数理解析研究所講究録
第1941巻 2015年 57-65
2014年度冬のLAシンポジウム [E-1]



# 行列多項式 $I+A+A^2+\cdots+A^{N-1}$ の計算における行列乗算回数

松本 耕太朗* 高木 直史† 高木 一義‡

## 1 はじめに

行列多項式 $G(N,A)=I+A+A^2+\cdots+A^{N-1}$ ($A$は正方行列) の計算は，三角行列の関数の計算 [6] や，ラドン変換における逆写像の計算 [7] などで現れる．$G(N,A)$ の計算において，計算時間の多くを占める演算は行列乗算である．特に $A$ の次数が大きい場合，行列の乗算に多大な計算時間を要するため，行列乗算の回数を削減することが重要である．また，行列乗算の回数を削減することは，丸め誤差の蓄積による精度の低下を抑制する上でも重要である．このため，行列乗算の回数の少ない計算法の研究がなされてきた．これまでに，$G(N,A)$ に特有の性質を利用することで，少ない行列乗算回数で計算を行う手法が考案されてきた [1–5]．これらの計算法では，行列乗算回数が $\log N$ に比例する．

Westreich [1] は，$N$ が $N=S\times T$ と因数分解できるとき，$G(N,A)=G(S,A)*G(T,A^S)$ により計算できることを利用し，$N$ の素因数分解に基づく計算法を提案した．(本稿では，$*$ は行列の乗算を表す.) さらに，この計算法による行列乗算回数が $3\lfloor\log_2 N\rfloor$ 以下であることを示した．

Lei と Nakamura [2] は，$N$ の2進表現に基づく計算法を提案し，$N$ の2進表現が $[1x_{n-2}x_{n-3}\cdots x_0]_2$ であるとき，行列乗算回数が $2\lfloor\log_2 N\rfloor-2+x_{n-2}$ であることを示し，これが行列乗算回数の下限であると推測した．Roy と Minocha [3] も，$N$ の2進表現に基づく計算法を提案し，行列乗算回数が $2\lfloor\log_2 N\rfloor-2$ 以上，$3\lfloor\log_2 N\rfloor-3$ 以下であることを示したが，行列乗算回数は Lei と Nakamura の計算法より少なくなることはない．

Dimitrov と Donevsky [4] は，$N$ の3進表現に基づく計算法を提案し，3進表現において桁の数が2である割合を $\beta$ とするとき，行列乗算回数がおよそ $(3+\beta)\lfloor\log_3 N\rfloor$ であることを示すことで，Lei と Nakamura の推測が正しくないことを示した．

Dimitrov と Cooklev [5] は，桁の数として2を含まない $N$ の2進3進混合表現に基づく計算法を提案し，いくつかの $N$ について，行列乗算回数がそれまでに知られていた計算法よりも少ないことを示した．

本稿では，これまでに提案された計算法よりも，必要な行列乗算回数が少ない $G(N,A)$ の計算法を提案する．まず，$G(S,A)*G(T,A^S)$ の計算において用いる $A^S$ の新しい計算法を示す．この計算法により，$S$ の値によらず，$A^S$ を $G(S,A)$ から一回の行列乗算で計算することができる．次に，この $A^S$ の計算法を，素因数分解に基づく手法，および混合基数表現に基づく手法それぞれに適用することで，行列乗算の回数の少ない計算法を提案する．それぞれの手法について，計算機を用いた実験による行列乗算回数の比較，および，マルコフ連鎖を用いた平均の行列乗算回数の比較を示す．

本稿の構成は次のようになる．2節で，既存の計算法と行列乗算回数について述べる．3節で，$G(N,A)$ の計算に関する新しい計算法を提案する．4節で，平均乗算回数に関する評価を行い，5節で，各 $N$ について，各計算法の行列乗算回数の比較を行う．5節で，本稿のまとめを述べる．

*京都大学
†京都大学
‡京都大学

## 2 既存の計算法

### 2.1 $N$ の素因数分解に基づく計算法 [1]

Westreich は，$N$ が $N = S \times T$ と因数分解できるとき，

$$G(N, A) = G(S, A) * G(T, A^S) \quad (1)$$

が成立することを利用し，$N$ の素因数分解に基づく計算法を提案した．この手法では，まず，対象とする $N$ の最大値を $N_{max}$ とし，$N_{max}$ 以下のすべての素数 $p$ について，事前に $G(p, A)$ と $A^p$ の行列乗算回数最小の計算法を求めておく．$A^p$ の計算においては，$G(p, A)$ の計算過程で現れる $A$ のべき乗を利用する．[1] に示された，31 以下の素数に対する $G(p, A)$ と $A^p$ の行列乗算回数最小の計算法を，表 1 に示す．(次節で述べるが，$A^p$ は，より少ない行列乗算回数で計算することができる．) $N$ が与えられれば，$N = \Pi_{i=1}^{m} p_i$ （$p_i \leq p_{i+1}$）と素因数分解し，

$$\begin{aligned} G(N, A) =& G(p_1, A) * G(p_2, A^{p_1}) * \cdots \\ & * G(p_m, A^{p_1 p_2 \cdots p_{m-1}}) \end{aligned}$$

により計算する．

この計算法による行列乗算の回数は，

$$\sum_{i=1}^{m} MMC_{min}(p_i) + \sum_{i=1}^{m-1} MPC(p_i) + m - 1$$

となる．ここに，$MMC_{min}(p_i)$ は $G(p_i, A)$ を計算するために必要な最小の行列乗算回数，$MPC(p_i)$ は $A^{p_i}$ を $G(p_i, A)$ の計算に現れる $A$ のべき乗を利用して計算するために必要な行列乗算回数である．この計算法では，$G(N, A)$ の計算に必要な行列乗算回数が $3 \cdot \lfloor \log_2 N \rfloor$ 以下であることが示されている．

たとえば，$G(35, A)$ は，$35 = 5 \cdot 7$ より，

$$\begin{aligned} G(35, A) &= G(5, A) * G(7, A^5) \\ &= (I + (I + A^2) * (A + A^2)) \\ &\quad * (I + (A^5 + (A^5)^2) \\ &\quad * (I + (A^5)^2 + (A^5)^4)) \end{aligned}$$

と計算される．行列乗算回数は，$G(5, A)$ の計算に 2 回，$A^5$ の計算に 2 回，$G(7, A^5)$ の計算に 3 回，$G(5, A)$ と $G(7, A^5)$ を掛け合わせるために 1 回必要となり，計 8 回となる．

この計算法では，事前に $N_{max}$ 以下のすべての素数 $p$ について，$G(p, A)$ の乗算回数最小の計算法を求めておく必要があり，実現が困難である．そのため，Westreich は，

$$G(ST + 1, A) = I + A * G(S, A) * G(T, A^S) \quad (2)$$

と計算できることに着目し，この計算法を改良した．

事前に小さいものから $k$ 番目までの素数，すなわち $\Pi_k = \{2, 3, 5, \cdots, p_k\}$ の元となる素数に限り，$G(p, A)$ と $A^p$ の乗算回数最小の計算法を求めておく．$N$ が与えられれば，これを素因数分解し，$k$ 番目より大きな素数 $q$ を含む場合は，$G(q, B)$ （$B$ は $A$ のべき乗）を $I + B * G(q - 1, B)$ により計算する．$G(q - 1, B)$ の計算は，$q - 1$ の素因数分解に基づいて行う．再び $k$ 番目より大きな素数が現れれば，この方法を再帰的に適用する．

例として，$N_{max} = 1000$，素数の集合 $\Pi_k$ として $\sqrt{N_{max}}$ 以下のすべての素数をとるとき（$k = 11$）の，$N = 205$ の場合の $G(205, A)$ の計算を考える．$205 = 5 \cdot 41 = 5 \cdot (2 \cdot 2 \cdot 2 \cdot 5 + 1)$ より，$G(205, A)$ は，

$$\begin{aligned} G(205, A) =& (I + (I + A^2) * (A + A^2)) \\ & * (I + A^5 * (I + A^5) * (I + A^{10}) \\ & * (I + A^{20}) \\ & * (I + (I + A^{80}) * (A^{40} + A^{80}))) \end{aligned}$$

として計算される．この計算に必要な行列乗算の回数は 14 となる．

### 2.2 $N$ の 2 進表現に基づく計算法 [2]

Lei と Nakamura は，$G$ の因数分解に基づく式である，式 (1)，および，式 (2) において，$S = 2$ の場合に基づき，以下の場合分けに従い再帰的に計算を

表 1: 31 以下の素数に対する $G(p,A)$ および $A^p$ の行列乗算回数最小の計算法

| $p$ | $G(p,A)$ | | $A^p$ | |
|---|---|---|---|---|
| | 計算法 | 乗算回数 | 計算法 | 乗算回数 |
| 2 | $I+A$ | 0 | $A*A$ | 1 |
| 3 | $I+(A+A^2)$ | 1 | $A*A^2$ | 1 |
| 5 | $I+(I+A^2)*(A+A^2)$ | 2 | $A*A^2*A^2$ | 2 |
| 7 | $I+(A+A^2)*(I+A^2+A^4)$ | 3 | $A*A^2*A^4$ | 2 |
| 11 | $I+(A+A^2)*(I+(I+A^4)*(A^2+A^4))$ | 4 | $A*A^2*A^4*A^4$ | 3 |
| 13 | $I+(I+A^2)*(A+A^2)*(I+A^4+A^8)$ | 5 | $A*A^4*A^8$ | 2 |
| 17 | $I+(I+A^2)*(A+A^2)*(I+A^4)*(I+A^8)$ | 6 | $A*A^8*A^8$ | 2 |
| 19 | $I+(A+A^2)*(I+A^2+A^4)*(I+A^6+A^{12})$ | 6 | $A*A^6*A^{12}$ | 2 |
| 23 | $I+(A+A^2)*(I+(A^2+A^4)*(I+(I+A^8)*(A^4+A^8))$ | 6 | $A*A^2*A^4*A^8*A^8$ | 4 |
| 29 | $I+(I+A^2)*(A+A^2)*(I+(A^4+A^8)*(I+A^8+A^{16}))$ | 7 | $A*A^4*A^8*A^{16}$ | 3 |
| 31 | $I+(A+A^2)*(I+A^2+A^4)*(I+(I+A^{12})*(A^6+A^{12}))$ | 7 | $A*A^6*A^{12}*A^{12}$ | 3 |

行う計算法を提案した.(以降, 2 進計算法と呼ぶ.)

$$G(N,A)=\begin{cases}(I+A)*G(T,A^2) & \text{if } N=2T\\ I+(A+A^2)*G(T,A^2) & \text{if } N=2T+1\end{cases}$$

この計算法では, $N=2T$ の場合は, 式 (1) を適用する式変形を行い, $N=2T+1$ の場合は, 式 (2) を適用する式変形を行う. これらを再帰的に適用することで, 計算式を得る. 再帰の各ステップでは, $A$ から $A^2$ を計算するための乗算, および, $(I+A)$ もしくは $(A+A^2)$ と $G(T,A^2)$ との乗算の計 2 回の行列乗算が必要である. また, この計算法により得られる $G(N,A)$ の式は, $N$ の 2 進展開に対応する.

一般に, 2 進計算法では, $G(N,A)$ の計算における行列乗算の回数 $MMC_2(N)$ は, $N$ の 2 進表現が $[1x_{n-2}\cdots x_0]_2$ のとき, $2(\lfloor\log_2 N\rfloor-1)+x_{n-2}$ となる. $n=\lfloor\log_2 N\rfloor+1$ であるので, $n$ を用いて $MMC_2(N)$ を表すと, $MMC_2(N)=2(n-2)+x_{n-2}$ となる.

## 2.3 $N$ の 3 進表現に基づく計算法 [4]

Dimitrov と Donevsky は, 式 (1), および, 式 (2) において $S=3$ の場合に基づき, 以下の場合分けに従い再帰的に計算を行うアルゴリズムを提案した. (以降, 3 進計算法と呼ぶ.)

$$G(N,A)=\begin{cases}(I+A+A^2)*G(T,A^3)\\ \qquad \text{if } N=3T\\ I+(A+A^2+A^3)*G(T,A^3)\\ \qquad \text{if } N=3T+1\\ I+A+A*(A+A^2+A^3)*G(T,A^3)\\ \qquad \text{if } N=3T+2\end{cases}$$

この計算法では, 2 進計算法と同様に, $N=3T$ の場合は, 式 (1) を適用し, $N=3T+1$ の場合は, 式 (2) を適用する. $N=3T+2$ の場合は, これらの二つの場合より一回多い行列乗算回数により計算する. これらを再帰的に適用することで, 計算式を得る. したがって, 再帰の各ステップでは, $N=3T$ のとき, および, $N=3T+1$ のときの行列乗算は 3 回, $N=3T+2$ のときの行列乗算は 4 回となる.

この計算法により得られる $G(N,A)$ の式は, $N$ の 3 進展開と対応する.

一般に, 3 進計算法では, $N$ の 3 進表現が $[x_{n-1}x_{n-2}\cdots x_0]_3$ であるとき, $G(N,A)$ の計算にお

ける行列乗算回数 $MMC_3(N)$ は，

$$MMC_3(N) = \sum_{i=0}^{n-3} f(x_i) + \epsilon_3(N)$$

となる．ここで，

$$f(x_i) = \begin{cases} 3 & \text{if } x_i = 0,1 \\ 4 & \text{if } x_i = 2 \end{cases}$$

$$\epsilon_3(N) = \begin{cases} x_{n-2} + 1 & \text{if } x_{n-1} = 1 \\ f(x_{n-2}) & \text{if } x_{n-1} = 2 \end{cases}$$

である．

3進計算法では，3進表現において桁の数が2である割合が $2\log_2 3 - 3$ 未満となる $N$ については，2進計算法よりも乗算回数が少なくなる．しかし，桁の数が2である割合が多い $N$ については，2進計算法よりも乗算回数が多くなる．

### 2.4 $N$ の2進3進混合表現に基づく計算法 [5]

3進計算法では，$N = 3T+2$ の場合に対応するステップでの行列乗算回数が，他の場合の行列乗算回数より1回多くなる．そこで，Dimitrov と Cooklev は，3進計算法を改良し，$N = 3T+2$ の場合には2進計算法を適用し，以下の場合分けに従い再帰的に計算を行うアルゴリズムを提案した．(以降，DB (double base) 法と呼ぶ.)

$$G(N, A) = \begin{cases} (I + A + A^2) * G(T, A^3) \\ \quad \text{if } N = 3T \\ I + (A + A^2 + A^3) * G(T, A^3) \\ \quad \text{if } N = 3T + 1 \\ (I + A) * G(3T + 1, A^2) \\ \quad \text{if } N = 3(2T) + 2 \\ I + (A + A^2) * G(3T + 2, A^2) \\ \quad \text{if } N = 3(2T + 1) + 2 \end{cases} \tag{3}$$

この場合分けに従い得られる $G$ の式は，$N$ の桁の値として2を含まない2進3進混合表現への展開と対応している．

DB 法による $G(N, A)$ の行列乗算回数 $MMC_{DB}(N)$ は，

$$MMC_{DB}(N) = \sum_{i=0}^{n-3} r_i + x_{n-2}^{[r_{n-2}]} + r_{n-2} - 2$$

多くの $N$ については，DB 法による計算に必要な行列乗算回数は，2進計算法や3進計算法による計算に必要な行列乗算回数以下となる．たとえば，$N = 35$ の場合，2進計算法，3進計算法，DB 法により計算する場合に必要な行列乗算回数は，それぞれ8，9，8回となる．また，$N$ の桁の数に2を含まない2進3進混合表現は，複数存在する．式 (3) に従う展開が，それらの表現と対応する計算式のなかで，行列乗算回数最小になるとは限らない．

## 3 提案手法

$G(p, A)$ から $A^p$ を計算する新しい方法と，剰余が1の場合に対応する式に関する新しい計算法を提案し，それを因数分解による手法と，混合基数表現に基づく手法にそれぞれ組み込むことで，$G(N, A)$ を計算するための新しい計算法を提案する．

### 3.1 $G(p, A)$ からの $A^p$ の計算法

Westreich は，$A^p$ を $G(p, A)$ の計算で現れる $A$ のべき乗を利用し，$\log_2 p$ 回以下の行列乗算で求めていた [1]．本項では，$G(p, A)$ から $A^p$ を1回の行列乗算回数で計算する方法を説明する．$G(p, A)$ が得られているとき，次式に示すように，$A^p$ は，$p$ によらず1回の行列乗算で計算することができる．

$$A^p = G(p, A) * (A - I) + I$$

この計算法により，Westreich の手法と比較して，5以上の素数で因数分解する場合は，$A^p$ の計算法として，行列乗算回数を削減することができる．

例として，$G(35,A)$ の計算を考える．素因数分解による手法では，次式に示すように，$G$ の素因数分解に基づき計算される．

$$\begin{aligned} G(35,A) &= G(5,A) * G(7,A^5) \\ &= (I+(I+A^2)*(A+A^2)) * G(7,A^5) \end{aligned}$$

Westreich の計算法では，表 1 にあるように，$A^5$ を，$A^5 = A*A^2*A^2$ として 2 回の行列乗算で計算する．一方，ここで提案した計算法では，$A^5 = G(5,A)*(A-I)+I$ として 1 回の行列乗算で計算できる．

### 3.2 剰余が 1 の場合と対応する計算法

$N = ST+1$ が成り立つとき，$G(N,A)$ は次式のように変形できる．

$$G(N,A) = I + A * G(S,A) * G(T,A^S)$$

2 進計算法の分岐式にあるように，$S=2$ のとき，この式を式 (4) として計算することで，$G(2T,A)$ の計算の $G(T,A^2)$ の計算への還元を，$G(2T+1,A)$ の計算の $G(T,A^2)$ の計算への還元（式 (5)）に必要な行列乗算回数と同じ行列乗算回数で行うことができる．

$$G(N,A) = I + (A+A^2) * G(T,A^2) \quad (4)$$

$$G(N,A) = (I+A) * G(T,A^2) \quad (5)$$

3 進計算法の分岐式にあるように，$S=3$ の場合も同様に，$G(3T,A)$ の計算の $G(T,A^3)$ の計算への還元を，$G(3T+1,A)$ の計算の $G(T,A^3)$ の計算への還元に必要な行列乗算回数と同じ行列乗算回数で行うことができる．

一方，$S > 3$ の場合には，$G(ST,A)$ の計算を $G(T,A^S)$ に還元するために必要な行列乗算と同じ回数で，$G(ST+1)$ の計算を $G(T,A^S)$ に還元する計算法はこれまでに考慮されていなかった．次式を用いることで，そのような計算法を得ることができる．

$$G(N,A) = I + (G(S,A) + A^S - I) * G(T,A^S)$$

実際，$G(ST,A)$ の計算を $G(T,A^S)$ の計算に還元する場合には，$G(S,A)$ の計算に必要な行列乗算と，$G(S,A)$ を用いて $A^S$ を計算するための一回の行列乗算，および，$G(S,A)$ と $G(T,A^S)$ の間の一回の行列乗算が必要となる．一方，$G(ST+1)$ の計算を $G(T,A^S)$ に還元する場合には，$G(S,A)$ を計算に必要な行列乗算と，項 $(G(S,A)+A^S-I)$ に含む $A^S$ を $G(S,A)$ から計算するための一回の行列乗算，および，項の間の一回の行列乗算が必要となる．$G(T,A^S)$ の計算には，項 $(G(S,A)+A^S-I)$ において計算した $A^S$ を再び用いる．

### 3.3 因数分解に基づく新しい計算法

項 3.1，項 3.2 で示した，$A^p$ の $G(p,A)$ からの計算法，および，剰余が 1 の場合に対応する計算法を，因数分解に基づく計算法に組み込むことで，$G(N,A)$ を計算するための新しい計算法を提案する．また，これまでの評価で，$N$ =16，34 については，$G(N,A)$ を因数分解による計算法に基づき，次式のように計算するよりも，DB 法により計算するほうが，1 回少ない行列乗算で計算できることが分かっている．

$$\begin{aligned} G(16,A) =& G(2,A) * G(2,A^2) \\ & * G(2,A^4) * G(2,A^8) \\ G(34,A) =& G(2,A) * G(2,A^2) \\ & * G(2,A^4) * G(2,A^8) \end{aligned}$$

したがって，因数の候補として，素因数だけでなく，16，34 も含める．以降，本項で提案する新しい計算法を，Decomp 法と呼ぶ．

Decomp 法では，31 以下の素数全体の集合 $\Pi = \{2,3,5,\cdots,29,31\}$ に，$\{16,34\}$ を加えた集合 $S = \{2,3,5,7,11,13,16,17,19,23,29,31,34\}$ を因数の候補として因数分解を行う．ただし，34，16，$p \in \Pi$ の順に因数分解を試みる．

$N$ が与えられたとき，$S$ に含まれる因数による $N$ の因数分解 $N = s_1 s_2 s_3 \cdots s_m t$ $(s_i \in S, s_i \leq s_{i+1}, s_i \nmid t)$ に従い，$G(N,A)$ について次式のよう

に因数分解を行う．

$$G(N,A) = G(s_1,A) * G(s_2,A^{s_1}) * \cdots * G(s_m,A^{s_1 s_2 \cdots s_{m-1}}) \quad (6)$$

この $G$ の積を，左の $G$ から順に計算していくことで，$G(N,A)$ を計算する．$s_i \in S$ となる因数 $s_i$ については，$G(s_i,B)$（$B$ は $A$ のべき乗）を DB 法により計算する．$t \notin S$ となる因数 $t$ については，$G(t,B)$ を，次式に従い計算する．

$$G(t,B) = I + B * G(t-1,B) \quad (7)$$

ただし，$G(t-1,B)$ は，Decomp 法により計算を行う．また，$S$ による因数分解において，$t-1$ が二つ以上の因数に分解されるとき，すなわち $t-1 = r \times u$，$r \in S$ と因数分解されるとき，項 3.2 で提案した桁が 1 の場合と対応する計算法を用いることで，式 (8) として計算を行うことができる．

$$G(t,B) = I + (G(r,B) + B^r - I) * G(u,B^r) \quad (8)$$

一般に，$N$ の因数分解として $N = s_1 s_2 s_3 \cdots s_m t$ $(s_i \in S, s_i \leq s_{i+1}, s_i \nmid t)$ が得られたとき，Decomp 法で $G(N,A)$ を計算したときに必要な行列乗算回数 $MMC_{Decomp}(N)$ は，次式で与えられる．

$$MMC_{Decomp}(N) = \sum_{s \in S} MMC_{DB}(s) + MMC_{Decomp}(t-1) + \epsilon_{t-1} + 2(m-1)$$

ここで，$\epsilon_{t-1}$ は，次式で与えられる．

$$\epsilon_{t-1} = \begin{cases} 0 & \text{if } t-1 = ru (r,u \in S) \\ 1 & \text{if } otherwise \end{cases}$$

### 3.4 混合基数表現に基づく新しい計算法

まず，基数を追加することによって行列乗算回数が削減されるかどうかを見積もるため，基数 $r$ とその桁の値 $x$ に対して，次式として $cost(r,x)$ を定義する．

$$cost(r,x) = \frac{MM(r,x)}{\log_2 r}$$

表 2: 7 までの素数についての cost

| $r$ | $x$ | $cost(r,x)$ |
|---|---|---|
| 2 | 0 | 2 |
| 2 | 1 | 2 |
| 3 | 0 | 1.892789 |
| 3 | 1 | 1.892789 |
| 3 | 2 | 2.523719 |
| 5 | 0 | 1.722706 |
| 5 | 1 | 1.722706 |
| 5 | 2 | 2.153382 |
| 7 | 0 | 1.781036 |
| 7 | 1 | 1.781036 |
| 7 | 2 | 2.137243 |

ここで，$MM(r,x)$ は，$N = r * s + r$ の場合に，$G(N,A)$ の計算を $G(s,A^r)$ の計算に還元するために必要な行列乗算回数である．たとえば，$MM(3,1)$ は，$G(N,A) = I + (A + A^2 + A^3) * G(\lfloor \frac{N-1}{3} \rfloor, A^3)$ という展開において，$G(N,A)$ の計算を，$G(\lfloor \frac{N-1}{3} \rfloor, A^3)$ の計算に還元するために必要な行列乗算回数，すなわち 3 となる．$cost(r,x)$ は，二進展開したときの桁あたりの行列乗算回数という意味を持つ．

7 までの素数について，$cost$ をまとめたものを表 2 に示す．

$cost(r,x)$ が 2 以下であるとき，基数 $r$ とその桁の値 $x$ に対応する計算法を分岐式に含めることにより，平均の行列乗算回数を削減できることが期待される．したがって，表 2 において，cost が 2 以下をとる場合をすべて混合基数に含めた計算法を，式 (9) として提案する．以降，この計算法を，$QB_{2+3+7+5+}$ 法とよぶ．「+」は，桁として 1 をとることを意味している．$cost(5,0)$，$cost(5,1)$ は $cost(7,0)$，$cost(7,1)$ より小さいため，この計算法では，基数として 7 よりも 5 を優先させる．基数として 5，および 7 をとる場合，$A^5$，および $A^7$ は，節 3.1 で提案した計算法を用いて，$G(5,A)$，もしくは $G(7,A)$ から 1 回の行列乗算で計算する．

$$G(N,A)=\begin{cases}(I+(I+A)*(A+A^2))*G(T,A^5) & \text{if } N=5T\\ ((I+(I+A)*(A+A^2))+A^5-I)*G(T,A^5) & \text{else if } N=5T+1\\ (I+(A+A^2)*(I+A^2+A^4))*G(T,A^7) & \text{else if } N=7T\\ ((I+(A+A^2)*(I+A^2+A^4))+A^7-I)*G(T,A^7) & \text{else if } N=7T+1\\ (I+A+A^2)*G(T,A^3) & \text{else if } N=3T\\ I+(A+A^2+A^3)*G(T,A^3) & \text{else if } N=3T+1\\ (I+A)*G(T,A^2) & \text{else if } N=2T\\ I+(A+A^2)*G(T,A^2) & \text{else if } N=2T+1\end{cases} \tag{9}$$

この計算法により，$N=[1x_{n-2}^{[r_{n-2}]}\cdots x_2^{[r_2]}x_1^{[r_1]}], r_i \in \{2,3,5,7\}$ と表現されたとき，$G(N,A)$ の計算に必要な行列乗算回数 $MMC_{QB_{2+3+7+5+}}(N)$ は，次式で表される．

$$MMC_{QB_{2+3+7+5+}}(N)=\sum_{i=0}^{n-2}a_i+\sum_{i=0}^{n-3}b_i,$$

ここで，

$$a_i=\begin{cases}3+x_i & \text{if } r_i=7\\ 2+x_i & \text{if } r_i=5\\ 1+x_i & \text{if } r_i=3\\ 0+x_i & \text{if } r_i=2\end{cases}$$

$$b_i=2-x_i$$

となる．

## 4 平均行列乗算回数の評価

計算過程における剰余の移り変わりをマルコフ連鎖とみなすことで，$k\log_2 N$ の形で平均乗算回数を算出した．例として，DB 法の場合について考える．$p_j^{(i)}, i\in\{0,1,2,3,4,5\}$ を DB 法の分岐式に従った再帰の $j$ 番目のステップで，商が $6k+i$ の形で表される値をとる確率とする．このとき，商と余りに着目することにより，式 (10)〜(15) のような漸化式が得られる．

$$p_j^{(0)}=\tfrac{1}{3}p_{j-1}^{(0)}+\tfrac{1}{3}p_{j-1}^{(1)} \tag{10}$$
$$p_j^{(1)}=\tfrac{1}{2}p_{j-1}^{(2)}+\tfrac{1}{3}p_{j-1}^{(3)}+\tfrac{1}{3}p_{j-1}^{(4)} \tag{11}$$
$$p_j^{(2)}=\tfrac{1}{3}p_{j-1}^{(0)}+\tfrac{1}{3}p_{j-1}^{(1)}+\tfrac{1}{2}p_{j-1}^{(5)} \tag{12}$$
$$p_j^{(3)}=\tfrac{1}{3}p_{j-1}^{(3)}+\tfrac{1}{3}p_{j-1}^{(4)} \tag{13}$$
$$p_j^{(4)}=\tfrac{1}{3}p_{j-1}^{(0)}+\tfrac{1}{3}p_{j-1}^{(1)}+\tfrac{1}{2}p_{j-1}^{(2)} \tag{14}$$
$$p_j^{(5)}=\tfrac{1}{3}p_{j-1}^{(3)}+\tfrac{1}{3}p_{j-1}^{(4)}+\tfrac{1}{2}p_{j-1}^{(5)} \tag{15}$$

$p_0^{(0)}=p_0^{(1)}=p_0^{(2)}=p_0^{(3)}=p_0^{(4)}=p_0^{(5)}=\frac{1}{6}$ とおくと，定常分布は，

$$p_\infty^{(0)}=p_\infty^{(3)}=0.1$$
$$p_\infty^{(1)}=p_\infty^{(2)}=p_\infty^{(4)}=p_\infty^{(5)}=0.2$$

と算出される．基数に 3 をとる確率 $p_T=p_0^{(0)}+p_0^{(1)}+p_0^{(3)}+p_0^{(4)}=0.6$，基数に 2 をとる確率 $p_B=p_0^{(2)}+p_0^{(5)}=0.4$ を用いると，平均の底 $b$ は，$b=3^{p_T}2^{p_B}$，ステップごとの平均の乗算回数 $m=p_T*3+p_B*2$ と表される．したがって，平均乗算回数は $m\log_b N=1.92\log_2 N$ となる．

同様の方法により，$QB_{2+3+7+5+}$ 法，$QB_{2+3+5+7+}$ 法，$QB_{2+3+75}$ 法，$QB_{2+3+7}$ 法，および $QB_{2+3+5}$ 法について平均乗算回数をもとめた結果を，DB 法の結果と共に表 3 に示す．

## 5 各計算法の行列乗算回数の比較

各 $N$ について，$G(N,A)$ の計算に必要となる行列乗算回数の比較を行った．$3\le 1000$ までの $N$ に

ついての比較結果を表4に，$3 \leq 1000000$ までの $N$ についての比較結果を表5に示す．比較対象として，$QB_{2+3+7+5+}$ 法と比べ，基数7と基数5の優先度を逆にした $QB_{2+3+5+7+}$ 法，基数5,7について桁の値として1をとらない計算法 $QB_{2+3+75}$ 法，基数7をとらず，基数5については桁の値として1をとらない計算法 $TB_{2+3+5}$ 法，および，基数5をとらず，基数7については桁の値として1をとらない計算法 $TB_{2+3+7}$ 法も用いた．

「A VS B」の列は，A の乗算回数を基準に計算している．たとえば，「DB VS Decomp」の列の「−4」の行は，$G(N,A)$ の計算を行う際に，Decomp 法による計算で必要な行列乗算回数が，DB 法による計算で必要な行列乗算回数と比較して4回少ない $N$ の個数を表している．Decomp 法は，$QB_{2+3+7+5+}$ 法より大きくなり，1000までの $N$ については $QB_{2+3+57}$ 法より大きくなる一方，1000000までの $N$ については $QB_{2+3+57}$ に勝る．DB 法，$QB_{2+3+57}$ 法，$QB_{2+3+5+7+}$ 法と $QB_{2+3+7+5+}$ との比較では，表3で示した平均の行列乗算回数の大小関係と一致する結果が得られた．

## 6 まとめ

本研究では，行列多項式 $G(N,A) = I + A + A^2 + \cdots + A^{N-1}$ の評価を行う計算法を提案した．まず，$G(N,A)$ から $A^p$ を1回の行列乗算で計算する手法，および，桁1の基数展開に対応する計算法として，桁0の場合と同じ行列乗算回数で計算する手法を提案した．そして，因数分解に基づく手法，および，混合基数展開に基づく手法にそれらを組み込み，$G(N,A)$ の新しい計算法を提案した．マルコフ連鎖に基づく考え方を用いて平均乗算回数を算出し，この値がこれまでに提案されている手法よりも小さくなることを確かめた．1000までの $N$，1000000までの $N$ について実験を行い，各 $N$ について $G(N,A)$ を計算するために必要な行列乗算回数の比較を行った．

## 参考文献


[1] D. Westreich, "Evaluating the matrix polynomial $I + A + ... + A^{N-1}$," IEEE Trans. Circuits Syst., vol. 36, pp. 162-164, Jan. 1989.

[2] L. Lei and T. Nakamura, "A fast algorithm for evaluating the matrix polynomial $I + A + ... + AN - 1$," IEEE Trans. Circuits Syst., vol. 39, pp. 299-300, Apr. 1992.

[3] S. C. Dutta Roy and S. Minocha, "On the evaluation of the matrix polynomial $I + A + ... + A^{N-1}$," IEEE Trans. Circuits Syst., vol. 39, pp. 567-570, July 1992.

[4] V. S. Dimitrov and B. D. Donevsky, "A limited dispoof to the conjecture of the evaluation of the matrix polynomial $I + A + ... + A^{N-1}$," IEEE Trans. Circuits Syst., vol. 41, pp. 247-248, Mar. 1994.

[5] V. S. Dimitrov and T. V. Cooklev. "Hybrid algorithm for the computation of the matrix polynomial $I + A + \cdots + A^{N-1}$," IEEE Trans. Circuits Syst. , vol. 42, pp. 377-380, July 1995.

[6] Ç, . K. Koç, and B. Bakkaloğlu "A parallel algorithm for functions of triangular matrices," Computing, vol. 57, no. 1, pp. 85-92, Mar. 1996.

[7] W. H. Press, "Discrete Radon transform has an exact, fast inverse and generalizes to operations other than sums along lines," PNAS, vol. 103, no. 51, pp. 19 249-19 254, Dec. 2006.

表 3: $k\log_2 N$ として平均行列乗算回数を算出したときの $k$ の値

| | $QB_{2+3+7+5+}$ 法 | $QB_{2+3+5+7+}$ 法 | $QB_{2+3+75}$ 法 | $TB_{2+3+7}$ 法 | $TB_{2+3+5}$ 法 | DB 法 |
|---|---|---|---|---|---|---|
| ステップごとの行列乗算回数 | 3.487 | 3.529 | 3.061 | 2.855 | 2.850 | 2.6 |
| 平均の底 | 3.811 | 3.861 | 3.136 | 2.839 | 2.869 | 2.551 |
| $k$ | 1.806 | 1.811 | 1.858 | 1.896 | 1.875 | 1.925 |

表 4: 1000 までの $N$ についての行列乗算回数の比較

| | DB VS Decomp | $QB_{2+3+57}$ VS Decomp | $QB_{2+3+7+5+}$ VS Decomp | DB VS $QB_{2+3+7+5+}$ | $QB_{2+3+57}$ VS $QB_{2+3+7+5+}$ | $QB_{2+3+5+7+}$ VS $QB_{2+3+7+5+}$ |
|---|---|---|---|---|---|---|
| -2 | 5 | | | 17 | 2 | |
| -1 | 316 | 72 | 28 | 534 | 246 | 23 |
| 0 | 659 | 844 | 687 | 450 | 753 | 976 |
| 1 | 21 | 85 | 281 | | | 2 |
| 2 | | | 5 | | | |

表 5: 1000000 までの $N$ についての行列乗算回数の比較

| | DB VS Decomp | $QB_{2+3+57}$ VS Decomp | $QB_{2+3+7+5+}$ VS Decomp | DB VS $QB_{2+3+7+5+}$ | $QB_{2+3+57}$ VS $QB_{2+3+7+5+}$ | $QB_{2+3+5+7+}$ VS $QB_{2+3+7+5+}$ |
|---|---|---|---|---|---|---|
| -4 | 57 | 1 | | 1339 | 8 | |
| -3 | 15034 | 342 | 37 | 122782 | 5447 | 72 |
| -2 | 234415 | 21648 | 3502 | 523981 | 130307 | 3591 |
| -1 | 528077 | 237375 | 59583 | 313690 | 494131 | 74223 |
| 0 | 213340 | 532573 | 329506 | 37818 | 362079 | 900684 |
| 1 | 9078 | 195754 | 455177 | 391 | 7962 | 20846 |
| 2 | | 12197 | 143306 | | 66 | 581 |
| 3 | | 111 | 8847 | | | 3 |
| 4 | | | 43 | | | |