Square roots of matrices

Aryaman Maithani

June 5, 2022

§1. Introduction

Given a complex square matrix A, can we always find a square matrix B such that $B^2 = A$? We shall see that the answer to this is "no" (see Exercise 3.1).
We shall show that this *is* true for invertible matrices. The crux will be to show that this is true for (invertible) Jordan blocks. The general result follows from that quite simply.

After that, we will show that the square root can actually be written as a polynomial in A. This has a pleasant consequence that an invertible symmetric matrix has a symmetric square root. Again, the trick will be to show it first for Jordan blocks. However, the generalisation is not so easy now since the polynomials we get will depend on the Jordan block. Thus, we need to get a suitable "interpolating" polynomial to finish the task.

The facts used will be quite simple, namely the existence of Jordan canonical form and the existence of a (formal) power series of $\sqrt{1+x}$.

This was inspired by `https://math.stackexchange.com/q/4465256/427810`.

§2. Basic notions and preliminaries

§§2.1. Jordan blocks

We shall use $M_n(\mathbb{C})$ to denote the set of all $n \times n$ matrices with complex entries. The identity matrix will be denoted by I, the size will be clear from context.
Given *any* $M \in M_n(\mathbb{C})$, we define $M^0 := I$.

Recall that a Jordan block refers to a matrix of the form

$$J = \begin{bmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & \ddots & 0 & 0 \\ 0 & 0 & \lambda & \ddots & 0 & 0 \\ 0 & 0 & 0 & \ddots & 1 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda \end{bmatrix}.$$

In words: it is a matrix with all diagonal entries λ, all superdiagonal entries 1, and all other entries 0. The value λ is the *eigenvalue* of J.

Lastly, recall the existence of a *Jordan (canonical) form*.

Theorem 2.1 (Jordan form)**.** Let $A \in M_n(\mathbb{C})$. Then, there exists an invertible matrix P such that $P^{-1}AP$ is of the form

$$\mathbf{J} = \begin{bmatrix} J_1 & O & O & \cdots & O \\ O & J_2 & O & \cdots & O \\ O & O & J_3 & \cdots & O \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ O & O & O & \cdots & J_k \end{bmatrix}, \tag{2.1}$$

where each J_i is a Jordan block (of possibly different sizes) and each O is a zero matrix of the appropriate size.

Note that it is possible that the same λ appears in different Jordan blocks.

The above form is particularly useful since block matrices can be multiplied in the naïve way. In particular, one has

$$\begin{bmatrix} A_1 & O & \cdots & O \\ O & A_2 & \cdots & O \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \cdots & A_k \end{bmatrix}^2 = \begin{bmatrix} A_1^2 & O & \cdots & O \\ O & A_2^2 & \cdots & O \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \cdots & A_k^2 \end{bmatrix}, \tag{2.2}$$

where $A_1, \ldots, A_k$ are *any* square matrices (and the Os are zero matrices of appropriate sizes).

Thus, to find a square root for the matrix $\mathbf{J}$ in (2.1), it suffices to find square roots for each Jordan block J_i. Moreover, once we have found a square root of $\mathbf{J}$, we also have a square of A, by the following observation.

Observation 2.2. Given $M, P \in M_n(\mathbb{C})$ with P invertible, we have

$$(PMP^{-1})^k = PM^kP^{-1}$$

for all $k \geqslant 0$.

In particular, if $M^2 = \mathbf{J}$ and $A = P\mathbf{J}P^{-1}$, then

$$(PMP^{-1})^2 = PM^2P^{-1} = P\mathbf{J}P^{-1} = A.$$

§§2.2. Formal square root

We wish to find a power series expansion for "$\sqrt{1+X}$". What we mean is: we wish to find a sequence $(a_n)_{n \geqslant 0}$ of complex numbers such that

$$\left(\sum_{n \geqslant 0} a_n X^n\right)^2 = 1 + X,$$

where the above equality is to be interpreted *formally*, i.e., in the power series ring $\mathbb{C}[\![X]\!]$. If you do not know what this means, you can simply just restrict your attention to the following:

Proposition 2.3. There exists a sequence of complex numbers $(a_n)_{n \geqslant 0}$ such that the following conditions are true:

$$\begin{aligned} a_0^2 &= 1, \\ 2a_0a_1 &= 1, \text{ and} \\ \sum_{k=0}^{n} a_k a_{n-k} &= 0 \text{ for all } n \geqslant 2. \end{aligned}$$

Sketch. Start by setting $a_0 = 1$. Check that the remaining a_n can be recursively calculated. The crucial point to note is that in each linear equation, the coefficient of the highest index term will be $2a_0$ and we can divide by $2a_0$. □

In the proof above, we get a unique sequence $(a_n)_{n \geqslant 0}$ once we fix $a_0 = 1$. We will use the suggestive notation $\binom{\frac{1}{2}}{n}$ for a_n.

Remark 2.4. The reader familiar with some analysis might have already known that the above sequence exists and is explicitly given as

$$\binom{\frac{1}{2}}{n} = \frac{\left(\frac{1}{2}\right)\left(\frac{1}{2}-1\right)\cdots\left(\frac{1}{2}-(n-1)\right)}{n!}.$$

However, note that we are satisfied by the equality being a purely formal one, and not bothering with any convergence issues. We also do not care about the exact value of the coefficient above.

§§2.3. Polynomials in matrices

Let $A \in M_n(\mathbb{C})$ be a square matrix and $p(X) \in \mathbb{C}[X]$ be a polynomial, say

$$p(X) = a_0 + a_1X + \cdots + a_mX^m.$$

Then, it makes sense to talk about the evaluation at A, denoted $p(A)$, given by

$$p(A) = a_0I + a_1A + \cdots + a_mA^m.$$

A matrix that can be written as $p(A)$ for some polynomial $p(X)$ is said to a polynomial in A.

Note the following subtlety: We are assuming that we have written the polynomial in expanded form and *then* we replace X by A (and the constant is treated as a scalar multiple of the appropriate size identity matrix).
To emphasise the importance of the above, consider the following equality in $\mathbb{C}[X]$:

$$(X-1)(X+1) = X^2 - 1.$$

If we wish to evaluate the above polynomial at A, then the definition says that we must substitute A on the *right hand side*. It does **not** say that we can evaluate it as $(A-I)(A+I)$. However, convince yourself that this *is* actually always valid. Similarly, convince yourself that a similar thing holds true for addition of polynomials.
In fancy lingo, we have a *homomorphism*.

We now state two results on polynomial evaluations, the proofs of which are elementary and are left to the reader.

Theorem 2.5. Let $A, P \in M_n(\mathbb{C})$ with P invertible, and let $p(X) \in \mathbb{C}[X]$. Then,

$$p(P^{-1}AP) = P^{-1}p(A)P.$$

Theorem 2.6. Suppose $A_1, \ldots, A_k$ are square matrices of possibly different sizes, and $p(X) \in \mathbb{C}[X]$. Then, the polynomial can be evaluated on a block diagonal matrix as follows:

$$p\left(\begin{bmatrix} A_1 & O & \cdots & O \\ O & A_2 & \cdots & O \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \cdots & A_k \end{bmatrix}\right) = \begin{bmatrix} p(A_1) & O & \cdots & O \\ O & p(A_2) & \cdots & O \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \cdots & p(A_k) \end{bmatrix}.$$

In fact, (2.2) was a special case of the above.

§3. Square roots of Jordan blocks

In this section, we tackle the problem of finding square roots for Jordan blocks. We immediately start by seeing an example where a Jordan block does *not* have a square root.

Exercise 3.1. Let $J = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. Show that there is no $M \in M_2(\mathbb{C})$ such that $M^2 = J$.

Solution. One way of solving the above is to simply assume four variables as the entries of M and show that there is no solution.

Another way is to use the following fact: Suppose $M \in M_n(\mathbb{C})$ is a nilpotent matrix, i.e., $M^k = O$ for *some* $k \geqslant 1$. Then, $M^n = O$ (note that n is the size of M).[1]
Now, we see that any supposed square root M would have to satisfy $M^4 = O$. But the fact then would force that $M^2 = O \neq J$. □

Thus, going forward, we shall assume that the Jordan block has nonzero eigenvalue. This is equivalent to the Jordan block being invertible. Moreover, in the notations of Theorem 2.1, A being invertible is equivalent to each Jordan block J_i being invertible.

Let J be a Jordan block with eigenvalue $\lambda \neq 0$. Then, we can write

$$J = \lambda(I + N),$$

where N is the matrix with $1/\lambda$ on the superdiagonal, and 0 everywhere else.

[1] One way of proving this fact is by showing that the only eigenvalue of M is 0 and then consider the characteristic polynomial.

Note that N is a nilpotent matrix with $N^n = O$. Thus, $I + N$ has a square root given by the binomial power series

$$(I+N)^{1/2} = \sum_{k \geqslant 0} \binom{\frac{1}{2}}{k} N^k = I + \frac{1}{2}N - \frac{1}{8}N^2 + \cdots .$$

The crucial point to note is that the power series above will actually reduce to a finite sum since the terms involving N^n and higher powers will vanish.

Thus, we have shown the following.

Theorem 3.2. Let J be a Jordan block of size n with eigenvalue $\lambda \neq 0$. Define $N := \frac{1}{\lambda}J - I$, and let $\alpha \in \mathbb{C}$ be a square root of λ. Then, J has a square S given by

$$S = \alpha \sum_{k=0}^{n} \binom{\frac{1}{2}}{k} N^k. \tag{3.1}$$

Exercise 3.3. Convince yourself that S^2 is indeed $\lambda(I + N)$, using Proposition 2.3.

Observation 3.4. Note that the S is actually a polynomial in J since N is so.

§4. Square roots of invertible matrices

Combining the results and observations of the previous sections, we get the following.

Theorem 4.1. Let $A \in M_n(\mathbb{C})$ be an invertible matrix. Then, there exists $B \in M_n(\mathbb{C})$ such that $B^2 = A$.

We had already seen that A being invertible is not completely unnecessary since we have a counterexample with $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

Proof. We first put A in Jordan form as

$$P^{-1}AP = \begin{bmatrix} J_1 & O & \cdots & O \\ O & J_2 & \cdots & O \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \cdots & J_k \end{bmatrix}.$$

Then, for each J_i, we find a square root, let us denote this by $\sqrt{J_i}$.[2] Then, the matrix

$$P \begin{bmatrix} \sqrt{J_1} & O & \cdots & O \\ O & \sqrt{J_2} & \cdots & O \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \cdots & \sqrt{J_k} \end{bmatrix} P^{-1}$$

is a square root for A, simple! □

Now, note that we observed that $\sqrt{J_i}$ is actually a polynomial in J_i (Observation 3.4). Moreover, we noted how polynomials of block diagonal matrices are computed (Theorem 2.6), and how polynomial evaluations interacted with similarity (Theorem 2.5). Using these two facts, one would hope that we can write $\sqrt{A}$ also as a polynomial in A. However, the hindrance is the following: We did *not* find a common polynomial $p(X)$ such that $p(J_i) = \sqrt{J_i}$. Rather, for each J_i, we found some polynomial $p_i(X)$ such that $p_i(J_i) = \sqrt{J_i}$.

The next section is devoted to finding a common polynomial.

§5. Interpolation

In this section, given a Jordan block J, we shall denote the square found in Section 3 by $\sqrt{J}$. Similarly, given $\lambda \in \mathbb{C}$, $\sqrt{\lambda}$ will denote some square root of λ.

Theorem 5.1. Let $J_1, \ldots, J_k$ be Jordan blocks (of possibly different sizes), all having the same eigenvalue $\lambda \neq 0$. Then, there exists a common polynomial $p(X) \in \mathbb{C}[X]$ such that

$$p(J_i) = \sqrt{J_i}$$

for all $i \in \{1, \ldots, k\}$.

Proof. Following our earlier calculations, we see that if we set m as the size of the largest Jordan block, then the polynomial

$$p(X) := \sqrt{\lambda} \sum_{k=0}^{m-1} \binom{\frac{1}{2}}{k} \left(\frac{X}{\lambda} - 1 \right)^k$$

does the job. □

[2] Note that each Jordan block can have multiple square roots. We just found one explicitly, which we are denoting by $\sqrt{J_i}$.

Remark 5.2. Note that the polynomial above depends on λ as well as the size of the largest Jordan block. Thus, the theorem is only applicable to a finite collection of Jordan blocks. In particular, we have *not* found a polynomial that gives a square root for all Jordan blocks with eigenvalue λ.

Theorem 5.3. Fix $m \geqslant 1$ and distinct complex numbers $\lambda, \mu \in \mathbb{C}$.
Then, there exists a polynomial $q(X) \in \mathbb{C}[X]$ with the following property: $q(A) = O$ for all Jordan blocks of size at most m with eigenvalue μ, and $q(B) = I$ for all Jordan blocks of size at most m with eigenvalue λ.

Proof. Consider the polynomials $a(X) = (X - \mu)^m$ and $b(X) = (X - \lambda)^m$. The polynomials are coprime and thus, by the Chinese Remainder Theorem, there exists a polynomial $q(X) \in \mathbb{C}[X]$ such that

$$\begin{aligned} q(X) &\equiv 0 \mod a(X), \\ q(X) &\equiv 1 \mod b(X). \end{aligned}$$

Now, let A and B be matrices as given in the hypothesis. Then, $a(A) = O$ and in turn, $q(A) = O$. Similarly, $b(B) = O$ and thus, $q(B) = I$, as desired. □

Corollary 5.4. Let $J_1, \ldots, J_k$ be arbitrary Jordan blocks. There exists a polynomial $p(X) \in \mathbb{C}[X]$ such that $p(J_i) = \sqrt{J_i}$ for all i.

Proof. Let $\Lambda = \{\lambda_1, \ldots, \lambda_r\}$ be the set of distinct eigenvalues corresponding to the Jordan blocks. Let m be the size of the largest Jordan block.
For each $\lambda \in \Lambda$, let $p_\lambda(X) \in \mathbb{C}[X]$ be such that $p_\lambda(J_i) = \sqrt{J_i}$ for those J_i having λ as its eigenvalue (existence is given by Theorem 5.1).
For each $\lambda, \mu \in \Lambda$ with $\lambda \neq \mu$, let $q_{\lambda,\mu}(X) \in \mathbb{C}[X]$ be a polynomial that is O on the Jordan blocks corresponding to μ and is I on those corresponding to λ (existence is given by Theorem 5.3).

Next, for each $\lambda \in \Lambda$, define the polynomial

$$Q_\lambda(X) := \prod_{\mu \in \Lambda \setminus \{\lambda\}} q_{\lambda,\mu}(X).$$

Then, note that if J_i is a block with eigenvalue λ, then we have $Q_\lambda(J_i) = I$. Otherwise, we have $Q_\lambda(J_i) = O$.

Finally, defining the polynomial

$$p(X) := \sum_{\lambda \in \Lambda} Q_\lambda(X) p_\lambda(X)$$

does the job. □

Remark 5.5. The reader familiar with Lagrange interpolation would have realised that we are essentially trying to cook up the analogous Lagrange polynomials in the above proof.

§6. Square roots as polynomials

Combining the results of the previous sections, we see that we have proven the following theorem.

Theorem 6.1. Let $A \in M_n(\mathbb{C})$ be an invertible square matrix. Then, there exists a polynomial $p(X) \in \mathbb{C}[X]$ such that $(p(A))^2 = A$.

In words: A has a square root that can be written as a polynomial in A.

Proof. Let $J_1, \ldots, J_k$ be as in Theorem 2.1. Let $p(X)$ be as in Corollary 5.4, i.e., $(p(J_i))^2 = J_i$ for all $i \in \{1, \ldots, k\}$. Check that $(p(A))^2 = A$. □

The above has the following interesting corollary.

Corollary 6.2. Let $A \in M_n(\mathbb{C})$ be a symmetric invertible matrix. Then, A has a symmetric square root.

Proof. By the earlier result, A has a square root that can be expressed as a polynomial in A. Any polynomial in a symmetric matrix is again symmetric. □

Remark 6.3. You may be tempted to use Spectral theorem to somehow deduce the above. However, note that Spectral theorem deals with *Hermitian* matrices and not symmetric.

§7. Extensions to other fields

We briefly discuss the dependence of our discussion on the underlying field $\mathbb{C}$.

To begin with, the existence of Jordan form (for every matrix) is guaranteed precisely when the field is algebraically closed. Secondly, we needed a formal square root of $1 + X$. One can check that the proof sketch of Proposition 2.3 works in any field with characteristic different from 2. Lastly, we also required the existence of square roots of the eigenvalues (of course, this is automatically guaranteed if the field is algebraically closed).

Theorem 7.1. Let k be an algebraically closed field with $\operatorname{char}(\mathsf{k}) \neq 2$. Let $A \in M_n(\mathsf{k})$ be invertible. Then, A has a square root (which can be written as a polynomial in A).

Another relaxation is the following: The existence of Jordan form of a fixed matrix A is also granted if the characteristic polynomial of A factors into linear factors.

Theorem 7.2. Let $A \in M_n(\mathbb{R})$ be a real matrix such that the characteristic polynomial of A factors into real linear factors with each root positive. Then, A has a square root (which can be written as a polynomial in A).