MA TRẬN NGUYÊN TỐ - ĐIỂM GIỐNG VÀ KHÁC VỚI SỐ NGUYÊN TỐ

Nguyễn Thị Khánh Hoà[(1)]
(1) Trường Đại học Thủ Dầu Một
Ngày nhận bài 20/4/2024; Chấp nhận đăng 26/7/2024
Liên hệ email: hoantk@tdmu.edu.vn

Tóm tắt

Dựa trên những kiến thức đã có về số nguyên tố trong tập số tự nhiên và ma trận vuông, bài viết làm rõ khái niệm ma trận nguyên tố (Rivett & Mackinnon, 1986). Bài viết cũng sẽ chứng minh chi tiết trong tập M gồm các ma trận vuông cấp 2 với hệ số nguyên không âm và định thức bằng 1 chỉ có hai ma trận nguyên tố và mọi ma trận trong tập M (ngoại trừ ma trận đơn vị I) đều có thể biểu diễn được duy nhất thành tích của hai ma trận nguyên tố này. Bài viết cũng đề xuất phương pháp phân tích một ma trận (vuông cấp 2 với hệ số nguyên không âm và định thức bằng 1) thành tích các ma trận nguyên tố này và trình bày các ví dụ minh hoạ cụ thể.

Từ khoá: *ma trận cấp 2, ma trận nguyên tố, số nguyên tố*

Abstract

PRIME MATRICES – SIMILARITIES AND DIFFERENCES WITH PRIME NUMBERS

Based on existing knowledge about prime numbers in the set of natural numbers and square matrices, the article clarifies the concept of prime matrices (according to Rivett & Mackinnon, 1986). The article also prove in detail that there are only two prime matrices in the set M of 2×2 matrices with entries in the non-negative integers and with determinant 1 and any member of M (except identity matrix I) can be uniquely factorised into a product of those prime matrices. The article also proposes a method to factorise a matrix (2×2) matrix with entries in the non-negative integers and with determinant 1) into a product of those prime matrices and presents specific illustrative examples.

1. Đặt vấn đề

Trong tập số tự nhiên, số nguyên tố là số tự nhiên lớn hơn 1 không phải là tích của hai số tự nhiên nhỏ hơn chính nó. Chúng ta đều biết rằng có vô số số nguyên tố và có một định lý đóng vai trò cực kỳ quan trọng trong lý thuyết số, đó là Định lý cơ bản của số học: "Mỗi số tự nhiên lớn hơn 1 đều phân tích được thành tích những thừa số nguyên tố và sự phân tích đó là duy nhất nếu không kể đến thứ tự của các thừa số". Định lý này đã cho chúng ta rất nhiều ứng dụng. Chẳng hạn, trong nội tại toán học, ta có thể dùng định lý để tìm ước chung lớn nhất và bội chung nhỏ nhất của các số tự nhiên, đếm số các ước của một số tự nhiên và tính tổng của chúng (Tài, 1999). Còn trong thực tế cuộc sống, định lý này chính là cơ sở toán học của một số thuật toán mật mã khoá công khai như RSA (Rivest và nnk., 1978). Đây là thuật toán đầu tiên được sử dụng để tạo ra chữ ký điện tử. Hiện nay RSA đang được sử dụng phổ biến trong thương mại điện tử và được cho là đảm bảo an toàn với điều kiện độ dài khóa đủ lớn.

Khái niệm "ma trận nguyên tố" đã được Rivett và Mackinnon (1986) định nghĩa tương tự như số nguyên tố. Tuy nhiên chúng ta đều biết rằng các phép toán trong tập số tự nhiên có nhiều điểm khác biệt so với các phép toán trong tập các ma trận. Chẳng hạn phép nhân các số tự nhiên có tính giao hoán nhưng phép nhân các ma trận thì không (Dũng, 2018; Lay và nnk., 2016). Như vậy, hai tính chất quan trọng của số nguyên tố được nêu ở trên (Có vô số số nguyên tố và Định lý cơ bản của số học) liệu rằng có còn đúng đối với ma trận nguyên tố? Đi tìm đáp án cho câu hỏi trên chính là mục đích của bài viết. Qua bài viết, chúng ta sẽ thấy được một số điểm giống nhau và khác nhau giữa hai khái niệm tương tự này.

2. Lịch sử nghiên cứu vấn đề

Khái niệm "ma trận nguyên tố" trong tập hợp các ma trận đã được nhiều nhà toán học trên thế giới định nghĩa. Tuy nhiên chúng được định nghĩa theo những cách khác nhau với mục đích nghiên cứu khác nhau.

Richman và Schneider (1974) đã định nghĩa "ma trận nguyên tố" trong tập các ma trận vuông cấp n với hệ số không âm là ma trận (khác ma trận đơn) không phải là tích của hai ma trận khác ma trận đơn (ma trận đơn là ma trận có duy nhất một phần tử là số dương trên mỗi dòng và mỗi cột). Picci, van den Hof, van Schuppen (1998) cũng đã dùng khái niệm "ma trận nguyên tố" do Richman và Schneider định nghĩa trong bài viết của mình. Trong hai bài viết này, các tác giả đều chỉ tập trung tìm điều kiện cần hoặc đủ để một ma trận là nguyên tố mà không đề cập đến vấn đề là các ma trận khác ma trận đơn có thể phân tích được thành tích của các ma trận nguyên tố hay không. Sở dĩ các tác giả định nghĩa "ma trận nguyên tố" theo nghĩa này và tìm các điều kiện để nhận dạng ma trận nguyên tố vì chúng có nhiều ứng dụng trong lĩnh vực lý thuyết điều khiển.

Khái niệm "ma trận nguyên tố" cũng đã được Rivett và Mackinnon (1986) giới thiệu theo một cách khác vào năm 1986. Trong tập các ma trận vuông với hệ số nguyên không âm, một ma trận (khác ma trận đơn vị) được gọi là nguyên tố nếu nó không phải là tích của hai ma trận khác ma trận đơn vị. Có thể nói khái niệm này được định nghĩa một cách đơn giản, gần gũi và tương đồng nhất với khái niệm số nguyên tố (vì ma trận đơn vị trong tập ma trận vuông có tính chất tương tự như số 1 trong tập số tự nhiên). Các tác giả cũng đã khẳng định chỉ có hai ma trận nguyên tố trong tập các ma trận vuông cấp 2 với hệ số nguyên không âm và định thức bằng 1. Hơn nữa, mọi ma trận đều có thể biểu diễn được duy nhất thành tích của hai ma trận nguyên tố này. Tuy nhiên bài viết chỉ đưa ra hai ma trận nguyên tố mà không chứng minh. Thêm vào đó phần chứng minh nội dung "mọi ma trận đều có thể biểu diễn được duy nhất thành tích của hai ma trận nguyên tố này" được trình bày khá giản lược dưới dạng ý tưởng và thiếu nhiều trường hợp, do đó chưa thể hiện tường minh phương pháp phân tích một ma trận thành tích các ma trận nguyên tố.

Alan Beardon (2009) cũng sử dụng khái niệm "ma trận nguyên tố" do Rivett và Mackinnon định nghĩa. Tuy nhiên trong bài viết của mình tác giả tiếp cận vấn đề dưới một góc nhìn khác để tập trung chính vào mục đích tìm hiểu ma trận nguyên tố cấp n tuỳ ý.

Ở Việt Nam hiện nay chưa có bài viết nào giới thiệu về "ma trận nguyên tố". Với mục đích giới thiệu khái niệm thú vị này tới những độc giả quan tâm đến số nguyên tố và ma trận, tôi chọn hiểu khái niệm "ma trận nguyên tố" do Rivett và Mackinnon định nghĩa. Tôi sẽ làm rõ những phần đã được lược giản trong bài viết của Rivett và Mackinnon. Cụ thể là chứng minh hai ma trận nguyên tố, chứng minh nội dung "mọi ma trận đều có thể biểu diễn được duy nhất thành tích của hai ma trận nguyên tố này" một cách chi tiết hơn cho mọi trường hợp, từ đó đề xuất phương pháp phân tích một ma trận (vuông cấp 2 với hệ số nguyên không âm và định thức bằng 1) thành tích các ma trận nguyên tố.

3. Kết quả nghiên cứu

3.1. Ma trận nguyên tố

3.1.1. Định nghĩa: Rivett & Mackinnon (1986) Cho M là một tập hợp ma trận. Một ma trận (khác ma trận đơn vị) trong tập M được gọi là nguyên tố nếu nó không phải là tích của hai ma trận khác ma trận đơn vị chứa trong M.

Trong bài viết này, ta luôn xét M là tập hợp các ma trận vuông cấp 2 với hệ số nguyên không âm và có định thức bằng 1.

3.1.2. Ví dụ. $P = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ và $Q = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ là hai ma trận nguyên tố trong tập M.

Chứng minh

* Rõ ràng các phần tử của P và Q đều là số nguyên không âm và hai ma trận này đều có định thức bằng 1 nên chúng thuộc M.

* Giả sử $P=\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}=\begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}x & y\\ z & t\end{bmatrix}$

với $a,b,c,d,x,y,z,t\in\mathbb{N}; ad-bc=xt-yz=1.$

Khi đó ta có hệ phương trình $\begin{cases}ax+bz=1\ (1)\\ ay+bt=0\ (2)\\ cx+dz=1\ (3)\\ cy+dt=1\ (4)\end{cases}$

Vì $a,b,c,d,x,y,z,t\in\mathbb{N}$ nên từ (2) ta có thể kết luận chỉ có 4 trường hợp như sau:

$a=b=0$ hoặc $a=t=0$ hoặc $y=b=0$ hoặc $y=t=0.$

Kết hợp với (1) và (4) ta loại trường hợp $a=b=0$ và $y=t=0.$

+ Nếu $a=t=0$ thì từ (1) và (4) ta suy ra $bz=1$ và $cy=1.$

Do $b,c,y,z\in\mathbb{N}$ nên $b=c=y=z=1.$

Khi đó $P=\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}=\begin{bmatrix}0 & 1\\ 1 & d\end{bmatrix}\begin{bmatrix}x & 1\\ 1 & 0\end{bmatrix}.$

Tuy nhiên hai ma trận này đều có định thức bằng -1 nên chúng không thuộc M. Ta loại trường hợp này.

+ Nếu $y=b=0$ thì từ (1) và (4) ta suy ra $ax=1$ và $dt=1.$

Do $a,d,x,t\in\mathbb{N}$ nên $a=d=x=t=1.$

Thay vào (3) ta được $c+z=1.$ Lại vì $c,z\in\mathbb{N}$ nên $c=1,z=0$ hoặc $c=0,z=1.$

Khi đó $P=\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}=\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$ hoặc $P=\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}$

Ta cũng loại trường hợp này vì $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$ là ma trận đơn vị.

Vậy P không là tích của hai ma trận khác ma trận đơn vị chứa trong M. Do đó P là ma trận nguyên tố.

* Giả sử $Q=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}=\begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}x & y\\ z & t\end{bmatrix}$

với $a,b,c,d,x,y,z,t\in\mathbb{N}; ad-bc=xt-yz=1.$

Khi đó ta có hệ phương trình $\begin{cases}ax+bz=1\ (1)\\ ay+bt=1\ (2)\\ cx+dz=0\ (3)\\ cy+dt=1\ (4)\end{cases}$

Vì $a,b,c,d,x,y,z,t\in\mathbb{N}$ nên từ (3) ta có thể kết luận chỉ có 4 trường hợp như sau:

$c=d=0$ hoặc $x=d=0$ hoặc $c=z=0$ hoặc $x=z=0.$

Kết hợp với (1) và (4) ta loại trường hợp $c=d=0$ và $x=z=0.$

+ Nếu $x=d=0$ thì từ (1) và (4) ta suy ra $bz=1$ và $cy=1.$

Do $b,c,y,z\in\mathbb{N}$ nên $b=c=y=z=1.$

Khi đó $Q=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}=\begin{bmatrix}a & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & t\end{bmatrix}.$

Tuy nhiên hai ma trận này đều có định thức bằng -1 nên chúng không thuộc M. Ta loại trường hợp này.

+ Nếu $c=z=0$ thì từ (1) và (4) ta suy ra $ax=1$ và $dt=1.$

Do $a,d,x,t\in\mathbb{N}$ nên $a=d=x=t=1.$

Thay vào (2) ta suy ra $y+b=1$. Lại vì $b,y\in\mathbb{N}$ nên $b=1,y=0$ hoặc $b=0,y=1$.

Như vậy, $Q=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$ hoặc $Q=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$

Ta cũng loại trường hợp này vì $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$ là ma trận đơn vị.

Vậy Q không là tích của hai ma trận khác ma trận đơn vị chứa trong M. Do đó Q là ma trận nguyên tố.

3.1.3. Nhận xét. Với P,Q là các ma trận nguyên tố ở ví dụ trên.

i) Không tồn tại $X\in M$ sao cho $I=PX$ hoặc $I=QX$.

ii) Không tồn tại $X,Y\in M$ sao cho $PX=QY$.

iii) Nếu $A_1A_2\dots A_m=B_1B_2\dots B_n$ (*)

với A_i,B_j là P hoặc Q $(m,n,i,j\in\mathbb{N};i,j\le m\le n)$

thì $m=n$ và $A_i=B_i$, với mọi i.

Chứng minh

i) Giả sử tồn tại $X\in M$ sao cho $I=PX$ hoặc $I=QX$.

Khi đó $X=P^{-1}=\begin{bmatrix}1 & 0\\ -1 & 1\end{bmatrix}$ hoặc $X=Q^{-1}=\begin{bmatrix}1 & -1\\ 0 & 1\end{bmatrix}$.

Nhưng hai ma trận này không thuộc M. Điều này mâu thuẫn với giả thiết.

Vậy ta được điều phải chứng minh.

ii) Giả sử tồn tại các ma trận $X=\begin{bmatrix}a & b\\ c & d\end{bmatrix},Y=\begin{bmatrix}x & y\\ z & t\end{bmatrix}\in M$ sao cho

$$PX=QY\Leftrightarrow\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}.\begin{bmatrix}a & b\\ c & d\end{bmatrix}=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}.\begin{bmatrix}x & y\\ z & t\end{bmatrix}$$

$$\Leftrightarrow\begin{bmatrix}a & b\\ a+c & b+d\end{bmatrix}=\begin{bmatrix}x+z & y+t\\ z & t\end{bmatrix}$$

$$\Leftrightarrow\begin{cases}a=x+z\ (1)\\ b=y+t\ (2)\\ a+c=z\ (3)\\ b+d=t\ (4)\end{cases}$$

Từ (1) và (3) suy ra $x+c=0\Leftrightarrow x=c=0$ (vì $x,c\in\mathbb{N}$).

Từ (2) và (4) suy ra $y+d=0\Leftrightarrow y=d=0$ (vì $y,d\in\mathbb{N}$).

Khi đó hai ma trận $X=\begin{bmatrix}a & b\\ 0 & 0\end{bmatrix},Y=\begin{bmatrix}0 & 0\\ z & t\end{bmatrix}$ có định thức bằng 0.

Điều này mâu thuẫn với giả thiết $X,Y\in M$. Vậy ta được điều phải chứng minh.

iii) Nếu $A_1\neq B_1$ thì vì A_1,B_1 là P hoặc Q nên

$$A_1A_2\dots A_m=B_1B_2\dots B_n\Longrightarrow PX=QY$$

Với X và Y là $A_2\dots A_m$ hoặc $B_2\dots B_n$.

Theo ii) điều này là vô lý. Vậy $A_1=B_1$. Từ đó ta được

$(*)\Leftrightarrow A_2\dots A_m=B_2\dots B_n$ (vì P và Q là các ma trận khả nghịch).

Lập luận tương tự trên ta được $A_i=B_i$, với mọi $i\le m$ và $m=n$.

Vì nếu $m<n$ thì

$$(*)\Leftrightarrow I=B_{m+1}B_{m+2}\dots B_n\ (**)$$

Vì $B_{m+1}=P$ hoặc $B_{m+1}=Q$. Nên (**) được viết lại thành:

$I = PX$ hoặc $I = QX$ với $X = B_{m+2} \dots B_n \in M$.

Theo i) điều này là vô lý. Vậy $m = n$. Ta được điều phải chứng minh.

3.1.4. Định lý (Rivett & Mackinnon, 1986). $P = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ và $Q = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ là hai ma trận nguyên tố duy nhất trong tập M và mọi ma trận (khác ma trận đơn vị) thuộc M đều phân tích được thành tích của các ma trận P, Q và sự phân tích này là duy nhất.

Chứng minh

* Ta chứng minh khẳng định "Mọi ma trận (khác ma trận đơn vị) thuộc M đều phân tích được thành tích của các ma trận P, Q" bằng cách chứng minh mệnh đề tương đương với nó:

"Nếu một ma trận thuộc M nhưng không phân tích được thành tích của các ma trận P, Q thì ma trận đó phải là ma trận đơn vị".

Giả sử $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M$ nhưng

$A \neq XP, A \neq YQ, A \neq PZ, A \neq QT$ với mọi $X, Y, Z, T \in M$.

Giả thiết này cho ta kết luận

$A.P^{-1} \notin M, A.Q^{-1} \notin M, P^{-1}.A \notin M, Q^{-1}.A \notin M$ vì nếu ngược lại thì ta chọn

$X = A.P^{-1}, Y = A.Q^{-1}, Z = P^{-1}.A, T = Q^{-1}.A$

và ta lại có $A = A.P^{-1}P = XP, A = A.Q^{-1}Q = YQ,$

$A = P.P^{-1}.A = PZ, A = Q.Q^{-1}.A = QT$

Điều này mâu thuẫn với giả thiết.

Do đó $\begin{bmatrix} a & b \\ c & d \end{bmatrix}.\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^{-1} \notin M, \begin{bmatrix} a & b \\ c & d \end{bmatrix}.\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{-1} \notin M$ (5)

Và $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^{-1}\begin{bmatrix} a & b \\ c & d \end{bmatrix} \notin M, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{-1}.\begin{bmatrix} a & b \\ c & d \end{bmatrix} \notin M$ (6)

+ Từ (5) ta có $\begin{bmatrix} a & b \\ c & d \end{bmatrix}.\begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \notin M$ và $\begin{bmatrix} a & b \\ c & d \end{bmatrix}.\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \notin M$

Nghĩa là $\begin{bmatrix} a-b & b \\ c-d & d \end{bmatrix} \notin M$ và $\begin{bmatrix} a & -(a-b) \\ c & -(c-d) \end{bmatrix} \notin M$

Vì hai ma trận này đều có định thức bằng 1 và $a, b, c, d \in \mathbb{N}$ nên để chúng không thuộc M thì $a - b$ và $c - d$ phải là các số nguyên trái dấu nhau.

Nghĩa là $\begin{cases} a-b>0 \\ c-d<0 \end{cases}$ hoặc $\begin{cases} a-b<0 \\ c-d>0 \end{cases} \Leftrightarrow \begin{cases} a \geq b+1 \\ d \geq c+1 \end{cases}$ hoặc $\begin{cases} a \leq b-1 \\ d \leq c-1 \end{cases}$

Do đó ta có hai bất phương trình $ad \geq (b+1)(c+1)$ hoặc $ad \leq (b-1)(c-1)$.

+ Từ (6) ta có $\begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}.\begin{bmatrix} a & b \\ c & d \end{bmatrix} \notin M$ và $\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}.\begin{bmatrix} a & b \\ c & d \end{bmatrix} \notin M$

Nghĩa là $\begin{bmatrix} a & b \\ -(a-c) & -(b-d) \end{bmatrix} \notin M$ và $\begin{bmatrix} a-c & b-d \\ c & d \end{bmatrix} \notin M$

Vì hai ma trận này đều có định thức bằng 1 và $a, b, c, d \in \mathbb{N}$ nên để chúng không thuộc M thì $a - c$ và $b - d$ phải là các số nguyên trái dấu nhau.

Nghĩa là $\begin{cases} a-c>0 \\ b-d<0 \end{cases}$ hoặc $\begin{cases} a-c<0 \\ b-d>0 \end{cases} \Leftrightarrow \begin{cases} a \geq c+1 \\ d \geq b+1 \end{cases}$ hoặc $\begin{cases} a \leq c-1 \\ d \leq b-1 \end{cases}$

Ta lại có hai bất phương trình $ad \geq (b+1)(c+1)$ hoặc $ad \leq (b-1)(c-1)$.

+ Hơn nữa, vì $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M$ nên $ad - bc = 1$.

Thay vào các bất phương trình trên ta đều được $b + c \leq 0$. Do đó $b = c = 0$.

Lúc này từ giả thiết $ad - bc = 1$ ta suy ra $a = d = 1$.

Khi đó $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ (ta được điều phải chứng minh).

* Bây giờ ta chứng minh ngoài hai ma trận P và Q ở trên thì trong tập M không còn ma trận nguyên tố nào khác.

Giả sử A là một ma trận khác ma trận đơn vị thuộc M. Khi đó theo chứng minh trên, tồn tại ma trận X thuộc M sao cho

$A = XP$ hoặc $A = XQ$ hoặc $A = PX$ hoặc $A = QX$

Nếu $X \neq I$ thì vì $P, Q \neq I$ nên A không phải ma trận nguyên tố.

Nếu $X = I$ thì $A = P$ hoặc $A = Q$.

Vậy ta chỉ có hai ma trận nguyên tố P và Q trong tập M.

* Cuối cùng, ta chứng minh sự phân tích một ma trận thành tích của các ma trận P, Q là duy nhất.

Giả sử $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ là một ma trận khác ma trận đơn vị thuộc M. Khi đó theo chứng minh trên, tồn tại ma trận X_1 thuộc M sao cho

$A = X_1P$ hoặc $A = X_1Q$ hoặc $A = PX_1$ hoặc $A = QX_1$

Bằng cách đồng nhất các vế của đẳng thức ma trận ta tìm được ma trận X_1 (lần lượt) có dạng như sau:

$\begin{bmatrix} a-b & b \\ c-d & d \end{bmatrix}$ hoặc $\begin{bmatrix} a & b-a \\ c & d-c \end{bmatrix}$ hoặc $\begin{bmatrix} a & b \\ c-a & d-b \end{bmatrix}$ hoặc $\begin{bmatrix} a-c & b-d \\ c & d \end{bmatrix}$

Dễ thấy các phần tử trong ma trận X_1 nhỏ hơn hoặc bằng các phần tử trong ma trận A.

+ Nếu $X_1 = I$ thì sự phân tích kết thúc.

+ Nếu $X_1 \neq I$ thì theo chứng minh trên, tồn tại ma trận X_2 thuộc M sao cho

$X_1 = X_2P$ hoặc $X_1 = X_2Q$ hoặc $X_1 = PX_2$ hoặc $X_1 = QX_2$

Và các phần tử trong ma trận X_2 nhỏ hơn hoặc bằng các phần tử trong ma trận X_1.

Quá trình phân tích trên sẽ kết thúc bởi vì các phần tử trong ma trận $X_i \in M$ $(i \in \mathbb{N})$ là các số tự nhiên và ngày càng giảm dần. Do đó tồn tại $n \in \mathbb{N}$ hữu hạn sao cho $X_n = I$.

Hơn nữa vì phép nhân hai ma trận không có tính giao hoán nên cuối cùng ta được:

$A = A_1A_2 \dots A_n$ với A_i là P hoặc Q $(n, i \in \mathbb{N}; i \leq n)$

Tính duy nhất của phân tích trên được suy ra từ 2.1.3 iii).

3.2. Sự phân tích ma trận thành tích các ma trận nguyên tố

Giả sử $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ là một ma trận khác ma trận đơn vị thuộc M. Khi đó theo phần chứng minh trên, luôn tồn tại ma trận X thuộc M sao cho

$A = XP$ hoặc $A = XQ$ hoặc $A = PX$ hoặc $A = QX$.

Với ma trận X (tương ứng với từng phân tích trên) là một trong bốn dạng sau:

$\begin{bmatrix} a-b & b \\ c-d & d \end{bmatrix}$ hoặc $\begin{bmatrix} a & b-a \\ c & d-c \end{bmatrix}$ hoặc $\begin{bmatrix} a & b \\ c-a & d-b \end{bmatrix}$ hoặc $\begin{bmatrix} a-c & b-d \\ c & d \end{bmatrix}$

Như vậy, ma trận X sẽ:

+ có dạng 1 nếu ma trận A có các phần tử ở cột 1 lớn hơn hoặc bằng cột 2.

+ có dạng 2 nếu ma trận A có các phần tử ở cột 2 lớn hơn hoặc bằng cột 1.

+ có dạng 3 nếu ma trận A có các phần tử ở dòng 2 lớn hơn hoặc bằng dòng 1.

+ có dạng 4 nếu ma trận A có các phần tử ở dòng 1 lớn hơn hoặc bằng dòng 2.

Do đó ta rút ra được quy tắc để phân tích A thành tích các ma trận nguyên tố như sau:

3.2.1. Phương pháp

*Nếu A có các phần tử ở cột 1 lớn hơn hoặc bằng cột 2 ($a \geq b, c \geq d$) thì A được phân tích thành: $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a-b & b \\ c-d & d \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = XP$.

*Nếu A có các phần tử ở cột 2 lớn hơn hoặc bằng cột 1 ($b \geq a, d \geq c$) thì A được phân tích thành: $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b-a \\ c & d-c \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = XQ$.

*Nếu A có các phần tử ở dòng 1 lớn hơn hoặc bằng dòng 2 ($a \geq c, b \geq d$) thì A được phân tích thành: $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a-c & b-d \\ c & d \end{bmatrix} = QX$.

*Nếu A có các phần tử ở dòng 2 lớn hơn hoặc bằng dòng 1 ($c \geq a, d \geq b$) thì A được phân tích thành: $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c-a & d-b \end{bmatrix} = PX$.

Lặp lại quá trình phân tích trên cho ma trận X. Quá trình này sẽ kết thúc và cuối cùng ta được:

$A = P^{n_1}Q^{n_2}P^{n_3} \dots P^{n_{k-1}}Q^{n_k}$ hoặc $A = Q^{n_1}P^{n_2}Q^{n_3} \dots Q^{n_{k-1}}P^{n_k}$

hoặc $A = P^{n_1}Q^{n_2}P^{n_3} \dots Q^{n_{k-1}}P^{n_k}$ hoặc $A = Q^{n_1}P^{n_2}Q^{n_3} \dots P^{n_{k-1}}Q^{n_k}$

với $n_1, \dots, n_r \in \mathbb{N}$.

3.2.2. Ví dụ

a) Cho ma trận $A = \begin{bmatrix} 3 & 2 \\ 4 & 3 \end{bmatrix} \in M$. Hãy phân tích A thành tích của các ma trận P và Q.

b) Cho ma trận $B = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \in M$. Hãy phân tích B thành tích của các ma trận P và Q.

Giải. Để lời chú thích được gọn, từ giờ thay vì viết "dòng/cột i có các phần tử lớn hơn hoặc bằng dòng/cột j" ta sẽ ký hiệu $d_i \geq d_j$ hoặc $c_i \geq c_j$.

a) * Ta có $A = \begin{bmatrix} 3 & 2 \\ 4 & 3 \end{bmatrix} = \underbrace{\begin{bmatrix} 3-2 & 2 \\ 4-3 & 3 \end{bmatrix}}_{X_1}\underbrace{\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}}_{P} = \underbrace{\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}}_{X_1}P$ (vì A có $c_1 \geq c_2$)

$= \underbrace{\begin{bmatrix} 1 & 2-1 \\ 1 & 3-1 \end{bmatrix}}_{X_2}\underbrace{\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}}_{Q}P = \underbrace{\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}}_{X_2}QP$ (vì X_1 có $c_2 \geq c_1$)

$= \underbrace{\begin{bmatrix} 1 & 1-1 \\ 1 & 2-1 \end{bmatrix}}_{X_3}\underbrace{\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}}_{Q}QP = \underbrace{\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}}_{X_3=P}QQP$ (vì X_2 có $c_2 \geq c_1$)

Vậy $A = PQ^2P$.

* Quá trình phân tích ma trận A có thể triển khai theo cách khác. Tuy nhiên đáp số vẫn sẽ giống nhau. Chẳng hạn,

Ta có $A = \begin{bmatrix} 3 & 2 \\ 4 & 3 \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}}_{P}\underbrace{\begin{bmatrix} 3 & 2 \\ 4-3 & 3-2 \end{bmatrix}}_{X_1} = P\underbrace{\begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix}}_{X_1}$ (vì A có $d_2 \geq d_1$)

$= P\underbrace{\begin{bmatrix} 3-2 & 2 \\ 1-1 & 1 \end{bmatrix}}_{X_2}\underbrace{\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}}_{P} = P\underbrace{\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}}_{X_2}P$ (vì X_1 có $c_1 \geq c_2$)

$$= P\underbrace{\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}}_{Q}\underbrace{\begin{bmatrix}1-0 & 2-1\\ 0 & 1\end{bmatrix}}_{X_3}P = PQ\underbrace{\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}}_{X_3=Q}P \qquad (\text{vì } X_2 \text{ có } d_1 \geq d_2)$$

Vậy $A = PQ^2P$.

b) Tương tự như câu a, nhưng ta có thể trình bày ngắn gọn hơn như sau:

$$B = \begin{bmatrix}1 & 2\\ 3 & 7\end{bmatrix} = \begin{bmatrix}1 & 1\\ 3 & 4\end{bmatrix}Q = \begin{bmatrix}1 & 0\\ 3 & 1\end{bmatrix}Q^2 = \begin{bmatrix}1 & 0\\ 2 & 1\end{bmatrix}PQ^2 = \begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}P^2Q^2 = P^3Q^2.$$

4. Kết luận

Bài viết đã làm rõ khái niệm "ma trận nguyên tố" (theo nghĩa của Rivett & Mackinnon). Bài viết cũng đã làm rõ những phần được lược giản trong bài viết của Rivett và Mackinnon. Cụ thể là chứng minh chi tiết, đầy đủ mọi trường hợp cho kết quả: trong tập gồm các ma trận vuông cấp 2 với hệ số nguyên không âm và định thức bằng 1 chỉ có hai ma trận nguyên tố và mọi ma trận trong tập này (ngoại trừ ma trận đơn vị) đều có thể biểu diễn được duy nhất thành tích của hai ma trận nguyên tố đó. Bài viết cũng đề xuất phương pháp phân tích một ma trận (vuông cấp 2 với hệ số nguyên không âm và định thức bằng 1) thành tích các ma trận nguyên tố này và trình bày các ví dụ minh hoạ cụ thể. Nội dung này, Rivett và Mackinnon đã không nhắc đến trong bài viết của họ.

Như vậy, thông qua bài viết chúng ta có thể thấy khái niệm "ma trận nguyên tố" (theo nghĩa của Rivett & Mackinnon) được định nghĩa tương đồng với khái niệm số nguyên tố. Tính chất có vô số số nguyên tố đã không còn đúng đối với ma trận nguyên tố cấp 2. Tuy nhiên kết quả về sự phân tích các số thành tích của các số nguyên tố vẫn còn đúng đối với ma trận nguyên tố cấp 2 (xét trong tập các ma trận vuông cấp 2 với hệ số nguyên không âm và định thức bằng 1).

Nội dung của bài viết có thể được phát triển tiếp theo hướng ứng dụng sự phân tích thành tích của các ma trận nguyên tố trong việc tìm ước chung lớn nhất và bội chung nhỏ nhất của các ma trận vuông đã được tác giả trình bày trong (Hoà & Trinh, 2016) và (Hoà, 2017).

TÀI LIỆU THAM KHẢO

[1] Alan F. Beardon (2009). Prime matrices and prime polynomials. *The Mathematical Gazette*, 93(528), pp.433-440.

[2] D.J. Richman and H. Schneider (1974). Primes in the semigroup of non-negative matrices. *Linear and multilinear Algebra*, Vol.2, pp.135-140.

[3] David C.Lay, Steven R.Lay, Judi J.McDonald (2016). *Linear algebra and it's applications – 5th ed.* Boston: Pearson.

[4] G.Picci, J.M. van den Hof, J.H. van Schuppen (1998). Primes in several classes of the possitive matrices. *Linear algebra and it's applications*, 277, pp.149-185.

[5] Nguyễn Thị Khánh Hòa, Nguyễn Thị Kiều Trinh (2016). Ước chung lớn nhất của các ma trận vuông. *Tạp chí khoa học Đại học Thủ Dầu Một*, số 27, p.68-75.

[6] Nguyễn Thị Khánh Hòa (2017). Bội chung nhỏ nhất của các ma trận. *Tạp chí khoa học Đại học Thủ Dầu Một*, số 32, p.198-205.

[7] Nguyễn Tiến Dũng (2018). *Đại số tuyến tính - Lý thuyết và ứng dụng*. NXB Đại học Quốc Gia thành phố Hồ Chí Minh.

[8] Nguyễn Tiến Tài (1999). *Số học*. NXB Giáo dục.

[9] P.F. Rivett and N.I.P. Mackinnon. (1986). Prime matrices. *The Mathematical Gazette*, 70(454), pp.257-259.

[10] R. Rivest, A. Shamir, L. Adleman (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communication of the ACM*, *21*(2), pp. 120-126.