

Quantum Information and Quantum Computation Report

The following contents are some summaries and notes of my course learning process.

Luotong, Jun 20, 2024

1 Quantum elementary concepts

1 Dirac notation

If

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \quad |\phi\rangle = \begin{pmatrix} \gamma \\ \delta \end{pmatrix} \quad (1)$$

then

$$\langle\psi|\phi\rangle \stackrel{def}{=} \langle\psi||\phi\rangle = (\bar{\alpha} \quad \bar{\beta}) \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \bar{\alpha}\gamma + \bar{\beta}\delta. \quad (2)$$

If the norm of V is defined:

$$\|v\| = \sqrt{\langle v|v\rangle}. \quad (3)$$

then

$$\langle v|u\rangle = \frac{1}{4}(\|v+u\|^2 - \|v-u\|^2 + i\|v+iu\|^2 - i\|v-iu\|^2). \quad (4)$$

Note

Here, $\langle v|u\rangle$ is correct. Because $\langle v|u\rangle$ is different from the notation $\langle v, u\rangle$ which means inner product in linear algebra. According to matrix definition of Dirac notation in equation (2), $\langle v|u\rangle$ is equal to $\langle u, v\rangle$. As $\langle u, v\rangle$ is equal to right part of equation (4) which is proved in linear algebra, $\langle v|u\rangle$ is equal to them as well.

2 Matrix Representation of Operator

$$A = \sum_{j,k} a_{jk} |j\rangle\langle k|, \quad a_{jk} = \langle j|A|k\rangle. \quad (5)$$

3 Complex Spectrum Theorem

A is a **normal** operator on n dimensional complex inner product space. Then A is diagonalizable under a set of orthonormal basis $\{|u_1\rangle, \dots, |u_n\rangle\}$:

$$A = \sum_i^n \lambda_i |u_i\rangle\langle u_i|. \quad (6)$$

4 A probabilistic model

The state of bits is represented by probability vector where the sum of entries equal to 1. The effect of performing linear operation on the bits is performing corresponding linear transforming on probability distribution. The transformation could be represented as probability matrix, whose entries are nonnegative numbers, and every column is a probability vector.

5 Quantum bits

In order to depict quantum bit, the superposition (or quantum state) is introduced. Similar to probabilistic model, vector is used for superposition. But the entry is allowed to be in complex field, and only normalized vector is legal. Accordingly, probability matrix is replaced by unitary matrix.

If the superposition of a qubit is

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \quad (7)$$

After measurement, the probability of outcome 0 and 1 is $|\alpha|^2$ and $|\beta|^2$ respectively.

2 Overview of quantum information

1 Multiple qubits and tensor product

Multiple qubits example: $\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$

Tensor product is defined as follows:

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,m} \end{pmatrix} \quad B = \begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,l} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,l} \\ \vdots & \vdots & \ddots & \vdots \\ b_{k,1} & b_{k,2} & \cdots & b_{k,l} \end{pmatrix} \quad (8)$$

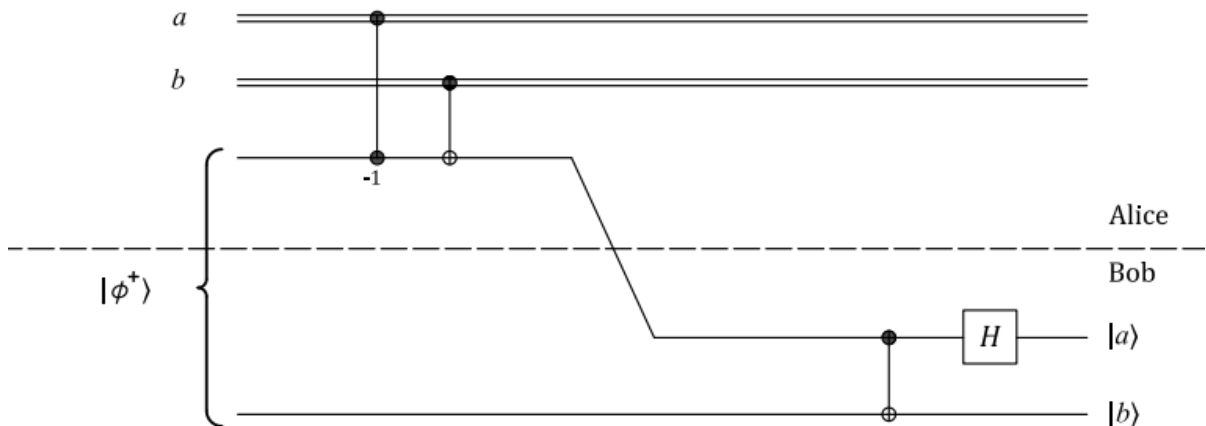
$$A \otimes B = \begin{pmatrix} a_{1,1}B & a_{1,2}B & \cdots & a_{1,m}B \\ a_{2,1}B & a_{2,2}B & \cdots & a_{2,m}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1}B & a_{n,2}B & \cdots & a_{n,m}B \end{pmatrix} \quad (9)$$

Important property about tensor product:

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$$

3 Superdense coding, quantum circuits, and partial measurements, Quantum teleportation

1 A quantum circuit diagram for superdense coding.



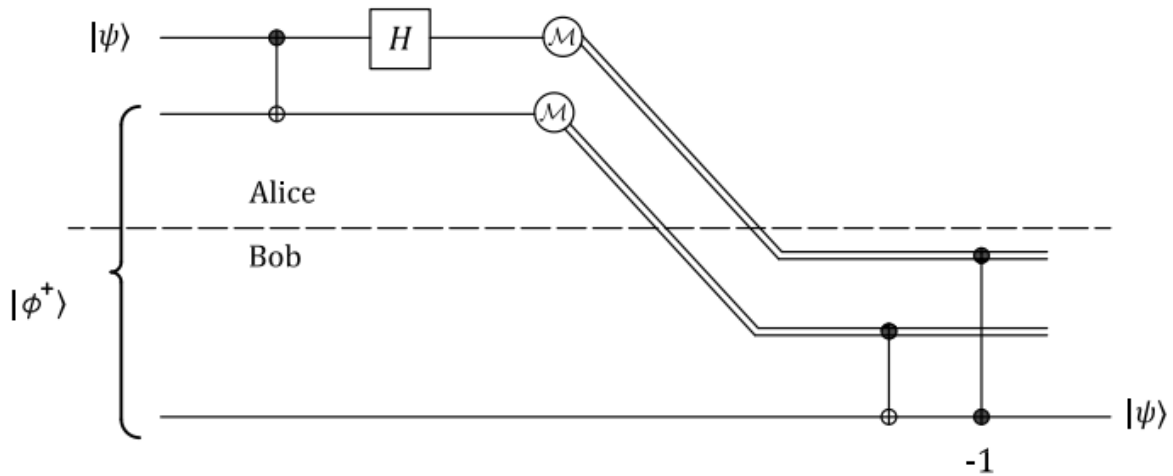
2 Partial measurements

The essence is conditional probability distribution. According to the definition of conditional probability

$$p(A|B) = \frac{p(AB)}{p(B)} \quad (10)$$

and definition of superposition in equation (7), it could be inferred how to make partial measurements over superposition of multiple qubits.

3 Quantum teleportation



If Alice's initial qubit was entangled with other qubits, this entanglement will be preserved. In other words, teleportation works like a perfect quantum channel—it is exactly as if Alice had physically sent her qubit to Bob. (Why?)

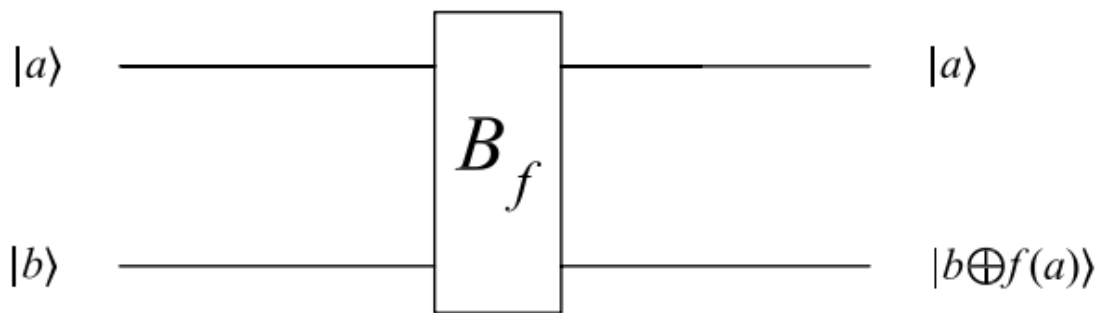
4 Deutsch's Algorithm

	f_0	f_1	f_2	f_3
Input 0	0	0	1	1
Input 1	0	1	0	1

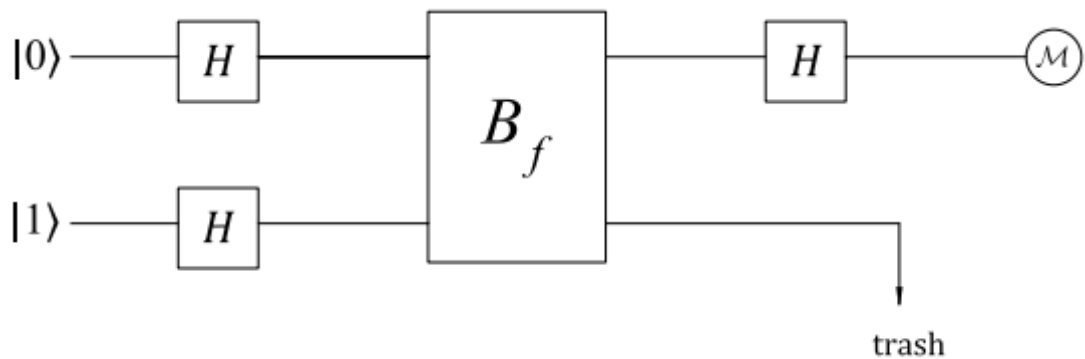
Determining whether a f is constant or balanced.

A quantum transformation B_f is defined as:

$$B_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle \quad (11)$$



Deutsch's Algorithm is as follows:



phase kick-back will happen during the above process, where the state of second qubit is completely independent of the first one, then is thrown away as trash.

The state of the first qubit after the final Hadmard transform is $(-1)^{f(0)}|f(0) \oplus f(1)\rangle$.

If the measured value is 0, f is constant, balanced otherwise.

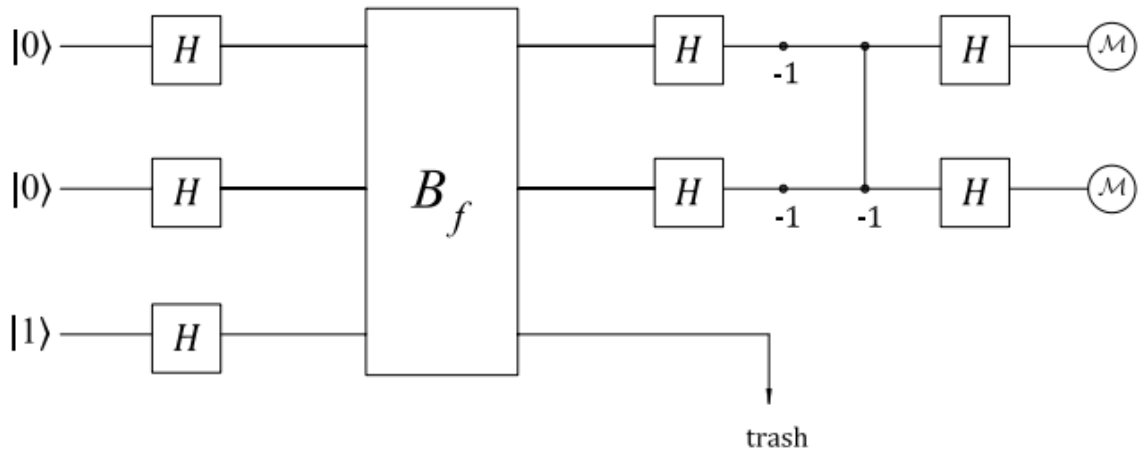
5 A simple searching algorithm; the Deutsch-Jozsa algorithm

Searching algorithm:

Determining which one of the following function is the given f .

f_{00}		f_{01}		f_{10}		f_{11}	
input	output	input	output	input	output	input	output
00	1	00	0	00	0	00	0
01	0	01	1	01	0	01	0
10	0	10	0	10	1	10	0
11	0	11	0	11	0	11	1

Algorithm:

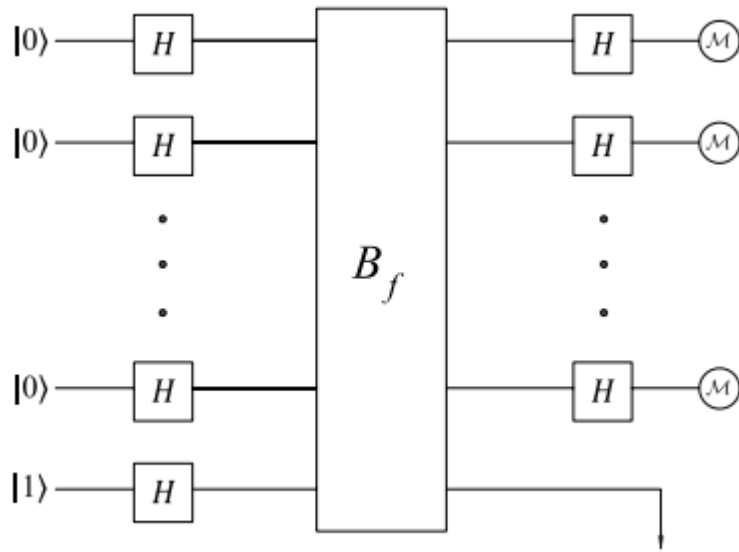


After B_f query and phase kickback, the possible state of first two qubits form an orthonormal set. And the following circuit is performing a unitary transformation and results in the subspace of f of the original set.

The Deutsch-Jozsa Algorithm

Given a function $f : \{0, 1\}^n \rightarrow \{0, 1\}$, determining whether f is constant or balanced.

Algorithm:



Phase kick-back is also applied in the algorithm.

If the measured outcome is all 0, f is constant, otherwise balanced.

6 Simon's Algorithm

Assume

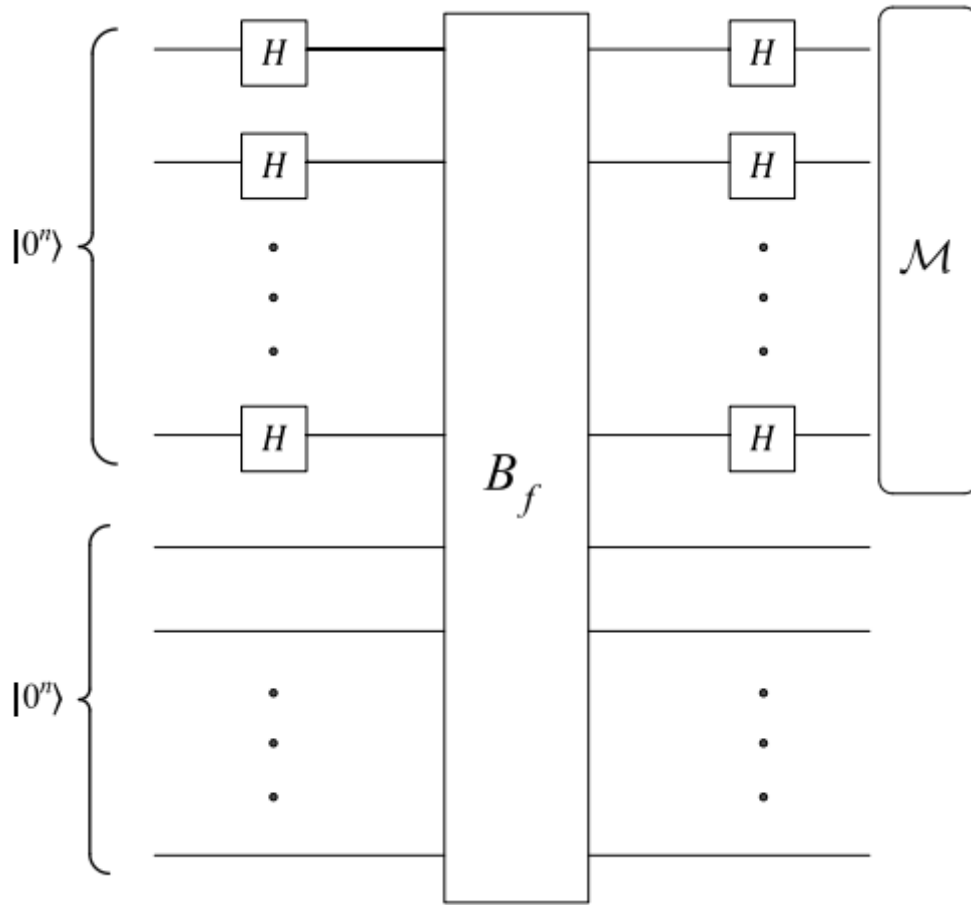
$$f : \{0, 1\}^n \rightarrow \{0, 1\}^n \quad (12)$$

and

$$[f(x) = f(y)] \Leftrightarrow [x \oplus y \in \{0^n, s\}] \quad (13)$$

The goal is to find the string s .

Simon's algorithm:



Phase kick-back is not used in this algorithm.

The analysis of the state show that the measurement result is always a uniformly sample from the orthogonal complement of string s . So the above circuit could be ran $n - 1$ times to obtain $n - 1$ linear independent vectors that are orthogonal to s . Solve the linear equation to get unique s' .

(Only $n - 1$ equation is sufficient, because calculation is performed in binary field.) If

$f(s') = f(0^n)$, then $s = s'$. Otherwise $s = 0^n$.

According to classical analysis, $n - 1$ vectors above is independent with a probability greater than $\frac{1}{4}$.

We can repeat the circuit $4m$ times, and the algorithm complexity is $O(n)$.

7 Quantum information revisited

1 Density matrices

For a quantum state $|\psi\rangle$, its density matrix(operator) representation is defined as follows:

$$|\psi\rangle\langle\psi| = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \begin{pmatrix} \bar{\alpha} & \bar{\beta} \end{pmatrix} = \begin{pmatrix} |\alpha|^2 & \alpha\bar{\beta} \\ \bar{\alpha}\beta & |\beta|^2 \end{pmatrix} \quad (14)$$

Note

Density matrix representation loss some information compared with vector representation of superposition. $|\psi\rangle\langle\psi|$ could be viewed as projection operator. Given projection operator P , the corresponding $|\psi\rangle$ is not unique. For example, $e^{i\theta}|\psi\rangle$ is another candidate.

Mixture state:

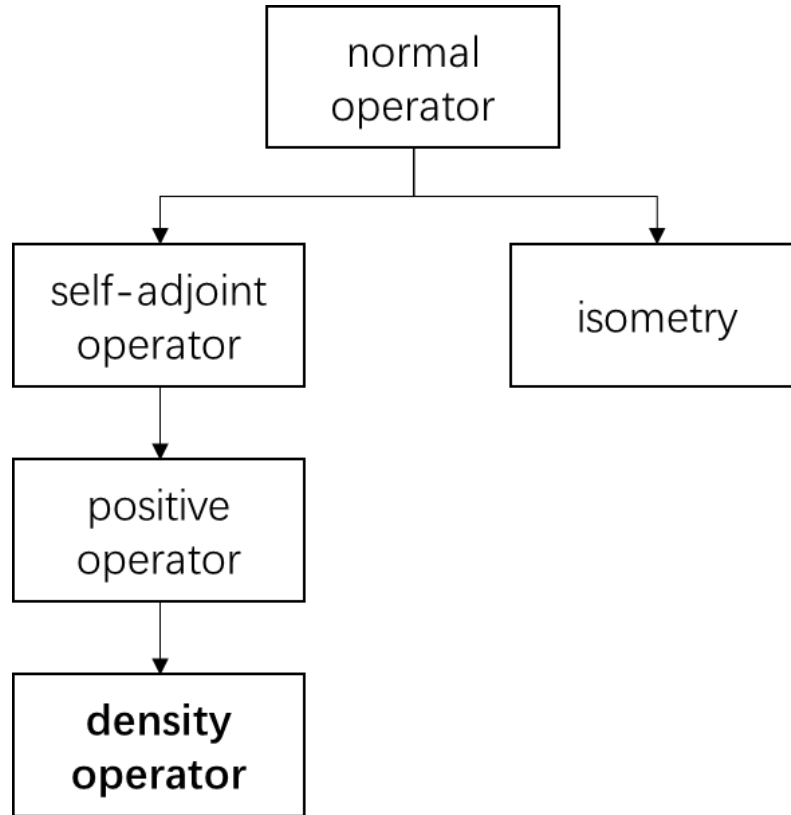
$$\sum_{j=1}^k p_j |\psi_j\rangle \langle \psi_j|. \quad (15)$$

Important Facts(If and only if):

- The trace of a density matrix is 1
- Every density matrix is positive semidefinite

Important

Connection to the operators in inner product space:



2 Operations on density matrices

Admissible operations(namely quantum channel, completely positive trace preserving operations) on density matrices is as follow :

$$\begin{aligned} \Phi(\rho) &= \sum_{j=1}^k A_j \rho A_j^\dagger, \\ \sum_{j=1}^k A_j^\dagger A_j &= I \end{aligned} \quad (16)$$

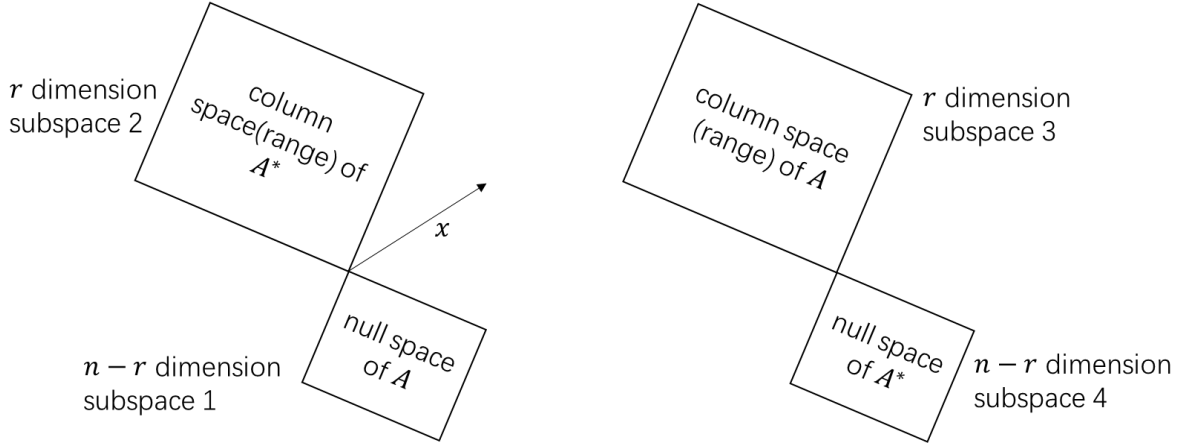
A linear transformation is a completely positive trace preserving **if and only if** it meet the form in equation (16).

Note

Quantum channel transform a density matrix to another density matrix.

Appendix: Viewing operators in inner product space from the perspective of Singular Value Decomposition

Assume A is a linear operator from n dimensional inner product space to itself, A^* is the adjoint of A , r is the rank. Their relationship could be illustrated as follows:



Lemma 1 : The nullspace of A^*A is equal to the nullspace of A .

$$Ax = 0 \Rightarrow A^*Ax = 0.$$

$$A^*Ax = 0 \Rightarrow \langle x, A^*Ax \rangle = 0 \Rightarrow \langle Ax, Ax \rangle = 0 \Rightarrow Ax = 0 \quad \blacksquare$$

Due to orthogonal complement relation, the column space of A^* is also the column space of $(A^*A)^* = A^*A$.

A^*A is positive operator, so it has non-negative eigenvalue.

According to polar decomposition, $A = S\sqrt{A^*A}$, S is isometry. So A can be defined by perform $\sqrt{A^*A}$ on subspace 2, and transform subspace 2 to subspace 3 by S .

Lemma 2: If $\sqrt{A^*A}x = \sigma_i x$, then $AA^*Ax = A\sigma_i^2 x = \sigma_i^2 Ax$, which means $A = S\sqrt{A^*A}$ map the eigen-subspace of $\sqrt{A^*A}$ with eigenvalue σ_i to the eigen-subspace of $\sqrt{AA^*}$ with same eigenvalue σ_i .

Those eigen-subspaces from one linear operator with different eigenvalue are orthogonal, So the isometry S appears in polar decomposition. Choosing orthonormal basis α, β from those eigen-subspaces respectively, A 's matrix representation is:

$$\begin{bmatrix} \sigma_1 & & & \\ & \ddots & & \\ & & \sigma_r & \\ & & & \mathbf{0} \end{bmatrix}_{\alpha}^{\beta} \quad (17)$$

It's a form of SVD.

Above all, transform A could be viewed as stretching each eigen-subspace of $\sqrt{A^*A}$ with σ_i by σ_i , and isometrically transform them to the eigen-subspace of $\sqrt{AA^*}$ with σ_i respectively.

1 Normal operator

Definition: $A^*A = AA^*$.

It means $\sqrt{A^*A} = \sqrt{AA^*}$, so the eigen-subspaces of $\sqrt{A^*A}$ and $\sqrt{AA^*}$ are the same. Those eigen-subspaces are **invariant subspace** under operator A . So an orthonormal basis α could be chose to give a matrix representation:

$$\begin{bmatrix} \sigma_1 S_1 & & & \\ & \ddots & & \\ & & \sigma_k S_k & \\ & & & \mathbf{0} \end{bmatrix}_{\alpha}^{\alpha} \quad (18)$$

$k \leq r$ is the number of different singular values. S_i is restriction operator of S on the eigen-subspace of $\sqrt{A^*A}$ with eigenvalue σ_i , denoted as $S|_{E(\sigma_i, \sqrt{A^*A})}$.

If A is in complex vector space. S_i is isometry, so it's diagonalizable, and eigenvalue $|\lambda_i| = 1$. So, by choosing another proper orthonormal basis β , following matrix is obtained:

$$\begin{bmatrix} \sigma_1 \begin{bmatrix} e^{i\theta_1} & & \\ & \ddots & \\ & & e^{i\theta_{d_1}} \end{bmatrix} & & \\ & \ddots & \\ & & \sigma_k \begin{bmatrix} e^{i\theta_1} & & \\ & \ddots & \\ & & e^{i\theta_{d_k}} \end{bmatrix} & \\ & & & \mathbf{0} \end{bmatrix}_{\beta}^{\beta} \quad (19)$$

d_j is the dimension of the eigen-subspace of $\sqrt{A^*A}$ with eigenvalue σ_j .

Lemma 3: It could be inferred from matrix (19) that singular value σ_i of a complex normal operator is just the amplitude of the corresponding eigenvalue.

If A is in real vector space, matrix (19) could be viewed as a matrix of complexification of A . It is known that the eigenvalue λ_i and its conjugate $\overline{\lambda_i}$ come in pairs. So the complex eigenvalues in matrix (19) could be paired according to conjugate.

Another fact is that

$$\begin{bmatrix} e^{i\theta} & \\ & e^{-i\theta} \end{bmatrix}_a^a = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}_b^b \quad (20)$$

a, b are both some orthonormal basis of the 2-dimensional space. In addition, vectors in b are all real vector.

So the matrix representation of A is as follows:

$$\left[\begin{array}{c} \sigma_1 \left[\begin{array}{cc} \cos\theta_1 & -\sin\theta_1 \\ \sin\theta_1 & \cos\theta_1 \end{array} \right] \\ \ddots \\ \pm 1 \\ \vdots \\ \sigma_k \left[\begin{array}{cc} \cos\eta_1 & -\sin\eta_1 \\ \sin\eta_1 & \cos\eta_1 \end{array} \right] \\ \ddots \\ \pm 1 \\ \mathbf{0} \end{array} \right]_{\gamma}^{\gamma} \quad (21)$$

γ is the proper orthonormal basis.

Lemma 4: It could be inferred from matrix (21) that, real normal operator is acting like performing stretching and rotating on some 2-dimensional subspaces, and performing only stretching on the rest one dimensional eigen-subspaces. And singular value is also the absolute value of those stretching factors respectively. Particularly, $\sigma_i = |\lambda_i|$.

2 Self-adjoint operator

$A^* = A \Rightarrow A^*A = AA^*$, so the self-adjoint operator A or its complexification has the matrix form (19).

If A is in complex vector space, self-adjoint means the matrix in (19) equals its hermitian form. So all the $e^{i\theta}$ within the matrix must equal 1 or -1 . Then all the eigenvalues of a complex self-adjoint operator are real value. And singular value is exactly the absolute part of the eigenvalue.

If A is in real vector space, its complexification has the property above. Then a proper real orthonormal basis ζ could be chose to make A is diagonalizable on real field.

3 positive operator

Positive operator is a self-adjoint operator with eigenvalue ≥ 0 . Therefore, its singular value is exactly its eigenvalue.

4 density operator

Density operator is a positive operator with trace = 1.

5 isometry

S is defined to be isometry if $S^*S = I$.

$S^*S = I$ means $S^{-1} = S^*$. According to the property of linear inverse, $SS^* = I$. Then $S^*S = SS^* = I$, so S is normal operator.

So S or its complexification will have the matrix form in (19).

Then $S^*S = I$ means $|\lambda_i|^2 = \sigma_i^2 = 1$.

If S is in complex vector space, then $\lambda_j = e^{i\theta_j}$. Following matrix form is obtained: (proper orthonormal basis is omitted.)

$$\begin{bmatrix} e^{i\theta_1} & & & \\ & e^{i\theta_2} & & \\ & & \ddots & \\ & & & e^{i\theta_n} \end{bmatrix} \quad (22)$$

If S is in real vector space, then $\lambda_j = \pm 1$. The following matrix representation is derived from matrix (21).

$$\begin{bmatrix} \begin{bmatrix} \cos\omega_1 & -\sin\omega_1 \\ \sin\omega_1 & \cos\omega_1 \end{bmatrix} & & & \\ & \ddots & & \\ & & \begin{bmatrix} \cos\omega_k & -\sin\omega_k \\ \sin\omega_k & \cos\omega_k \end{bmatrix} & \\ & & & \pm 1 & \\ & & & & \ddots & \\ & & & & & \pm 1 \end{bmatrix} \quad (23)$$

Lemma 5: It could be inferred that complex isometry is just stretching with $|\lambda_i| = 1$. And real isometry acts like rotating on some 2-dimensional subspaces, identity on one subspace, as well as reflecting about the origin on one subspace. Those subspaces are all orthogonal.

Bibliographies

1. Axler, S. (2015). *Linear algebra done right*. springer.
2. Strang, G. (2022). *Introduction to linear algebra*. Wellesley-Cambridge Press.