複数の右辺ベクトルを有する有限素体上の対称線形方程式に対する擬逆行列を用いた反復解法

鈴木 優治　　指導教員：曽我部 知広

1　はじめに

本研究では，複数の右辺ベクトルを持つ有限素体上の線形方程式

$$AX = B \tag{1}$$

の解 X を求めることを考える．ここで，A は有限素体 $\mathbb{F}_p$ の元を要素に持つ n 次の対称行列である．そして，X，B は $X = [\boldsymbol{x}_1, \ldots, \boldsymbol{x}_s]$，$B = [\boldsymbol{b}_1, \ldots, \boldsymbol{b}_s]$ で，$\boldsymbol{x}_1, \ldots, \boldsymbol{x}_s, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_s$ は有限素体 $\mathbb{F}_p$ の元を要素に持つ n 次の列ベクトルである．

方程式 (1) の効率の良い解法としては Montgomery の Block Lanczos 法 [3] が知られており，RSA 暗号の解読にも用いられている．

2　体・有限体

四則演算が可能な集合を体と呼ぶ．例として，有理数体 $\mathbb{Q}$，実数体 $\mathbb{R}$，複素数体 $\mathbb{C}$ が挙げられる．そして，元の数が有限な体を有限体と呼び，元の数が q の有限体を $\mathbb{F}_q$ と表す．元の数が素数 p 個のとき，$\mathbb{F}_p$ は有限素体と呼ばれる．

3　研究目的

本研究の目的は，方程式 (1) の解 X を求めるための新しい解法を開発することである．近年，坂野 [1] により，有限素体上の線形方程式 $A\boldsymbol{x} = \boldsymbol{b}$ に対して共役勾配法が適用可能であることが示された．そこで本研究では，実数体上のブロック共役勾配法（以下 Block CG 法と略す）[2] に着目し，この解法のアルゴリズムを参考にして新しい解法を構築することを考える．Block CG 法のアルゴリズムを以下に示す．

Algorithm 1（実数体上の Block CG 法）

1: 初期値 $X_0 = O$，$R_0 = B - AX_0$，$P_0 = R_0$，
2: **for** $i = 0, 1, \ldots,$ until $\dfrac{\| R_{i+1} \|_{\mathrm{F}}}{\| B \|_{\mathrm{F}}} < \epsilon$ **do**
3: $\quad \alpha_i = \left(P_i^{\mathrm{T}} A P_i\right)^{-1} R_i^{\mathrm{T}} R_i$,
4: $\quad X_{i+1} = X_i + P_i \alpha_i$,
5: $\quad R_{i+1} = R_i - A P_i \alpha_i$,
6: $\quad \beta_i = \left(R_i^{\mathrm{T}} R_i\right)^{-1} R_{i+1}^{\mathrm{T}} R_{i+1}$,
7: $\quad P_{i+1} = R_{i+1} + P_i \beta_i$.
8: **end for**

4　本研究

4.1　有限体特有の問題点

有限体特有の性質を次に示す．

有限体特有の性質

1. 有限体上では実数体上の正定値行列[1] のような性質が成り立たない．
2. 有限体上の n 次ベクトル空間 $\mathbb{F}_q^n$ の部分空間を $\mathcal{V}$ とする．$\mathcal{V}$ の全てのベクトルと直交する[2] $\mathbb{F}_q^n$ の部分空間を $\mathcal{V}$ の双対空間と呼び，$\mathcal{V}^{\perp}$ と表す．このとき，$\mathcal{V} \cap \mathcal{V}^{\perp} = \{\boldsymbol{0}\}$ とは限らない．

この 2 つの性質により $\left(P_i^{\mathrm{T}} A P_i\right)^{-1}$，$\left(R_i^{\mathrm{T}} R_i\right)^{-1}$ を求められない場合がある．そして，$\left(P_i^{\mathrm{T}} A P_i\right)^{-1}$，$\left(R_i^{\mathrm{T}} R_i\right)^{-1}$ は Algorithm 1 で重要となるパラーメータ α_i, β_i に関係し，求められない場合，次に示す問題を引き起こす．

- α_i, β_i を求められない $\Rightarrow$ 計算破綻
- $\alpha_i = O, \beta_i = O \Rightarrow X_{i+1}$，$R_{i+1}$，$P_{i+1}$ が更新されない（無限に反復を繰り返す）

これらの問題を，射影行列 S_i を用いた擬逆行列によって回避することを試みる．

4.2　射影行列 S_i

S_i は次に示すような行列である．

1. $S_i \in \mathbb{F}_p^{s \times s'}$ は，$S_i^{\mathrm{T}} \left(P_i^{\mathrm{T}} A P_i\right) S_i$ が逆行列を持つように $P_i^{\mathrm{T}} A P_i$ の部分行列を取り出す行列である．
2. S_i は，列と行に関して次の制約を持つ．
   - 列：　任意の列に対して，1 つの成分が “1”で，その他の成分は “0”である．
   - 行：　任意の行に対して，最大で 1 つの成分が “1”で，その他の成分 “0”である．

以下に例を示す．

$$P_i^{\mathrm{T}} A P_i = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix},\ S_i = \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

のとき，$S_i^{\mathrm{T}} \left(P_i^{\mathrm{T}} A P_i\right) S_i = \begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix}$.

---

[1] 対称行列 A が正定値であるとは，$\forall \boldsymbol{x} \neq \boldsymbol{0}$ に対して $\boldsymbol{x}^{\mathrm{T}} A \boldsymbol{x} > 0$ を満たすことを言う．

[2] $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)^{\mathrm{T}}, \boldsymbol{b} = (b_1, b_2, \ldots, b_n)^{\mathrm{T}} \in \mathbb{F}_q^n$ に対して，$\boldsymbol{a}^{\mathrm{T}} \boldsymbol{b} = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n = 0$ となるとき，$\boldsymbol{a}$ と $\boldsymbol{b}$ は直交すると言う．

4.3 擬逆行列

擬逆行列の定義を次に示す．

擬逆行列

$M \in \mathbb{F}_p^{m\times n}$ に対して，

$$M = MM^{\dagger}M \tag{2}$$

を満たす $M^{\dagger} \in \mathbb{F}_p^{n\times m}$ を，M の擬逆行列と呼ぶ．

射影行列 S_i は $S_i^{\mathrm{T}}S_i = I_{s'}$，$S_iS_i^{\mathrm{T}}S_i = S_i$ を満たすことから，前節の例を用いて，$M = S_i\left(S_i^{\mathrm{T}}P_i^{\mathrm{T}}AP_iS_i\right)S_i^{\mathrm{T}}$，$M^{\dagger} = S_i\left(S_i^{\mathrm{T}}P_i^{\mathrm{T}}AP_iS_i\right)^{-1}S_i^{\mathrm{T}}$ とすると M，$M^{\dagger}$ は式 (2) を満たす．よって $M^{\dagger}$ は M の擬逆行列となる．これを用いて有限素体上の解法を構築した．構築した解法を以下に示す．

Algorithm 2 （提案手法）

初期値 $X_0 = O$，$R_0 = B - AX_0$，$P_0 = R_0$，
for $i = 0, 1, \ldots,$ until $R_{i+1} = O$ **do**
  $P_i^{\mathrm{T}}AP_i$ のランクに合わせて S_i を作成する，
  $\alpha_i = S_i\left(S_i^{\mathrm{T}}P_i^{\mathrm{T}}AP_iS_i\right)^{-1}S_i^{\mathrm{T}}R_i^{\mathrm{T}}R_i$，
  $X_{i+1} = X_i + P_i\alpha_i$，
  $R_{i+1} = R_i - AP_i\alpha_i$，
  $\beta_i = S_i\left(S_i^{\mathrm{T}}R_i^{\mathrm{T}}R_iS_i\right)^{-1}S_i^{\mathrm{T}}R_{i+1}^{\mathrm{T}}R_{i+1}$，
  $P_{i+1} = R_{i+1} + P_i\beta_i$．
end for

4.4 演算量の比較

提案手法と Montgomery の Block Lanczos 法の 1 反復あたりの演算量の比較を行った．演算量は行列サイズ n と右辺ベクトルの数 s に依存するため，n，s の大きさにより演算量の主要部は変化する．そのため，n が s よりも十分大きい場合（$n \gg s$），n と s が同程度の場合（$n \approx s$），n が s よりも十分小さい場合（$n \ll s$）の 3 通りについて比較を行った．結果を表 1 に示す．

3 通りのどの場合においても，2 つの解法の演算量のオーダーは等しいことが分かった．従って，提案手法の演算量は Montgomery の Block Lanczos 法の演算量と同程度であると言える．

4.5 提案手法の性質

Algorithm 1 の性質から，提案手法の R_i と P_i の直交性に関する性質を類推し，その性質を満たすかどうかを数値実験から調べた．

推測した性質

$$S_i^{\mathrm{T}}R_i^{\mathrm{T}}R_iS_i = O \ (i \neq j) \tag{3}$$
$$S_i^{\mathrm{T}}P_i^{\mathrm{T}}AP_iS_i = O \ (i \neq j) \tag{4}$$

3 つの線形方程式 $A_1X = B_1$，$A_2X = B_2$，$A_3X = B_3$ に対して，初期値 $X_0 = O$ として Algorithm 2 を用いて解 X を求めた．$A_1X = B_1$ は 6 反復目，$A_2X = B_2$ は 7 反復目，$A_3X = B_3$ は 8 反復目で正しい解 X が得られた．このとき，$A_1X = B_1$，$A_2X = B_2$ は式 (3)，(4) を満たした．しかし，$A_3X = B_3$ は式 (3)，(4) を一部満たさなかった．

5 まとめと今後の課題

本研究では，方程式 (1) の解 X を求めるための解法として，Algorithm 1 に着目し，射影行列 S_i による擬逆行列を用いて新しい解法を構築した．そして，提案手法と Montgomery の Block Lanczos 法の演算量の比較を行い，提案手法の演算量は Montgomery の Block Lanczos 法の演算量と同程度であることが分かった．また，Algorithm 1 の性質から提案手法の性質を類推し，その性質について調べた．直交性を満たさない場合でも正しい解が得られる場合が存在することが分かり，今後の課題として，その原因を調べることが挙げられる．加えて，直交性を完全に満たすような新しい解法を開発することも課題として挙げられる．

参考文献

[1] 坂野正英，有限素体上における対称線形方程式の反復法に関する研究，愛知県立大学情報科学部平成 22 年度卒業論文，2011.

[2] Dianne P. O'Leary, The block conjugate gradient algorithm and related methods, Linear Algebra and its Applications, Vol. 29, pp. 293-322, 1980.

[3] Peter L. Montgomery, A block Lanczos algorithm for finding dependencies over GF(2), Proc. Eurocrypt, 1995.

表 1　Montgomery の Block Lanczos 法と提案手法の演算量の比較．

	$n \gg s$	$n \approx s$	$n \ll s$
Montgomery の Block Lanczos 法	$2n^2s$	$29s^3 + 2n^2s + 10ns^2$	$29s^3$
提案手法	$2n^2s$	$18s^3 + 2n^2s + 18ns^2$	$18s^3$