Lyapunov方程的线性变换解法

贾利新*
(中国人民解放军信息工程大学电子技术学院 郑州 450004)

【摘要】利用线性变换以及方阵的Jordan标准型的方法，给出了Lyapunov矩阵方程存在唯一解的充分必要条件以及解的形式，采用初等的方法，得出的结果比已有结论丰富。该方法也可用来研究一般域上的矩阵方程，从而为研究密码学基础理论提供一种新方法。

关 键 词 矩阵； Lyapunov方程； Jordan标准型； 线性变换
中图分类号 O151.21

1 概 述

本文的结论中，假设$\chi(A)$表示由方阵A的所有特征值组成的集合，$M_{m,n}(K)$ ($M_m(K)$)表示复数域上$m\times n$阵(m 阶方阵)的全体。

设$A\in M_m(K)$,$B\in M_n(K)$,$C\in M_{m,n}(K)$,以$X\in M_{m,n}(K)$为未知矩阵的方程$AX-XB=C$称为Lyapunov方程。对于这类方程，目前的解法大多利用矩阵的张量积[1~3]。本文利用较为初等的方法，即线性变换的方法，给出这类方程有唯一解的充要条件以及唯一解的形式，所得结果比文献[1~3]丰富。

讨论中引用以下引理。

引理 1 设σ是数域F上有限维向量空间V上的线性变换，如果σ是单射，则σ必为满单射，即σ是可逆的。

这个引理的证明较简单，这里就不列出。

引理 2 设$A\in M_m(K)$，$B\in M_n(K)$，B的特征多项式为$f(x)$,且有$\lambda\neq u$, $\forall\lambda\in\chi(A)$，$\forall u\in\chi(B)$，则$f(A)$非奇异。

证明 设A的所有特征值为$\lambda_1,\lambda_2,\cdots,\lambda_m$，$B$的所有特征值为$\mu_1,\mu_2,\cdots,\mu_n$，因此$f(x)=\prod_{j=1}^{n}(x-\mu_j)$。注意到$f(A)$的特征值为$f(\lambda_i)=\prod_{j=1}^{n}(\lambda_i-\mu_j)$,$\forall\lambda_i\in\chi(A)$,故$f(A)$的每一个特征值都非零,从而$f(A)$非奇异。

2 主要结论

定理 1 设$A\in M_m(K)$，$B\in M_n(K)$，则Lyapunov方程$AX-XB=C$有唯一解的充分必要条件是

$$\lambda\neq u \qquad \forall\lambda\in\chi(A) \qquad \forall u\in\chi(B)$$

证明 充分性 在$M_{m,n}(K)$中定义如下变换σ

$$\sigma(X)=AX-XB$$
$$X\in M_{m,n}(K)$$

容易验证，对于任意X, $Y\in M_{m,n}(K)$及任意复数k有

$$\sigma(X+Y)=\sigma(X)+\sigma(Y)$$
$$\sigma(kX)=k\sigma(X)$$

2000年12月5日收稿
* 男 27岁 博士生

因此，σ 是 $M_{m,n}(K)$ 上的线性变换。

设 $\sigma(X)=AX-XB=0$，即 $AX=XB$。对于任意自然数 n，利用归纳法可得

$$A^n X = XB^n$$

对任意复多项式 $g(x)$ 进一步可推得

$$g(A)X = Xg(B)$$

特别地，对于 B 的特征多项式 $f(x)$ 应用上式并由Cayley-Hamilton 定理有

$$f(A)X = Xf(B) = 0$$

由已知 $\lambda \neq u, \forall \lambda \in \chi(A), \forall u \in \chi(B)$ 及引理2可知矩阵 $f(A)$ 非奇异，故 $X=0$，因此 σ 是单射。注意到 $\dim M_{m,n}(K)=nm$，由引理1可知 σ 可逆，即对任意 $C \in M_{m,n}(K)$，矩阵方程 $AX-XB=C$ 有唯一解。

必要性 利用反证法，假设存在 $\lambda_0 \in \chi(A)$ 和 $u_0 \in \chi(B)$ 满足 $\lambda_0=\sigma_0$，设 $A=P^{-1}J_A P$，$B=Q^{-1}J_B Q$,其中 J_A, J_B 分别为 A 和 B 的Jordan标准型，并且 J_A 的最后一个Jordan 块为

$$\begin{bmatrix} \lambda_0 & & & \\ 1 & \lambda_0 & & \\ & \ddots & \ddots & \\ & & 1 & \lambda_0 \end{bmatrix}$$

J_B 的最后一个Jordan块为

$$\begin{bmatrix} u_0 & & & \\ 1 & u_0 & & \\ & \ddots & \ddots & \\ & & 1 & u_0 \end{bmatrix}$$

令

$$X = P^{-1}\begin{bmatrix} 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix}Q$$

容易验证，$AX=XB$。即与Lyapunov方程 $AX-XB=C$ 相关的齐次方程 $AX=XB$ 有非零解，故矩阵方程 $AX-XB=C$ 的解不唯一，与已知矛盾。

定理 2 设矩阵B的特征多项式为

$$f(x)=a_0+a_1x+\cdots\cdots+a_nx^n \qquad a_n=1$$

则在定理1的条件下，Lyapunov方程 $AX-XB=C$ 的唯一解为

$$X = f(A)^{-1}\sum_{i=1}^{n}\sum_{j=0}^{i-1} a_i A^{i-1-j} C B^j$$

证明 利用数学归纳法，可以建立以下 $n+1$ 个等式

$$
\begin{aligned}
&X = X \\
&AX = XB + C \\
&A^2X = XB^2 + CB + AC \\
&\cdots\ \cdots\ \cdots\ \cdots \\
&A^nX = XB^n + \sum_{j=0}^{n-1} A^{n-1-j}CB^j
\end{aligned}
$$

将第一式两端同乘以a_0，第二式两端乘以a_1，第 $n+1$式两端同时乘以a_n，然后相加，同时注意到$f(\boldsymbol{B})=0$，可得

$$f(\boldsymbol{A})X = \sum_{i=1}^{n}\sum_{j=0}^{i-1} a_i A^{i-1-j}CB^j$$

由于在定理1的条件下，即$\lambda \neq u, \forall\lambda \in \chi(\boldsymbol{A}), \forall u \in \chi(\boldsymbol{B})$，$f(\boldsymbol{A})$可逆，故

$$X = f(\boldsymbol{A})^{-1}\sum_{i=1}^{n}\sum_{j=0}^{i-1} a_i A^{i-1-j}CB^j$$

参 考 文 献

1 Lancaster P，Timenetsky M. The theory of matrices, with aplications. Academic Press, NewYork: 1985

2 贾利新 .用矩阵的谱分解研究线性矩阵方程. 工科数学, 1997, 13(4):124~127

3 陈公宁. 矩阵理论与应用. 北京：高等教育出版社，1991

4 Zhu Wen, He Mingxing. A Fixed Point Theorem for Random Condensing Operators. Journal of University of Electronic Science and Technology of China, 2000, 29(3): 303~305[朱 雯, 何明星. 凝聚随机算子的一个不动点定理.电子科技大学学报, 2000, 29(3): 303~305]

5 Chen Huafu. A Pertubed Gradient Projektion Method for General Constrained Optimization Problems. Journal of University of Electronic Science and Technology of China, 1997, 26(4): 445~448[陈华富. 一般约束优化问题的摄动梯度投影法. 电子科技大学学报, 1997, 26(4): 445~448]

Linear Transformation Approach for Lyapunov Equation

Jia Lixin

(Institute of Electronic and Technology, University of Information Engneering of PLA Zhengzhou 450004)

Abstract By using linear transformation method, this paper gives the necessary and sufficient conditions for Lyapunov equation. The unique solutions are obtained. The method in this paper is elementary and the results are richer than those in references. The method can also be used to deal with matrix equations on general field, which supplies a new method to cryptography.

Key words matrix; lyapunov equation; jordan form; linear transformation