様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　２３　日現在

機関番号：　１４５０１
研究種目：　挑戦的萌芽研究
研究期間：　2014～2016
課題番号：　２６６１００３９

研究課題名（和文）有限体を用いた高精度数値計算法

研究課題名（英文）High precision numerical algorithms by finite fields

研究代表者

高山　信毅（Takayama, Nobuki）

神戸大学・理学研究科・教授

研究者番号：３０１８８０９９

交付決定額（研究期間全体）：（直接経費）　　1,500,000円

研究成果の概要（和文）：有限体を活用した高精度特に有理数上の数値解析手法を与え，実装および有効性を以下の場合に示した．(1) modular 計算と分散計算による一次変換の計算の高速化．(2) 常微分方程式の数値解析法 Bulirsch-Stoer method のQ上での効率的なアルゴリズム．(1) の応用は多変数A超幾何多項式の値の計算である．(2) の応用は線形常微分方程式の特異点近傍での数値解析である．

研究成果の概要（英文）：We give numerical analysis algorithms and implementations for the following problems over the rational number fields, which give high precision numerical outputs. (1) fast evaluation method of iterations of linear transformations by a modular arithmetic and a distributed computation. (2) an efficient variation of the Bulirsch-Stoer method to solve linear ordinary differential equations numerically over rational numbers. An application of (1) is an exact evaluation of A-hypergeometric polynomial. An application of (2) is a numerical analysis near singular points of linear ordinary differential equations.

研究分野：　数値解析

キーワード：　数値解析　有限体

1　研究開始当初の背景

数値解析の多くのアルゴリズム, たとえば常微分方程式の近似解を求めるための Runge-Kutta 法は double 型データを用いることを前提に研究されてきた. 常微分方程式の近似解を超高精度計算で求める手法はほぼ皆無といってよかった.

2　研究の目的

Runge-Kutta 法を代表とする常微分方程式の数値解析法は微分方程式の特異点近傍では誤差が大きくなるため、ステップ幅を小さく, かつ, 計算精度も高くして計算しないといけない. 特に不確定特異点では, 級数解が収束しないため, 特異点近傍でのみ級数解を用いて数値評価し, Runge-Kutta 法を使わない, という回避法が使えない. ステップ幅を小さく, かつ, 計算精度を高くしていくには, double 型データ, さらには任意精度浮動小数点数 (mpfr など) を使えばよいが, どちらも浮動小数点の計算のため, 分配則すら成立せず, 誤差評価をやりにくい. そこで単純な解決策として, すべて有理数を用いて計算を遂行するという, 方針が考えられる. しかしながら, 有理数のまま漸化式を計算していくと, 巨大な分子, 分母が出現する. これはいわゆる bignum の困難である. Newton 法においても全てを有理数で計算することにより, 解を高精度で計算することが可能となるがやはり一般に bignum の困難が生じる. (が, step 数が少ないので, こちらは有理数のみで計算しても問題ないと思われる. ただし有理式体などで Newton 法を行うと big polynomial 問題が生じる.)

有理数列 a_n の漸化式が与えられたとき, 有限体 $\mathbf{Z}/p\mathbf{Z}$ においてその漸化式できまる数列を $a_n(p)$ とする. さまざまな素数 p について数列 $a_n(p)$ を計算しておいて, そこから中国人剰余定理を用いて, 元の有理数列 a_n 復元し, さらに $a_n(p)$ を計算する段階では, 並列計算を行なう. これは bignum の困難を回避する計算代数における標準的手法であるが, 不思議なことに, Runge-Kutta 法や Newton 法の枠組みで考察されたことは無いようである. 本研究では, この方法の基礎づけ, 試験実装を与えることを目的とする.

3　研究の方法

1. Newton 法や Runge-Kutta 法の既存の実装を有理数対応にしていろいろな問題を解き有理数に対するその振る舞いを調べる.
2. 高速化のために有限体の活用を研究する.

有理数による計算の遅さを解消するため, 有限体の活用および並列計算を活用する.

中国人剰余定理による有理数の復元の計算の原理を例題を用いて説明しよう. 漸化式

$$a_{n+1} = a_n/2, a_1 = 1/6$$

を考える. $a_2 = \frac{1}{12}$ を中国人剰余定理により復元してみよう.

$3 \times 2 = 6 \equiv 1 \bmod 5$, $6 \times 1 = 6 \equiv 1 \bmod 5$ なので, この漸化式は $\mathbf{Z}/5\mathbf{Z}$ において,

$$a_{n+1} = 3a_n \bmod 5, \quad a_1 = 1$$

となり, $a_2 = 3$ となる. $p = 5$ の時の求める数という意味で $x_5 = 3$ と書く.

また, $4 \times 2 = 8 \equiv 1 \bmod 7$, $6 \times 6 = 36 \equiv 1 \bmod 7$ なので, この漸化式は $\mathbf{Z}/7\mathbf{Z}$ において,

$$a_{n+1} = 4a_n \bmod 7, \quad a_1 = 6$$

となり, $a_2 = 3$ となる. $p = 7$ の時の求める数という意味で $x_7 = 3$ と書く.

また, $6 \times 2 = 12 \equiv 1 \bmod 11$, $2 \times 6 = 12 \equiv 1 \bmod 11$ なので, この漸化式は $\mathbf{Z}/11\mathbf{Z}$ において,

$$a_{n+1} = 6a_n \bmod 11, \quad a_1 = 2$$

となり, $a_2 = 1$ となる. $p = 11$ の時の求める数という意味で $x_{11} = 1$ と書く.

さて $x = a_2 = \frac{z}{y}$, y, z は互いに素な整数, と置くとき, $xy = z$ なので次の式が成立する.

$$yx_5 \equiv z \bmod 5,\ yx_7 \equiv z \bmod 7,\ yx_{11} \equiv z \bmod 11$$

x_p 達に値を代入すると,

$$y \cdot 3 \equiv z \bmod 5,\ y \cdot 3 \equiv z \bmod 7,\ y \equiv z \bmod 11$$

これは次の連立不定方程式系に同値である.

$$3y - z + 5c_5 = 0, 3y - z + 7c_7 = 0, y - z + 11c_{11} = 0$$

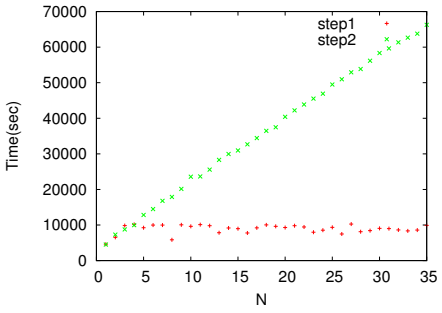
これの解を $1 \leq y, z \leq 14$ の範囲で探すと, $\frac{z}{y} = \frac{1}{12}$ を得る. このようにして元の数 a_2 が復元できた.

4 研究成果

有限体を活用した高精度特に有理数上の数値解析手法を与え, 実装および有効性を下記の場合に示した.

4.1 modular 計算と分散計算による一次変換の計算の高速化

多変数 A 超幾何多項式の値の計算にパラメータについての差分方程式 (漸化式) を用いると, double 型の範囲では, 誤差の蓄積が大きく真の値からおおきくずれる現象が見られる. これを回避するためには, すべてを有理数による正確計算で遂行すればよいが, この場合にはいわゆる bignum による速度低下が起きる. 計算代数での標準的手法である, mod 計算, 中国剰余定理, 分散計算 (まとめて modular method とよぶ) をこの場合に適用することにより, 高速に有理数上の正確計算が遂行可能であることを示した (論文 1). 次のグラフはわれわれの方法がサイズについての線形時間アルゴリズムであることを示している (下記論文 1 より引用).



実装は Risa/Asir のパッケージ gtt_ekn として公開している (その他, ホームページ等参照). 多変数超幾何多項式の値評価は分割表の条件付き推定への応用がある.

パッケージのマニュアルより我々の開発したソフトウエアを紹介する.

`gtt_ekn.chinese_itor(data,idlist)`

:: mod p で計算した結果 (ベクトル) から chinese remainder theorem, itor(integer to rational) で有理数ベクトルを得る.

戻り値. [val, n] ここで val は答え. また, $n = n_1 n_2 \cdots$.

data は [[val1,n_1],[val2,n_2], ...], ここで val mod n_1 = val1, val mod n_2 = val2, ...

idlist は chinese remainder theorem, itor を実行するサーバ ID のリスト.

この関数は中国人剰余定理を用いて val0 mod n_1 = val1, val0 mod n_2 = val2, ... となる val0 を求める. val に algorithm itor を適用する. sqrt(n) より val0 が大きい時は itor が適用されて val0 が有理数 val=a/b に変換される. つまり $bx = 1 \bmod n$ となる逆数 x を考えて, x*a % n = val0 となる数 val を戻す. 見つからないときは failure を戻す.

以下の例では [3!, $5^3$3!]=[6,750] が戻り値. 6 mod 109 =6, 750 mod 109=96 が最初の引数の [[6,96],109]. 以下同様.

```
gtt_ekn.setup(|nps=2,nprm=3,minp=101,
                    fgp="p_small.txt");
// 分散計算用サーバの初期化.
SS=gtt_ekn.get_svalue();
SS[0];
```

```
  [103,107,109]   // list of primes
SS[1];
  [0,2]           // list of server ID's
gtt_ekn.chinese_itor([[[ 6,96 ],109],
 [[ 6,29 ],103],[[ 6,1 ],107]],SS[1]);
  [[ 6 750 ],1201289]
// なお引数はスカラーでもよい.
gtt_ekn.chinese_itor([[96,109],
  [29,103]],SS[1]);
  [[ 750 ],11227]
```

4.2 Q 上での常微分方程式の数値解析法

常微分方程式の数値解析を有理数上で行う手法を与えた. 有理数での計算により, 誤差解析が数学的に明快になる他, 高精度計算が可能となる. Stoer-Bulirsch アルゴリズムを用いた常微分方程式の補間型数値解法と上記の modular method を組み合わせることにより, ある程度高速な有理数上の常微分方程式の数値解析アルゴリズムを与えることに成功した. 実装は Risa/Asir のパッケージ tk_bs として公開している (その他, ホームページ等参照).

ODE を解くための有名な Bulirsch-Stoer method の概要は以下のとおり.

入力: 微分方程式 $Y' = P(x)Y$ の $P(x)$, $x = t$ での Y の値 $Y(t)$. 数 H.

出力: $x = t + H$ での Y の値の近似値 $Y(t + H)$.

For $n \in [2, 4, 6, 8, 12, 16, 24, 32, 48, 64, 96]$,

1. $h = H/n$ を step size として $Y(t)$ より $Y(t+H)$ を通常の数値解法で解く. 値は n に依存するので $Y(t + H, n)$ と書く.
2. $Y(t + H, 2), Y(t + H, 4), \ldots, Y(t + H, n)$ より BS 法有理補間で $Y(t + H)$ の値をきめる. 値が十分妥当なら for を break

例: たとえば, $Y' = Y, Y(0) = 1$ を Euler 差分法で解くことは次の漸化式で $Y(t)$ を決めていくことに他ならない.

$$Y(t + h) = Y(t) + hY(t) = (1 + h)Y(t).$$

$H = 1$ としよう. この時, $h = H/n = 1/h$, $n = 1/h$ で, $Y(H, n) = (1 + h)^n$ である. BS 法では, $(1+h)^{1/h} = (1+1/n)^n$ の値達から $h = 0$ での値を有理補間推定をする.

さて我々の開発した, **Q** 上での Bulirsch-Stoer (BS) algorithm の概要は次のようになる.

1. 漸化式を解く部分は 分散計算 chinese remainder 版 matrix factorial (次の関数) を用いる (橘, 後藤, 高山, gtt_ekn, 4.2 節).

```
gtt_ekn.g_mat_fac_itor(Y,M,1,N,1,k,
   Tk_bs_plist,Tk_bs_idl);
```

2. 微分方程式の近似解法の誤差より精密な巨大有理数で計算しても意味がないので, BS 法の step 毎に巨大有理数は連分数近似で小さい有理数へ.

```
tk_approx_r.cont_frac(R,Err,Err_rel)
```

有理数の利点は, double の演算に伴う誤差 (たとえば分配法則等も成立せず) の解析が不要. 近似誤差の解析と連分数近似の誤差の解析でよいのでより明快.

この方法は例えば, Holonomic gradient method で解析したい常微分方程式の特異点近傍での高精度計算に有用である.

5 主な発表論文等

[雑誌論文] (計 1 件)

1. 橘義仁, 後藤良彰, 高山信毅, 2 元分割表に対する差分ホロノミック勾配法の実装, 出版予定, 数理研考究録, 査読なし.

[学会発表] (計 1 件)

1. 高山信毅, 常微分 (差分) 方程式用有理数対応数値解析パッケージ, Risa/Asir conference 2017, 金沢大学, 2017/03/28.

[図書] (計 0 件)
[産業財産権]
○ 出願状況 (計 0 件)
○ 取得状況 (計 0 件)

[その他] ホームページ等: http://www.math.kobe-u.ac.jp/OpenXM

6 研究組織

(1) 研究代表者
高山 信毅 (TAKAYAMA, Nobuki)
神戸大学・大学院理学研究科・教授
研究者番号: 30188099
(2) 研究分担者
研究者番号:
(3) 連携研究者
研究者番号:
(4) 研究協力者