INTRO

(SA204)

Qiskit

1. Linear Algebra
2. Quantum Theory
3. Theory of Computation
4. Quantum Algorithms

Goal: Construct Shor's factoring algorithm.

Idea: Bits represent classical information

$$\mathbb{Z}_2 = \{0, 1\}$$

We want to compute a function

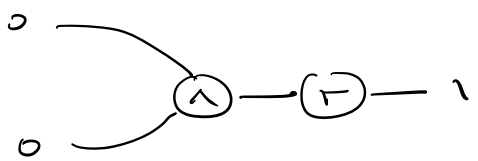
$$f : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2$$

We can do this by using basic gates

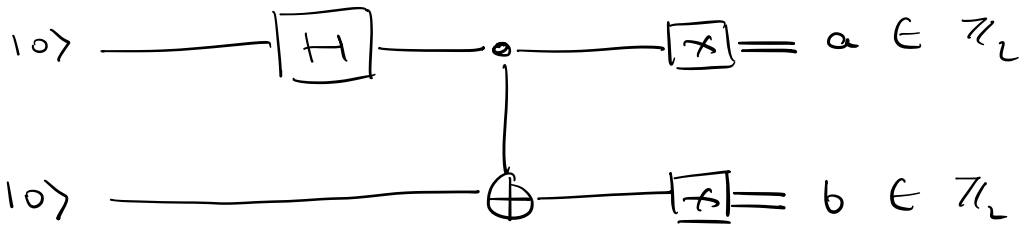
NOT: $\mathbb{Z}_2 \longrightarrow \mathbb{Z}_2$ $\quad 0 \mapsto 1$, $1 \mapsto 0$

AND: $\mathbb{Z}_2^2 \longrightarrow \mathbb{Z}_2$ $\quad 00 \mapsto 0$, $01 \mapsto 0$, $10 \mapsto 0$, $11 \mapsto 1$

e.g.



We can also compute any quantum circuits



bit $\mathbb{Z}_2$ ⟿ qubit $\mathbb{C}^2$

$\{0,1\}$ $\quad |\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$\alpha, \beta \in \mathbb{C}$

Fundamental question

Do we gain any computational power ?

Complexity classes

$O(2^{\sqrt{n}})$ ~ hard NP BQP QC

↓

FACTORING ~ $O(n^2)$

$n = \log N$

easy P

LINEAR ALGEBRA

Vector spaces

A vector space (only finite dimensional) is a set V together with

$$+ : V \times V \longrightarrow V \qquad (v, w) \longmapsto v + w$$

$$\cdot : \mathbb{C} \times V \longrightarrow V \qquad (\alpha, v) \longmapsto \alpha v$$

such that

$(V, +, 0)$ abelian group:

1. $v + w = w + v \quad \forall\, v, w \in V$
2. $(u + v) + w = u + (v + w) \quad \forall\, u, v, w \in V$
3. $\exists\, 0 \in V : 0 + v = v \quad \forall\, v \in V$
4. $\forall\, v \in V, \exists\, w \in W : v + w = 0$

scalar multiplication:

5. $(\alpha\beta)v = \alpha(\beta v) \quad \forall\, v \in V,\ \alpha, \beta \in \mathbb{C}$
6. $1 v = v \quad \forall\, v \in V$

distributive property:

7. $\alpha(u + v) = \alpha u + \alpha v \quad \forall\, u, v \in V,\ \forall\, \alpha \in \mathbb{C}$

$$(\alpha + \beta)v = \alpha v + \beta v$$

Ex $\mathbb{C}^n = \{ (\alpha_1, \dots, \alpha_n) : \alpha_i \in \mathbb{C} \}$

$$v = (\alpha_1, \dots, \alpha_n) \qquad w = (\beta_1, \dots, \beta_n)$$

$$v + w = (\alpha_1 + \beta_1, \dots, \alpha_n + \beta_n)$$

$$\lambda \cdot v = (\lambda\alpha_1, \dots, \lambda\alpha_n) \qquad \lambda \in \mathbb{C}.$$

$$0 = (0, \dots, 0)$$

Basis

Let Σ be a finite set and

$$S = \{ v_\alpha \in V : \alpha \in \Sigma \}.$$

S is called linearly dependent if

$$\exists \{ \lambda_\alpha \}_{\alpha \in \Sigma} \text{ not all zero} : \sum_\alpha \lambda_\alpha v_\alpha = 0.$$

Otherwise, S is called linearly independent.

The subspace

$$\operatorname{span}(S) = \left\{ v = \sum_\alpha \lambda_\alpha v_\alpha : \lambda_i \in \mathbb{C} \right\}$$

is called the span of S.

If $\operatorname{span}(S) = V$ then S is called spanning.

A linearly independent spanning set S is called a basis and

$$\dim(V) = \underbrace{|S|}_{\text{size of } S}.$$

Ex: $\mathbb{C}^n$ has basis $\{ e_i \}_{i=1}^n$ where

$$e_i = (0, \dots, 0, \underbrace{1}_{i\text{th}}, 0, \dots, 0)$$

Linear operators

A linear operator $A: V \longrightarrow W$ is a function such that

$$A\left(\sum_i \lambda_i v_i\right) = \sum_i a_i A(v_i)$$

$$\forall\, v_i \in V, \quad \forall\, \lambda_i \in \mathbb{C}.$$

We will write $L(V, W)$ for the set of linear operators.

$L(V, W)$ is a vector space:

$$(A+B)\,v = A(v) + B(v)$$

$$(\lambda A)\,v = \lambda A(v) \qquad \forall\, v \in V,\ \lambda \in \mathbb{C}.$$

Zero operator:

$$0: V \longrightarrow W, \quad v \mapsto 0 \quad \forall\, v \in V.$$

Identity operator

$$\mathbb{1}: V \longrightarrow V, \quad v \mapsto v \quad \forall\, v \in V.$$

Composition of operators:

$$L(U,V) \times L(V,W) \longrightarrow L(U,W)$$
$$(A, B) \longmapsto AB$$

$$(AB)(v) = A(B(v)).$$

We say V is isomorphic to W if there exists linear operators

$$A: V \longrightarrow W \quad \text{and} \quad B: W \longrightarrow V$$

such that $AB = \mathbb{1}_W$ & $BA = \mathbb{1}_V$.
In this case we write $V \cong W$.

Ex $L(\mathbb{C}, V) \xrightarrow{\cong} V$

$A: \mathbb{C} \to V \longmapsto A(1)$

Ex Let Σ be a finite set.

$$\mathbb{C}^\Sigma = \{ v : \Sigma \longrightarrow \mathbb{C} \text{ functions} \}$$

is a vector space:

$$(v+u)(a) = v(a) + u(a)$$
$$(\lambda v)(a) = \lambda v(a) \qquad \forall\, a \in \Sigma$$

Basis: $e_a : \Sigma \longrightarrow \mathbb{C}$

$$e_a(b) = \begin{cases} 1 & a = b \\ 0 & a \neq b \end{cases}$$

We can write

$$v = \sum_{a \in \Sigma} v(a)\, e_a .$$

Let $f : \Sigma \longrightarrow \{1, \dots, n\}$ be a bijection.

Then

$$\begin{array}{ccc} \mathbb{C}^{\Sigma} & \xrightarrow{\cong} & \mathbb{C}^{n} \\ e_a & \longmapsto & e_{f(a)} \end{array}$$

E.g. $\Sigma = \{00, 01, 10, 11\}$

$$\cong \{0,1\} \times \{0,1\}$$

More generally let $\{v_a\}_{a \in \Sigma}$ be a basis for V then

$$\begin{array}{ccc} V & \xrightarrow{\cong} & \mathbb{C}^{\Sigma} . \\ v_a & \longmapsto & e_a \end{array}$$

Composing linear operators:

$$\begin{array}{ccc} V & \xrightarrow{\cong} & \mathbb{C}^{\Sigma} \\ & \searrow^{\cong} & \downarrow \cong \\ & & \mathbb{C}^{n} \end{array}$$

$n = |\Sigma| = \dim(V)$

Inner product spaces

An inner product on V is a function

$$\langle -, - \rangle : V \times V \longrightarrow \mathbb{C}$$

such that

1. $\langle v, v \rangle \geq 0 \quad \forall\, v \in V$ and
   $\langle v, v \rangle = 0 \iff v = 0$
2. $\langle v, \sum_i \lambda_i v_i \rangle = \sum \lambda_i \langle v, v_i \rangle \quad \forall\, v, v_i \in V$, $\forall\, \lambda_i \in \mathbb{C}$
3. $\langle v, w \rangle = \overline{\langle w, v \rangle}$ (complex conjugate)

Ex: $\mathbb{C}^{\Sigma} \times \mathbb{C}^{\Sigma} \longrightarrow \mathbb{C}$

$$\langle v, w \rangle = \sum_{a \in \Sigma} \overline{v(a)}\, w(a).$$

A vector space V together with an inner product is called an inner product space, also known as a Hilbert space.

Norm of v:

$$\| v \| = \sqrt{\langle v, v \rangle}$$

Unit vector:

$$\| v \| = 1.$$

Orthogonal basis

Let $S = \{v_1, \dots, v_n : v_i \in V\}$.

S is called <u>orthogonal</u> if

$$\langle v_i, v_j \rangle = 0 \quad \forall\, i \neq j.$$

S is called <u>orthonormal</u> if

$$\langle v_i, v_j \rangle = \delta_{ij} = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$$

Orthonormal basis = orthonormal + basis
(orthogonal) (orthogonal)

<u>Ex</u> $\{e_a\}_{a \in \Sigma}$ is an orthonormal basis.

$$\langle e_a, e_{a'} \rangle = \sum_{b \in \Sigma} \overline{e_a(b)}\, e_{a'}(b)$$

$$= \sum_b \delta_{a,b}\, \delta_{a',b}$$

$$= \delta_{a,a'}.$$

Gram – Schmidt procedure

Let $\{w_1, \dots, w_n\}$ be linearly independent.

Then $\{v_1, \dots, v_n\}$ where

$$v_1 = \frac{1}{\|w_1\|} w_1$$

$$v_{k+1} = \frac{w_{k+1} - \sum_{i=1}^{k} \langle v_i, w_{k+1} \rangle v_i}{\left\| w_{k+1} - \sum_{i=1}^{k} \langle v_i, w_{k+1} \rangle v_i \right\|}$$

for $1 \le k \le n-1$

is orthonormal and

$$\operatorname{span}\{v_i\}_{i=1}^{n} = \operatorname{span}\{w_i\}_{i=1}^{n}.$$

Cauchy–Schwarz inequality

Suppose $v, w \in V$. Then

$$|\langle v, w \rangle| \leq \|v\| \, \|w\|.$$

This inequality is an equality $\Leftrightarrow$ one of v, w is a scalar multiple of the other

Proof: If $w = 0$ then equality holds.

If $w = \alpha v$ then

$$|\langle v, \alpha v \rangle| = |\alpha| \, |\langle v, v \rangle| = \|v\| \, \|\alpha v\|$$

i.e. equality holds.

Assume $w \neq 0$ & $\{w, v\}$ is linearly indep. ($w = v_1$, $v = v_2$)

Gram–Schmidt procedure gives an orthonormal set $\{v_1, v_2\}$ such that

$$v_1 = \frac{1}{\|w\|} w.$$

Then

$$\langle v, v \rangle \langle w, w \rangle = \sum_{i=1}^{2} \langle v, v_i \rangle \langle v_i, v \rangle \langle w, w \rangle$$

$$\geq \langle v, v_1 \rangle \langle v_1, v \rangle \langle w, w \rangle$$

$$= \langle v, w \rangle \langle w, v \rangle \frac{\langle w, w \rangle}{\|w\|^2}$$

$$= |\langle v, w \rangle|^2$$

$\square$

($v = \sum_{i=1}^{2} \langle v_i, v \rangle v_i$, $\Pi_W = \sum_{i=1}^{2} v_i v_i^+$, $W = \operatorname{span}\{w, v\}$)

Linear Isometry

A linear operator $A: V \to W$ is a linear isometry if

$$\langle A(v), A(w) \rangle = \langle v, w \rangle \quad \forall v, w \in V.$$

We write $U(V, W)$ for the set of linear isometries.

HW: Isometry $\iff$ $\| A(v) \| = v \quad \forall v \in V$.

If $W = V$ then we write

$$U(V) = U(V, V).$$

This is called the group of unitary operators:

$$- \circ - : U(V) \times U(V) \to U(V)$$

Associativity: $(AB)C = A(BC)$

Unit: $\mathbb{1}_V A = A \mathbb{1}_V = A$

Inverse: $A^+ A = A A^+ = \mathbb{1}_V$

i.e. A^+ is the inverse, also denoted by A^{-1}.

$U(V)$ is not abelian.

Ex: Let $\{v_a\}_{a \in \Sigma}$ be an orthonormal basis for V. Then

$$A: V \xrightarrow{\cong} \mathbb{C}^{\Sigma}$$

$$v_a \longmapsto e_a$$

is a linear isometry:

$$\langle A(v_a), A(v_b) \rangle = \langle e_a, e_b \rangle = \delta_{a,b}$$

and $(v_a, v_b) = \delta_{a,b}$.

Adjoint operator

Adjoint of a linear operator $A: V \to W$ is the linear operator

$$A^+ : W \to V$$

uniquely specified by

$$\langle w, A(v) \rangle_W = \langle A^+(w), v \rangle_V$$

$$\forall\, v \in V,\ w \in W.$$

Ex: Any $v \in V$ determines a linear operator

$$v : \mathbb{C} \to V,\quad 1 \mapsto v.$$

Let us compute the adjoint:

$$v^+ : V \to \mathbb{C}:$$

$$\langle u, \underbrace{v(a)}_{av} \rangle_V = \langle v^+(u), a \rangle_{\mathbb{C}}$$

$$\underbrace{a\langle u, v \rangle}_{a\langle u, v \rangle} = \overline{v^+(u)}\, a$$

$$v^+(u) = \langle v, u \rangle$$

In addition

$$\begin{array}{ccc} V & \xrightarrow{\cong} & L(V, \mathbb{C}) \\ v & \longmapsto & v^+ \end{array}$$

Outer product

More generally for $v \in V$ and $u \in U$ we can define a linear operator

$$uv^+ : V \longrightarrow W$$

$$v' \longmapsto (uv^+)(v') = \langle v, v' \rangle u.$$

(uv^+: outer product)

HW: $(uv^+)^+ = vu^+$

Trace:

Unique linear operator

$$Tr : L(V) \longrightarrow \mathbb{C}$$

that satisfies

$$Tr(uv^+) = \langle v, u \rangle \quad \forall v, u \in V.$$

HW: Show that $Tr(AB) = Tr(BA)$.

Ex: Let us compute

$$Tr^+ : \mathbb{C} \longrightarrow L(V)$$

$$\underbrace{\langle Tr^+(1), A \rangle_{L(V)}}_{Tr((Tr^+(1))^+ A)} = \langle 1, Tr\, A \rangle_{\mathbb{C}}$$

$$= Tr(A)$$

Then $Tr^+(1) = \mathbb{1}_V$.

Hilbert-Schmidt inner product

$$L(V,W) \times L(V,W) \longrightarrow \mathbb{C}$$

$$\langle A, B \rangle = \mathrm{Tr}(A^\dagger B)$$

HW: Show that this is an inner product.

Let $\{v_a\}_{a \in \Sigma}$ and $\{u_b\}_{b \in \Gamma}$ be orthonormal (orthogonal) bases for V and W then

$$\{u_b v_a^\dagger\}_{\substack{a \in \Sigma \\ b \in \Gamma}}$$

is an orthonormal (orthogonal) basis for $L(V,W)$:

$$\langle u_b v_a^\dagger, u_{b'} v_{a'}^\dagger \rangle = \mathrm{Tr}\left((u_b v_a^\dagger)^\dagger u_{b'} v_{a'}^\dagger\right)$$

$$= \mathrm{Tr}\left(v_a u_b^\dagger u_{b'} v_{a'}^\dagger\right)$$

$$= \mathrm{Tr}\left(u_{b'} v_{a'}^\dagger v_a u_b^\dagger\right)$$

$$= \delta_{(a,b),(a',b')}$$

In particular, $\{uv^\dagger\}_{\substack{u \in W \\ v \in V}}$ is spanning in $L(V,W)$.

↳ Composition :

$$(u_{b'} v_{a'}^{\dagger})(v_a u_b^{\dagger})(v) = \langle v_{a'}, v_a \rangle u_{b'} u_b^{\dagger}(v)$$

$$(v_a u_b^{\dagger})(v) = \langle u_b, v \rangle v_a$$

$$\langle v_{a'}, v_a \rangle \langle u_b, v \rangle u_{b'}$$

Matrix representation

Recall that $V \cong \mathbb{C}^{\Sigma}$ for any vector space V where $|\Sigma| = \dim(V)$.

In effect we can consider $V = \mathbb{C}^{\Sigma}$ and $W = \mathbb{C}^{\Gamma}$.

Then

$$L(\mathbb{C}^{\Sigma}, \mathbb{C}^{\Gamma}) \xrightarrow{\cong} \mathbb{C}^{\Sigma \times \Gamma}$$

$$A : \mathbb{C}^{\Sigma} \to \mathbb{C}^{\Gamma} \longmapsto A : \Sigma \times \Gamma \to \mathbb{C}$$

where

$$A(a,b) = \langle e_a, A e_b \rangle$$

Hilbert-Schmidt inner product:

Let $V = \mathbb{C}^{\Sigma}$, $W = \mathbb{C}^{\Gamma}$ and

$$E_{ab} : \Sigma \times \Gamma \to \mathbb{C}$$

$$(a',b') \longmapsto \begin{cases} 0 & (a',b') \neq (a,b) \\ 1 & (a',b') = (a,b) \end{cases}$$

The set $\{E_{ab}\}_{a \in \Sigma, b \in \Gamma}$ is an orthonormal basis for $L(\mathbb{C}^{\Sigma}, \mathbb{C}^{\Gamma})$:

1) $A = \sum_{a,b} A(a,b)\, E_{ab}$

2) $\operatorname{Tr}(E_{ab}^{+} E_{cd}) = \operatorname{Tr}(E_{ba} E_{cd})$

$= \delta_{ac} \operatorname{Tr}(E_{bd})$

$= \delta_{ac} \delta_{bd}$

$= \delta_{(a,b),(c,d)}$

Therefore

$L(\mathbb{C}^{\Sigma}, \mathbb{C}^{\Gamma}) \xrightarrow{\cong} \mathbb{C}^{\Sigma \times \Gamma}$

is a linear isometry.

Ex:

1) $L(\mathbb{C}, \mathbb{C}^{\Gamma}) \cong \mathbb{C}^{\{1\} \times \Gamma} \cong \mathbb{C}^{\Gamma}$

2) $L(\mathbb{C}^{\Sigma}, \mathbb{C}) \cong \mathbb{C}^{\Sigma \times \{1\}} \cong \mathbb{C}^{\Sigma}$.

In the case

$$\Sigma = \{1, \dots, n\} \quad \& \quad \Gamma = \{1, \dots, m\}$$

we write $A_{ij} = A(i,j)$ and

$$A = \begin{pmatrix} A_{11} & \cdots & A_{1m} \\ \vdots & & \vdots \\ A_{n1} & \cdots & A_{nm} \end{pmatrix}.$$

A vector $v \in \mathbb{C}^{\Sigma}$ is represented by a column

$$v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

where $v = \sum_i v_i e_i$.

The vector Av is computed by matrix multiplication.

Composition of linear operators

$$L(\mathbb{C}^\Sigma, \mathbb{C}^\Gamma) \times L(\mathbb{C}^\Gamma, \mathbb{C}^\Lambda) \longrightarrow L(\mathbb{C}^\Sigma, \mathbb{C}^\Lambda)$$

$$(A, B) \longmapsto AB$$

is represented by matrix multiplication:

$$(AB)(a,c) = \sum_{b \in \Gamma} A(a,b)\, B(b,c).$$

In the case $\Lambda = \{1, \dots, k\}$

$$AB = \begin{pmatrix} A_{11} & \cdots & A_{1m} \\ \vdots & & \vdots \\ A_{n1} & \cdots & A_{nm} \end{pmatrix} \begin{pmatrix} B_{11} & \cdots & B_{1k} \\ \vdots & & \vdots \\ B_{m1} & \cdots & B_{mk} \end{pmatrix}$$

Adjoint of A:

$$A^+(a,b) = \overline{A(b,a)} \qquad (\text{HW: } (AB)^+ = B^+ A^+)$$

that is

$$A = \begin{pmatrix} \overline{A}_{11} & \cdots & \overline{A}_{n1} \\ \vdots & & \vdots \\ \overline{A}_{1m} & \cdots & \overline{A}_{nm} \end{pmatrix} = (\overline{A})^T.$$

Ex: $v^+ = (\overline{v}_1 \ \cdots \ \overline{v}_n)$.

Tensor product (Kronecker product)

The tensor product of $V = \mathbb{C}^{\Sigma}$ and $W = \mathbb{C}^{\Gamma}$ is the vector space

$$V \otimes W = \mathbb{C}^{\Sigma \times \Gamma}.$$

We write $v \otimes w$ for the function

$$\begin{aligned} v \otimes w : \Sigma \times \Gamma &\longrightarrow \mathbb{C} \\ (a, b) &\longmapsto v(a)\, w(b) \end{aligned}$$

and call this an elementary tensor.

The set $\{ e_a \otimes e_b \}_{\substack{a \in \Sigma \\ b \in \Gamma}}$ is a basis.

In particular, $\{ v \otimes w \}_{\substack{v \in V \\ w \in W}}$ is spans.

Note that we have

$$v \otimes \Big(\sum_i \lambda_i w_i \Big) = \sum_i \lambda_i (v \otimes w_i)$$

and

$$\Big(\sum_j \mu_j v_j \Big) \otimes w = \sum_j \mu_j v_j \otimes w.$$

$V \otimes W$ is an inner product space:

$$\langle v \otimes w, v' \otimes w' \rangle_{V \otimes W} = \langle v, v' \rangle_V \langle w, w' \rangle_W$$

Linear operators on tensor products:

$$L(V_1, V_2) \otimes L(W_1, W_2) \xrightarrow{\cong} L(V_1 \otimes V_2, W_1 \otimes W_2)$$

$$A \otimes B \longmapsto A \otimes B : V_1 \otimes V_2 \longrightarrow W_1 \otimes W_2$$
$$v_1 \otimes v_2 \longmapsto Av_1 \otimes Av_2$$

$\Rightarrow$ a linear isometry.

In matrix notation:

$$A \otimes B = \begin{pmatrix} A_{11} & \cdots & A_{1m} \\ \vdots & & \vdots \\ A_{n1} & \cdots & A_{nm} \end{pmatrix} \begin{pmatrix} B_{11} & \cdots & B_{1l} \\ \vdots & & \vdots \\ B_{k1} & \cdots & B_{kl} \end{pmatrix}$$

$$= \begin{pmatrix} A_{11}B & \cdots & A_{1m}B \\ \vdots & & \vdots \\ A_{n1}B & \cdots & A_{nm}B \end{pmatrix}$$

Trace of the tensor:

$$\mathrm{Tr}(A \otimes B) = \mathrm{Tr}(A)\,\mathrm{Tr}(B).$$

(HW: $\mathrm{Tr}(A \otimes B) = \mathrm{Tr}(A)\,\mathrm{Tr}(B)$)

Dirac notation

Vectors are represented by kets:

$$|v\rangle$$

Adjoints of vectors v^+ are represented by bras:

$$\langle v|$$

The inner product $\langle v, u\rangle$ is represented by

$$\langle v|u\rangle \qquad v, u \in V$$

Outer product vw^+ is represented by

$$|w\rangle\langle v| \qquad v \in V,\ w \in W$$

It acts on a vector $|u\rangle$ as follows

$$(|w\rangle\langle v|)\,|u\rangle = |w\rangle\langle v|u\rangle$$
$$= \langle v|u\rangle\,|w\rangle.$$

Composition

$$(|w\rangle\langle v|)(|w'\rangle\langle v'|) =$$

$$= |w\rangle\langle v|w'\rangle\langle v'|$$

$$= \langle v|w'\rangle\, |w\rangle\langle v'|$$

Trace

$$\mathrm{Tr}(|w\rangle\langle v|) = \mathrm{Tr}(\langle v|w\rangle)$$

$$= \langle v|w\rangle .$$

Tensor product vow is represented by

$$|v\rangle \otimes |w\rangle \quad \text{or} \quad |v\rangle|w\rangle .$$

Qubit

Let $\mathbb{C}^2 = \mathbb{C}^{\{0,1\}}$ ($\Sigma = \{0,1\}$)

The basis vectors e_0 & e_1 of $\mathbb{C}^2$ are denoted using the ket notation:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

The space of linear operators

$$L(\mathbb{C}^2, \mathbb{C}^2)$$

has an orthogonal basis given by

$$E_{00} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$E_{01} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$E_{10} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

$$E_{11} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Pauli operators

$$\sigma_0 = \mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \sigma_1 = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_2 = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_3 = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Then $\{ \mathbb{1}, X, Y, Z \}$ is an orthogonal basis for $L(\mathbb{C}^2, \mathbb{C}^2)$:

$$\mathrm{Tr}(\sigma_i \sigma_j) = 2 \delta_{ij}.$$

$\left\{ \frac{1}{\sqrt{2}} \sigma_i \right\}$ is orthonormal basis.

We can write $A \in L(\mathbb{C}^2, \mathbb{C}^2)$ as

$$A = \frac{1}{2} \sum_i \langle G_i, A \rangle G_i$$

Relations among Pauli operators:

$$G_i^2 = \mathbb{1}$$

$$G_i G_j = - G_j G_i \qquad i \neq j$$

$$G_2 = i\, G_1 G_3$$

Some important unitary operators:

Hadamard gate

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Phase gate

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

T-gate

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$ (Qutrit)

Multi-qubits

$\{0,1\} \times \{0,1\} \cong \{00, 01, 10, 11\}$

The tensor product

$$\mathbb{C}^{\{0,1\}} \otimes \mathbb{C}^{\{0,1\}} = \mathbb{C}^{\{0,1\} \times \{0,1\}} \cong \mathbb{C}^{\{00, 01, 10, 11\}}$$

has basis vectors

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

In general

$$(\mathbb{C}^2)^{\otimes n} = \underbrace{\mathbb{C}^{\{0,1\}} \otimes \cdots \otimes \mathbb{C}^{\{0,1\}}}_{n \text{ copies}}$$

has basis given by

$$|a_1 \cdots a_n\rangle \qquad a_i \in \{0,1\}.$$

The operator space

$$L\left((\mathbb{C}^2)^{\otimes n}, (\mathbb{C}^2)^{\otimes n} \right)$$

has an orthogonal basis given by

$$\left\{ \sigma_{i_1} \otimes \sigma_{i_2} \otimes \cdots \otimes \sigma_{i_n} : i_1, \ldots, i_n \in \{0,1,2,3\} \right\}$$

Important unitary operators:

CNOT: $\mathbb{C}^2 \otimes \mathbb{C}^2 \longrightarrow \mathbb{C}^2 \otimes \mathbb{C}^2$

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

We can also write

$$CNOT\left(|ab\rangle \right) = |a \underbrace{(a+b)}_{\text{mod 2 sum.}}\rangle$$

SWAP: $\mathbb{C}^2 \otimes \mathbb{C}^2 \longrightarrow \mathbb{C}^2 \otimes \mathbb{C}^2$

$$SWAP\left(|ab\rangle \right) = |ba\rangle$$

HW: matrix rep. of SWAP.

Eigenvalues and eigenvectors

Let $A \in L(V)$.

A vector $v \neq 0$ in V is called an eigenvector of A corresponding to $\lambda \in \mathbb{F}$ if $Av = \lambda v$.

(λ: eigenvalue)

Eigenspace of A corresponding to λ:

$$V_\lambda = \{ v \in V \text{ eigenvector corresponding to } \lambda \} \cup \{0\}$$

λ is said to be degenerate if $\dim V_\lambda > 1$

Note that every A has at least one eigenvalue and a corresponding eigenvector since the characteristic polynomial

$$\det(A - \lambda \mathbb{1}_V)$$

has at least one root.

Suppose $A \in L(V)$.
A number $\lambda \in \mathbb{C}$ is an eigenvalue of A if there exists $v \neq 0$ in V such that

$$Av = \lambda v.$$

Let λ be an eigenvalue of A.

A is (unitarily) diagonalizable if there exists an orthonormal basis $\{v_a\}_{a \in \Sigma}$ such that

$$A = \sum_a \lambda_a \underbrace{v_a v_a^\dagger}_{\text{eigenvector corres. to eigenval. } \lambda_a} \qquad \lambda_a \in \mathbb{C}.$$

An operator $A \in L(\mathbb{C}^\Sigma)$ is diagonal if

$$A(a,b) = 0 \quad \text{for all} \quad a \neq b.$$

Then $A \in L(\mathbb{C}^\Sigma)$ is diagonalizable $\iff$ $\exists\, U \in U(\mathbb{C}^\Sigma)$ such that

$$U^\dagger A U \text{ is a diagonal operator.}$$

Ex $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is diagonal in the basis:

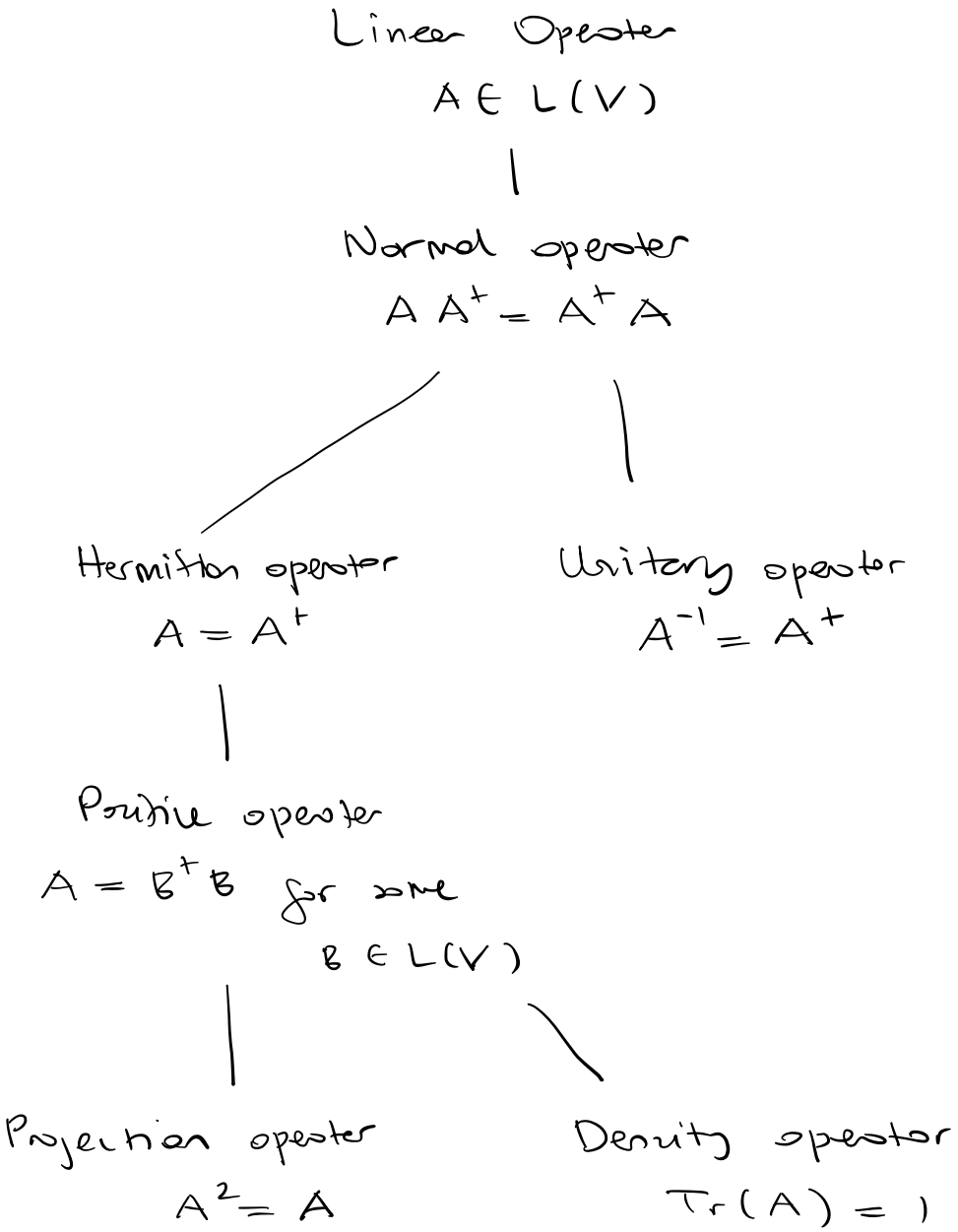
$$\{ |+\rangle = H|0\rangle \;,\; |-\rangle = H|1\rangle \}$$

$$= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \qquad = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

HW: $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ is diagonal in

$$\{ |i\rangle = SH|0\rangle \;,\; |-i\rangle = SH|1\rangle \}$$

Important classes of operators



HW: Describe them for $V = \mathbb{C}$.

Spectral decomposition

$A \in L(V)$ is diagonalizable $\iff$

A is normal: $AA^+ = A^+A$.

Proof: Assume A is diagonalizable:

$$A = \sum_a \lambda_a v_a v_a^+$$

for some orthonormal basis $\{v_a\}_{a \in \Sigma}$.

Then

$$A^+A = \left(\sum_b \overline{\lambda}_b v_b v_b^+ \right) \left(\sum_a \lambda_a v_a v_a^+ \right)$$

$$= \sum_{a,b} \overline{\lambda}_b \lambda_a \delta_{a,b} v_b v_a^+$$

$$= \left(\sum_a \lambda_a v_a v_a^+ \right) \left(\sum_b \overline{\lambda}_b v_b v_b^+ \right)$$

$$= A A^+.$$

For the other direction we will do induction on $d = \dim V$.

For $d = 1$: $L(V) \cong L(\mathbb{C}) \cong \mathbb{C}$.

Let $d \geq 2$.

Let λ be an eigenvalue of A.

Let Π be the projector onto V_λ.

Let $\Pi^\perp = \mathbb{1}_V - \Pi$

Then

$$A = \mathbb{1}_V A \mathbb{1}_V$$
$$= (\Pi + \Pi^\perp) A (\Pi + \Pi^\perp)$$
$$= \Pi A \Pi + \underbrace{\Pi^\perp A \Pi + \Pi A \Pi^\perp}_{\text{claim: this is } 0.} + \Pi^\perp A \Pi^\perp$$

Claim 1: $\Pi^\perp A \Pi = 0$:

$$\Pi^\perp A \underbrace{\Pi v}_{\text{in } V_\lambda} = \lambda \underbrace{\Pi^\perp \Pi}_{0} v = 0 \qquad \forall v \in V.$$

Claim 2: $\Pi A \Pi^\perp = 0$:

For $w \in V_\lambda$ we have

$$A A^+ w = A^+ A w = \lambda \underbrace{A^+ w}_{\text{Therefore in } V_\lambda}.$$

Then similar to claim 1 we can show

$$\Pi^\perp \overbrace{A^+ \underbrace{\Pi v}_{\text{in } V_\lambda}}^{\text{in } V_\lambda} = 0.$$

$\Pi^\perp A^+ \underbrace{\Pi v}_{\text{in } V_\lambda} = \lambda \underbrace{\Pi^\perp \Pi v}_{0} = 0.$

$$\Rightarrow \Pi^\perp A^+ \Pi = 0 \Rightarrow \Pi A \Pi^\perp = 0.$$

adjoint

Therefore $A = \Pi A \Pi + \Pi^\perp A \Pi^\perp$.

Claim 3: $\Pi^\perp A \Pi^\perp$ is normal:

First observe that

(A) $\Pi^\perp A = \Pi^\perp A (\Pi + \Pi^\perp) = \Pi^\perp A \Pi^\perp$

(B) $\Pi^\perp A^+ = \Pi^\perp A^+ (\Pi + \Pi^\perp) = \Pi^\perp A \Pi^\perp$.

Then

$$
\begin{aligned}
(\Pi^\perp A \Pi^\perp)(\Pi^\perp A^+ \Pi^\perp) &= (\Pi^\perp A \Pi^\perp) A^+ \Pi^\perp \\
&= \Pi^\perp A A^+ \Pi^\perp \\
&\overset{(A)}{=} \Pi^\perp A^+ A \Pi^\perp \\
&= (\Pi^\perp A^+ \Pi^\perp) A \Pi^\perp \\
&\overset{(B)}{=} (\Pi^\perp A \Pi^\perp)(\Pi^\perp A \Pi^\perp).
\end{aligned}
$$

Let $V_{\Pi^\perp} = \{ \Pi^\perp v : v \in V \}$.

Then $\Pi^\perp A \Pi^\perp \in L(V_{\Pi^\perp})$

where $\dim(V_{\Pi^\perp}) < \dim(V) = d$.

By induction $\Pi^\perp A \Pi^\perp$ is diagonalizable:

$$\Pi^\perp A \Pi^\perp = \sum_a \lambda_a u_a u_a^+$$

for some orthonormal basis $\{u_a\}_{a \in \Gamma}$ of $V_{\Pi^\perp}$.

Let $\{w_b\}_{b \in \Lambda}$ be an orthonormal basis for V_λ.

Then A is diagonal in the orthonormal basis

$$\{u_a, w_b\}_{\substack{a \in \Lambda \\ b \in \Gamma}}$$

of V.

□

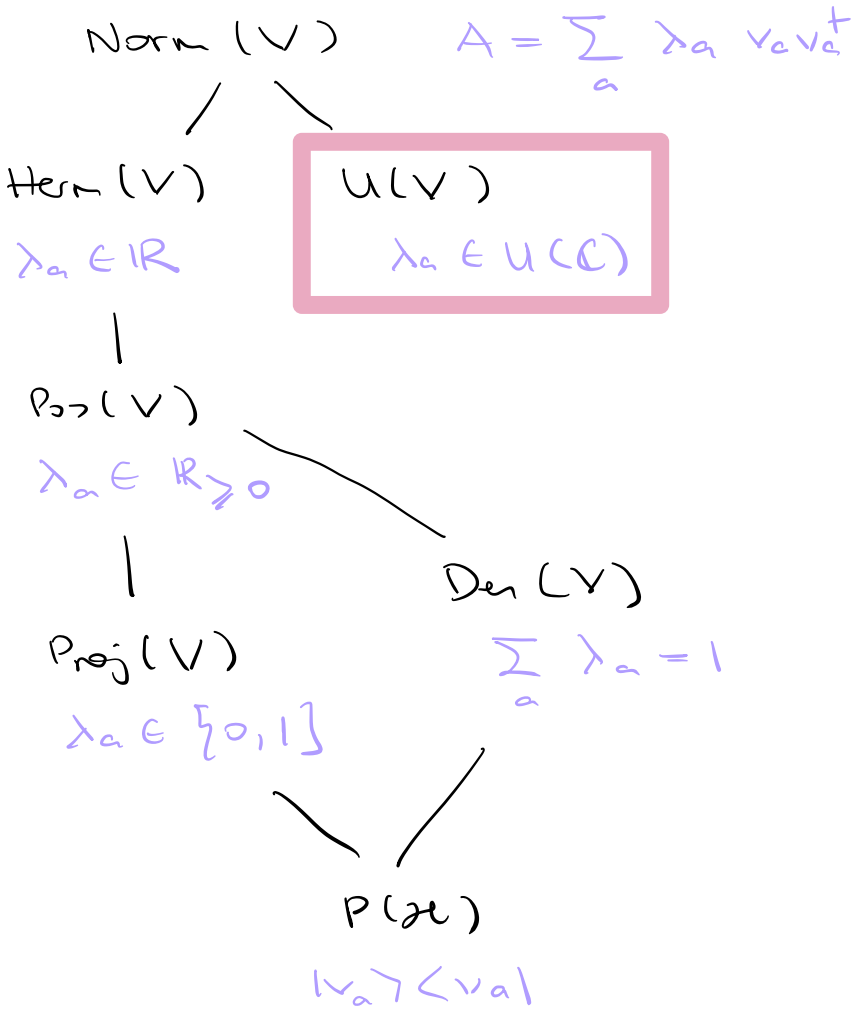
Let $\{\lambda_a\}_{a \in \Sigma} = \{\lambda_1, \dots, \lambda_m\}$ and

Π_{λ_i} projects onto V_{λ_i}.

The sets $\{\lambda_i\}$ and $\{\Pi_{\lambda_i}\}$ are unique and

$$A = \sum_{i=1}^{m} \lambda_i \Pi_{\lambda_i}.$$

Important operators:



U(V) acts on L(V):

$$U(V) \times L(V) \longrightarrow L(V)$$
$$(U, A) \longmapsto UAU^\dagger$$

If $A \in S$ then $UAU^\dagger \in S$ where $S = \text{Herm}(\mathcal{H}), U(V), \text{Pos}(V), \ldots$.

More on $\mathrm{Herm}(V)$ when $V = (\mathbb{C}^2)^{\otimes n}$:

Recall $\{ G_{i_1} \otimes \cdots \otimes G_{i_n} \}_{i_k = 0}^{= 3}$ is an orthonormal basis for $L(V)$.

Note that

$$(G_{i_1} \otimes \cdots \otimes G_{i_n})^\dagger = G_{i_1}^\dagger \otimes \cdots \otimes G_{i_n}^\dagger$$
$$= G_{i_1} \otimes \cdots \otimes G_{i_n}$$

i.e., $G_{i_1} \otimes \cdots \otimes G_{i_n}$ are Hermitian.

An operator $A \in L(V)$ where

$$A = \frac{1}{2^n} \sum_{i_1 \cdots i_n} \alpha_{i_1 \cdots i_n} G_{i_1} \otimes \cdots \otimes G_{i_n}$$

is Hermitian $\iff$ $\alpha_{i_1 \cdots i_n} \in \mathbb{R}$.

$\mathrm{Herm}(V)$ is a real inner product space:

$$\langle A, B \rangle = \mathrm{Tr}(AB).$$

Functions of normal operators

Let $f : \mathbb{C} \to \mathbb{C}$ be a function.

For a normal op. $A \in L(V)$ we define $f(A) \in L(V)$ by

$$f(A) = \sum_{i=1}^{m} f(\lambda_i)\, \Pi_{\lambda_i}.$$

Ex: $\exp(\alpha X) =$

$$= \exp\left(\alpha \left(|+\rangle\langle +| - |-\rangle\langle -|\right)\right)$$

$$= e^{\alpha} |+\rangle\langle +| + e^{-\alpha} |-\rangle\langle -|.$$

$$= e^{\alpha} \tfrac{1}{2} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \end{pmatrix} + e^{-\alpha} \tfrac{1}{2} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \begin{pmatrix} 1 & -1 \end{pmatrix}$$

$$= \frac{e^{\alpha}}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \frac{e^{-\alpha}}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

$$= \frac{1}{2} \begin{pmatrix} e^{\alpha} + e^{-\alpha} & e^{\alpha} - e^{-\alpha} \\ e^{\alpha} - e^{-\alpha} & e^{\alpha} + e^{-\alpha} \end{pmatrix} \neq \begin{pmatrix} 0 & e^{\alpha} \\ e^{\alpha} & 0 \end{pmatrix}$$

HW: Notation $v \cdot G = \sum_{i=1}^{3} v_i G_i$ $\quad v \in \mathbb{R}^3$ unit.

$$\exp(i\theta\, v \cdot G) = \cos\theta\, \mathbb{1} + i \sin\theta\, v \cdot G \qquad \theta \in \mathbb{R}.$$

HW: $\sqrt{X}$.

Simultaneous diagonalization → A & B commutes

Let A, B be Hermitian operators.

Then $AB = BA$ $\iff$ there exists an orthonormal basis $\{v_a\}_{a \in \Sigma}$ such that

$$A = \sum_a \lambda_a^A v_a v_a^\dagger \quad \& \quad B = \sum_a \lambda_a^B v_a v_a^\dagger.$$

proof: ($\Leftarrow$)

$$AB = \sum_a \lambda_a^A \lambda_a^B v_a v_a^\dagger = BA.$$

($\Rightarrow$)

Let $\{\lambda_1, \dots, \lambda_n\}$ denote distinct eigenvalues of A.

Let V_{λ_i} eigenspace corresponding to λ_i.

Key observation:

$$v \in V_{\lambda_i} \implies Bv_i \in V_{\lambda_i}:$$

$$A(Bv_i) = BAv_i = \lambda_i (Bv_i).$$

That is B is a Hermitian operator acting on V_{λ_i}.

Let $\{v_{ij}\}_{j=1}^n$ be an orthonormal basis of eigenvectors of B:

$$B v_{ij} = \lambda_{ij} v_{ij}.$$

$\{v_{ij}\}_{i,j}$ diagonalizes A & B ∎

Ex $(X \otimes X)(Z \otimes Z) = (Z \otimes Z)(X \otimes X)$

$Z \otimes Z$ is diagonal in $\{|ab\rangle\}_{a,b}$.

$V_1 = \text{Span}\{|00\rangle, |11\rangle\}$

Note that

$X \otimes X \; |00\rangle = |11\rangle$

Therefore $\left\{ \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \frac{|00\rangle - |11\rangle}{\sqrt{2}} \right\}$

is orthonormal basis of eig. vectors.

$V_{-1} = \text{Span}\{|01\rangle, |10\rangle\}$

$X \otimes X \; |01\rangle = |10\rangle$

$\left\{ \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \frac{|01\rangle - |10\rangle}{\sqrt{2}} \right\}$

Thus

$\left\{ \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \frac{|01\rangle - |10\rangle}{\sqrt{2}} \right\}$

diagonalizes both operators.

Polar decomposition

Let $A \in L(V)$. Then exists $U \in U(V)$ & $J \in Pos(V)$ such that

$$A = UJ.$$

If A is invertible then U is unique.

proof: let $J = \sqrt{A^+A}$: makes sense since $A^+A \in Pos(V)$

$$J = \sum_{i=1}^{n} \lambda_i \, v_i \qquad \lambda_i \in \mathbb{R}_{\geq 0}.$$

For $\lambda_i \neq 0$ define

$$w_i = \frac{1}{\lambda_i} A v_i.$$

Then

$$\begin{aligned} \langle w_j, w_i \rangle &= \left\langle \frac{1}{\lambda_j} A v_j, \frac{1}{\lambda_i} A v_i \right\rangle \\ &= \frac{1}{\lambda_i \lambda_j} \langle \underbrace{A^+A}_{J^2} v_j, v_i \rangle \\ &= \frac{1}{\lambda_i \lambda_j} \langle J v_j, J v_i \rangle \\ &= \frac{\lambda_i \lambda_j}{\lambda_i \lambda_j} \langle v_j, v_i \rangle = \delta_{ij}. \end{aligned}$$

Using Gram-Schmidt we can extend to an orthonormal basis $\{w_i\}_{i=1}^{n}$.

Define a unitary operator

$$U = \sum_{i=1}^{n} w_i v_i^t .$$

Claim: $A = UJ$:

For $\lambda_i \neq 0$:

$$UJ v_i = \lambda_i \sum_k w_k v_k^t v_i$$
$$= \lambda_i w_i$$
$$= A v_i .$$

For $\lambda_i = 0$, $UJ v_i = 0$.

Also $Av_i = 0$:

$$\| Av_i \|^2 = \langle Av_i , Av_i \rangle$$
$$= \langle A^t A v_i , v_i \rangle$$
$$= \langle J^2 v_i , v_i \rangle$$
$$= 0 .$$

Finally assume A is invertible:

$$0 \neq \det(A) = \det(UJ)$$
$$= \det(U) \underbrace{\det(J)}_{\neq 0}$$

$\Rightarrow$ J is invertible: $A = UJ$

$\Rightarrow$ $U = AJ^{-1}$ ∎

Singular value decomposition

Let $A \in L(\mathbb{C}^\Sigma)$.

Then there exists unitary matrices U & V, a diagonal D with nonnegative entries:

$$A = U D V.$$

Diagonal entries of D are called the singular values of A.

proof: By polar decomposition:

$$\begin{aligned} A &= W J && W \text{ unitary} \\ &= \underbrace{W T}_{U} D \underbrace{T^+}_{V} && T \text{ unitary} \end{aligned}$$

□

HW $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$

$$J = \sqrt{A^+ A} = \sqrt{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}}$$

$$= \sqrt{\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}}$$

$$U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \underbrace{\begin{pmatrix} \sqrt{2} & 1 \\ 1 & 1 \end{pmatrix}^{-1}}_{\frac{1}{\sqrt{2}-1}\begin{pmatrix} 1 & -1 \\ -1 & \sqrt{2} \end{pmatrix}} = \frac{1}{\sqrt{2}-1}\begin{pmatrix} 1 & -1 \\ 0 & \sqrt{2}-1 \end{pmatrix}$$