を参照されたい.

[3] の算法は floating 用に書かれているが, 除算

$$\text{phi} = \Pi_{j \neq k}(x_j - x_k) \tag{38}$$

は $\mathbf{F}_p$ 上においても 0 となることはありえないためそのまま用いることができる.

3.5 多変数の Lagrange 補間

多変数の Lagrange 補間は, 多変数のフーリエ変換を知っていれば自明である.
2 変数多項式 $f(x,y)$ を補間することを試みる.

	$x=0$	$x=1$	$x=2$
$y=0$	$f(0,0)=-2$	$f(1,0)=-2$	$f(2,0)=-2$
$y=1$	$f(0,1)=-2$	$f(1,1)=0$	$f(2,1)=4$
$y=2$	$f(0,2)=-2$	$f(1,2)=4$	$f(2,2)=14$

(39)

$y=0$ として y を fix し, x についての変数 x の Lagrange 補間をおこなう.

$y=0$	x の 0 次の coef$=-2$	x の 1 次の coef$=0$	x の 2 次の coef$=0$

(40)

同様のことを $y=1$ と $y=2$ についてもおこなう.

$y=0$	x の 0 次の coef= -2	x の 1 次の coef= 0	x の 2 次の coef= 0
$y=1$	x の 0 次の coef= -2	x の 1 次の coef= 1	x の 2 次の coef= 1
$y=2$	x の 0 次の coef= -2	x の 1 次の coef= 4	x の 2 次の coef= 2

(41)

x の 0 次の係数について変数 y の Lagrange 補間をおこなう.

	x の 0 次		
	y の 0 次の coef= -2		
	y の 1 次の coef= 0		
	y の 2 次の coef= 0		

(42)

同様のことを x の 1 次と 2 次についてもおこなう.

	x の 0 次	x の 1 次	x の 2 次
y の 0 次	coef= -2	coef= 0	coef= 0
y の 1 次	coef= 0	coef= 0	coef= 1
y の 2 次	coef= 0	coef= 1	coef= 0

(43)

これを, 一般の M 変数の場合に拡張することは容易である.

1. sampling data で M 次元の配列すべての要素を埋める. そのときの配列を W とする,

$$W[k_0][k_1]...[k_{M-1}] \quad 0 \leq k_i \leq N_i \quad (i=0,...,M-1). \tag{44}$$

2. $k_1,...,k_{M-1}$ をすべての組合せにおいて, k_0 における Lagrange 補間をおこなう. その Lagrange 補間の結果得られた係数を $k_1,...,k_{M-1}$ を止めたときの $W[j][k_1]...[k_{M-1}](0 \leq i \leq N_0)$ に再度格納する. 計算量は, $(N_0)^2 \times N_1...N_{M-1}$.

3. 残りの変数 $k_1,...,k_{M-1}$ についても同様の操作をくりかえす.

以上の操作をおこなうと, 配列 W には多変数の Lagrange 補間の係数が格納されている. $\mathbf{F}_p$ 上においてもまったく同様である.

計算量は,

$$(N_0)^2 N_1...N_{M-1} + N_0(N_1)^2...N_{M-1} + ... + N_0N_1...(N_{M-1})^2 = N_0N_1...N_{M-1}(N_0 + N_1 + ... + N_{M-1}) \tag{45}$$

である.

3.6 多変数多項式を要素とする行列式の算法

以上の準備より, 多変数多項式を要素とする行列式の算法を導入する.

例として, 我々は次の行列式を計算する,

$$A = \begin{vmatrix} x+y & 1 \\ 2 & xy \end{vmatrix}.$$

補間のために, 各変数の行列式 A における最大次数をみつもる. x についての最大次数は, 1 行より 1+2 行より 1=2 と 1 列より 1+2 列より 1=2 を比較し 2 である. y についても同様に 2 である.

次に, Lagrange 補間のための配列をつくる,

	$x=0$	$x=1$	$x=2$
$y=0$	det= -2	det= -2	det= -2
$y=1$	det= -2	det= 0	det= 4
$y=2$	det= -2	det= 4	det= 14

(46)

この sampling data をもとに, 行列式を補間によってもとめる. sampling の算法は, 講演では Hadamard の公式による中国剰余定理による方法で demo をおこなったがその後の研究で fraction free Gaussian elimination 法が多くの例題で高速であったので後者をもちいる.

次に配列 (46) を mod 3 で射影する,

	$x=0$	$x=1$	$x=2$
$y=0$	det= 1	det= 1	det= 1
$y=1$	det= 1	det= 0	det= 1
$y=2$	det= 1	det= 1	det= 2

mod3. (47)

配列 (47) に F_3 上の Lagrange 補間を適用し行列式 A を配列で表現する,

	x の 0 次	x の 1 次	x の 2 次
y の 0 次	coef= 1	coef= 0	coef= 0
y の 1 次	coef= 0	coef= 0	coef= 1
y の 2 次	coef= 0	coef= 1	coef= 0

mod3. (48)

次に配列 (46) を mod 5 で射影する,

	$x=0$	$x=1$	$x=2$
$y=0$	det= 3	det= 3	det= 3
$y=1$	det= 3	det= 0	det= 4
$y=2$	det= 3	det= 4	det= 4

mod5. (49)

配列 (49) に F_5 上の Lagrange 補間を適用し行列式 A を配列で表現する,

	x の 0 次	x の 1 次	x の 2 次
y の 0 次	coef= 3	coef= 0	coef= 0
y の 1 次	coef= 0	coef= 0	coef= 1
y の 2 次	coef= 0	coef= 1	coef= 0

mod5. (50)

配列 (48)(50) に中国剰余定理を適用すると,

	x の 0 次	x の 1 次	x の 2 次
y の 0 次	coef= -2	coef= 0	coef= 0
y の 1 次	coef= 0	coef= 0	coef= 1
y の 2 次	coef= 0	coef= 1	coef= 0

(51)

となる.

すなわち, 行列式 A の候補は

$$A = -2 + x^2y + xy^2. \tag{52}$$

中国剰余定理の結果は候補である. sample point

$$(x,y) = (0,0),(1,0),(2,0),(0,1),(1,1),(2,1),(0,2),(1,2),(2,2) \tag{53}$$

を式 (52) に代入したとき, 配列 (46) を復元することを確認しなければならない.

これを, 一般の M 変数の場合に拡張する.

1. sampling data で M 次元の配列すべての要素を埋める. そのときの配列を U とする,

$$U[k_0][k_1]...[k_{M-1}] \quad 0 \leq k_i \leq N_i \quad (i = 0,...,M-1). \tag{54}$$

計算量は, 行列サイズを T とすると

$$N_0N_1...N_{M-1}T^3 \tag{55}$$

である. 一般には,

$$T^3 \geq N_0 + N_1 + ... + N_{M-1} \tag{56}$$

であるから, sampling が計算の主な部分である.

2. 配列 W の素数 p_1 のよる像を $\widetilde{U_1}$ において, $\mathbf{F}_p$ 上の多変数 Lagrange 補間をおこなう. そのときの, 行列式の係数の配列を $\widetilde{V_1}$ とする. また, $W_1 = \widetilde{V_1}$ とする.

3. 違う素数 p_2 を用いて同様の操作をおこなったものを $\widetilde{V_2}$ として, 配列 $\widetilde{V_1}$ と $\widetilde{V_2}$ に中国剰余定理を適用する. その結果を W_2 とする. このとき $W_1 = W_2$ ならば stable として終了する.

4. 同様の操作を stable になるまで繰り返す.

最後の stable になったものに sampling point を代入して真の解であるかを確かめる.

3.7 Lagrange 補間による計算の問題点

	$x=0$	$x=1$	$x=2$
$y=0$	det$=-2$	det$=-2$	det$=-2$
$y=1$	det$=-2$	det$=0$	det$=4$
$y=2$	det$=-2$	det$=4$	det$=14$

(57)

をつくるということは, A を

$$A = (a_0 + a_1y + a_2y^2) + (a_3 + a_4y + a_5y^2)x + (a_6 + a_7y + a_8y^2)x^2 \tag{58}$$

と仮定していることに等しい.

しかし, a_8 の項を仮定する必要があろうか?

$$A=\begin{vmatrix} x+y & 1 \\ 2 & xy \end{vmatrix}.$$

A の total degree を見積もる. total degree は, 1 行より 1+2 行より 2=3 と 1 列より 1+2 列より 2=3 を比較し 3 である. すなわち, $a_8=0$ である.

しかし, 敢えて a_8 まで仮定しているのは多変数の Lagrange 補間の算法を簡便にするためである. 実は $a_8=0$ として多変数の Lagrange 補間をおこなうこともできるがそこまでも含めると多変数の Lagrange 補間は難しい算法となる.

この困難を克服する算法を, 次の講究録
「Computer Algebra-Design of Algorithms,Implementation and Applications」に紹介する.

3.8 Timing data

Timing data は, 途中段階の算法であるためあえてとることを控える.

参考文献

[1] Kinji Kimura and Ryogo Hirota:"Discretization of the Lagrange Top" Journal of the Physical Society of Japan Vol.69 No.10, October,2000 3193-3199

[2] 高木貞治, 初等整数論講義 第 2 版. 共立出版 (1971).

[3] William H.Press, Saul A.Teukolsky, William T.Vetterling, and Brian P.Flanney,Numerical Recipes in C, CAMBRIDGE UNIVERSITY PRESS

[4] 野呂正行, 計算機代数, Rokko lectures in Mathematics. 神戸大学理学部数学教室