

Schmidt decomposition

$A \in \mathbb{R}^{n \times m}$ $n > m$ $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}$ $n \times m$ rank m
 $(1) \quad Y = \sum_{j=1}^m \alpha_j (e_j \otimes f_j)$ $n \times m$ $A \in \mathbb{R}^{n \times m}$ $U \in \mathbb{R}^{n \times n}$ $V \in \mathbb{R}^{m \times m}$

$A \in \mathbb{R}^{n \times m}$ $n > m$ $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}$ $n \times m$ rank m
 $A = \sum_{j=1}^m \alpha_j (e_j \otimes f_j)$ $n \times m$
 $Y = \sum_{j=1}^m \lambda_j (v_j \otimes w_j)$ $n \times m$

$\lambda_j \geq 0, \lambda_j \in \mathbb{R}^+$ $n > m$

$n > m$ $m = \dim A$, $n = \dim A$ $n > m$

$(1) \quad \alpha_j$ $M = \begin{pmatrix} \alpha_{ij} \end{pmatrix}_{n \times m}$ $n \times m$

$U_{n \times n} \rightarrow$ orthogonal $D \in \mathbb{R}^{n \times n}$ $V_{m \times m} \rightarrow$ orthogonal

$D = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_m \\ & & & 0 \end{pmatrix}_{n \times m}$

$M = UDV^T$

$\alpha_{ij} = (M)_{ij} = \sum_{k=1}^m \lambda_k (e_i \cdot u_k) \cdot (v_k^T \cdot f_j) = \sum_{k=1}^m \lambda_k u_{ik} v_{kj}$

$\sum_{j=1}^m \alpha_{ij} e_i \otimes f_j = \sum_{k=1}^m \lambda_k \sum_{i=1}^n u_{ik} \cdot \sum_{j=1}^m v_{kj} \cdot (e_i \otimes f_j)$

$= \sum_{k=1}^m \lambda_k \left(\sum_{i=1}^n u_{ik} e_i \right) \left(\sum_{j=1}^m v_{kj} f_j \right) = \sum_{k=1}^m \lambda_k (u_k \otimes v_k)$

$$= \sum_{k=1}^m \lambda_k \cdot \underbrace{\sum_{i=1}^n u_{ik} e_i}_{\alpha_k = |\alpha\rangle} \otimes \underbrace{\sum_{j=1}^m v_{kj} f_j}_{\beta_k = |\beta\rangle}$$

$$\begin{aligned} \langle \alpha_k | \alpha_l \rangle &= \left(\sum_{i=1}^n u_{ik} e_i \right)^\dagger \sum_{j=1}^n u_{jl} e_j \\ &= \sum_{i,j} \overline{u_{ik}} u_{jl} \underbrace{e_i^\dagger e_j}_{\delta_{ij}} = \sum_{i=1}^n \overline{u_{ik}} u_{il} = \delta_{kl} \end{aligned}$$

$\sum_{i=1}^n \overline{u_{ik}} u_{il} = \delta_{kl}$
 $\{ \beta_k \} \quad \{ \tilde{\beta}_k \}$

$$\begin{aligned} T_D(|\psi\rangle) &= \sum_{i,j} u_{ij} |i\rangle \otimes |j\rangle \\ T_A(|\psi\rangle) &= \sum_{i,j} v_{ij} |i\rangle \otimes |j\rangle \end{aligned}$$

... ..

$$\begin{aligned} H_A \otimes H_B & \text{ on } \mathcal{H} \otimes \mathcal{H} \quad (2n) \\ T_D(|\psi\rangle) & \text{ on } \mathcal{H} \otimes \mathcal{H} \quad \{ \alpha_i \} \\ T_A(|\psi\rangle) & \text{ on } \mathcal{H} \otimes \mathcal{H} \quad \{ \beta_j \} \end{aligned}$$

$$\psi = \sum_i x_i |\alpha_i\rangle \otimes |\beta_i\rangle$$

Def. commitment

G

אפשר לומר $A \rightarrow B$ אם A אז B

אפשר לומר $B \rightarrow A$ אם B אז A

אפשר לומר AB אם A ואז B

אפשר לומר $A \rightarrow B$ אם A אז B

אפשר לומר A אם A אז A

אפשר

אפשר לומר $A \rightarrow B$ אם A אז B (1)

אפשר לומר B אם B אז B

אפשר לומר A

אפשר לומר $A \rightarrow B$ אם A אז B (2)

אפשר לומר $A \rightarrow B$ אם A אז B

אפשר לומר A אם A אז A

(BB84) מיון מדידות

Commitment

$$S_0 = \{|0\rangle, |1\rangle\}$$

$$S_1 = \{|+\rangle, |-\rangle\}$$

בה סדרה S_a נשלח N קוביטות. כל קוביטה i נשלחת באופן אקראי A או B .

Reveal

$\forall i$ אנו יודעים את S_{a_i} ואת S_{b_i} .
אם $S_{a_i} = S_{b_i}$ אז הקוביטה i היא חלק מהקוד.

אם $S_{a_i} \neq S_{b_i}$ אז הקוביטה i היא חלק מהשערור.

$$P_1 = \frac{1}{2} \left[\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \right] \quad P_0 = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$= \frac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

! מספר הקוביטות N

אם $S_{a_i} = S_{b_i}$ אז הקוביטה i היא חלק מהקוד.

? 7^{10}

$R_A \otimes R_B$ א תוצאות ψ, ϕ ב"ע ! בדיק

$$P = T_B(N \otimes \psi) = T_B(\psi \otimes \phi) \quad \text{ע"ש}$$

R_B א U - הפירוק הדיאגנלי העיקרי
 $(I \otimes U)\phi = \psi \quad \text{ע"ש}$

פ.ל. ה. ה. $\sum \alpha_i$ ו... הקשר

$$\begin{matrix} \sum \beta_j & 0 \\ \sum \gamma_j & 1 \end{matrix}$$

ע"ש

$$\psi = \sum \lambda_i | \alpha_i \rangle \otimes | \beta_i \rangle$$

$$\phi = \sum \lambda_i | \alpha_i \rangle \otimes | \gamma_i \rangle$$

אם β_i ו γ_i קשורים זה לזה אז $\beta_i = \gamma_i$ ו...
 ב"ע β_i ו γ_i הם בסיס

b.c. הקשרים בין ה... הקשר

$$T_B P_0 = T_B P_1 \quad \text{ל"ע}$$

ψ ו ϕ הם תוצאות של הפירוק הדיאגנלי העיקרי של B ו...
 הפירוק הדיאגנלי העיקרי של B הוא...

PS1/2 1/2/20

$$(1) \quad \sum [(\rightarrow + \leftarrow)] = \frac{1}{2} [(\rightarrow + \leftarrow)] \quad \text{for } A$$

for (Had to be) $\tau_4 - \tau_5$ 0 1 0 1

Fidelity

\mathcal{H} is dim ρ_0, ρ_1 (D) 553C2

$$F(\rho_0, \rho_1) \equiv \sup_{\substack{\psi_0 \in \text{supp } \rho_0 \\ \psi_1 \in \text{supp } \rho_1}} |\langle \psi_0 | \psi_1 \rangle|^2$$

$\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ and ρ_0, ρ_1 is sup in \mathcal{H}
 $\rho_0 = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ and $\rho_1 = \sum_j q_j |\phi_j\rangle\langle\phi_j|$
 $\text{Tr}_B |\psi_i\rangle\langle\psi_i| = \rho_{0i}$ \Rightarrow

$$\text{Tr}_B |\phi_j\rangle\langle\phi_j| = \rho_{1j}$$

ρ_0, ρ_1 is sup in \mathcal{H} 553C2
 $\text{dim}(\mathcal{H}_A) \leq \text{dim}(\mathcal{H}_B)$

$\rho_0 = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ and $\rho_1 = \sum_j q_j |\phi_j\rangle\langle\phi_j|$ 553C2
 $|\langle \psi_i | \phi_j \rangle|^2 = F(\rho_{0i}, \rho_{1j})$ \Rightarrow

$\rho_0 \otimes \rho_1 = \sum_{i,j} p_i q_j |\psi_i\rangle\langle\psi_i| \otimes |\phi_j\rangle\langle\phi_j|$ 553C2

$$\text{Tr}_B (|\psi_i\rangle\langle\psi_i| \otimes |\phi_j\rangle\langle\phi_j|) = |\langle \psi_i | \phi_j \rangle|^2$$

$(I \otimes U) \tilde{\psi}_0 \rightarrow \psi_0$ \Rightarrow \mathcal{H}_B is ρ_{0i} and ρ_{1j}
 $\psi_1 = (I \otimes U) \tilde{\psi}_1$ 553C2

$$\text{Tr}_B (|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|) = \rho_{0i} = \text{Tr}_B (|\tilde{\psi}_j\rangle\langle\tilde{\psi}_j|) = \rho_{1j}$$

$$\langle \psi_i | \psi_j \rangle = \langle (I \otimes U) \tilde{\psi}_i | (I \otimes U) \tilde{\psi}_j \rangle = \langle \tilde{\psi}_i | \tilde{\psi}_j \rangle = F(\rho_{0i}, \rho_{1j})$$

553C2

$$F(\rho_0, \rho_1) = \left[\|\sqrt{\rho_0} \cdot \sqrt{\rho_1}\|_{tr} \right]^2$$

(Uhlmann '70s) Geel

Geel (2000) $F(\rho, \rho) = F(\rho, \rho) = 1$, $0 \leq F(\rho, \rho) \leq 1$, ρ_0, ρ_1 ρ, ρ 1. Geel
 $F(\rho, \rho) = 1$ 2

$$F(\rho, \sigma) = |\langle \psi | \sigma | \psi \rangle| \quad \rho = |\psi\rangle\langle\psi| \quad \rho \neq \sigma \quad 3$$

$$F(\rho_0, \rho_1) = |\langle \psi_0 | \psi_1 \rangle|^2 \quad \rho_0 = |\psi_0\rangle\langle\psi_0|, \quad \rho_1 = |\psi_1\rangle\langle\psi_1| \quad \rho \neq \sigma \quad 4$$

$$F(\rho, \sigma) = \left[\|\sqrt{\rho} \sqrt{\sigma}\|_{tr} \right]^2 = \left[\text{Tr} \sqrt{\underbrace{\rho}_{A} \underbrace{\sqrt{\sigma} \sqrt{\rho}}_{A^*}} \right]^2$$

$$= \left[\text{Tr} \sqrt{|\psi\rangle\langle\psi| \underbrace{\sigma}_{\text{norm}} |\psi\rangle\langle\psi|} \right]^2 = |\langle \psi | \sigma | \psi \rangle| \cdot \left[\text{Tr} \sqrt{|\psi\rangle\langle\psi|} \right]^2$$

$$= |\langle \psi | \sigma | \psi \rangle| = \langle \psi | \sigma | \psi \rangle$$

Fuchs & van de Graaf '99 : Geel

$$1 - \sqrt{F(\rho_0, \rho_1)} \leq \frac{1}{2} \|\rho_0 - \rho_1\|_{tr} \leq \sqrt{1 - F(\rho_0, \rho_1)}$$

:- app. CB

Method - P, q b/s

$$F(P, Q) = F\left(\underbrace{\sum P_i |i\rangle\langle i|}_{P_1}, \underbrace{\sum Q_i |i\rangle\langle i|}_{P_2}\right)$$

$$\hat{=} \|\sqrt{P_1} \sqrt{P_2}\| = \text{Tr}(\sqrt{P_1 P_2})^2 = \left[\sum \sqrt{P_i Q_i}\right]^2$$

soln P, Q

P1 P2 dm P1, P2 SC : Gen

$$\|U A U^\dagger\|_{tr} = \|A\|_{tr}$$

$$F(P_1, P_2) = F(U P_1 U^\dagger, U P_2 U^\dagger)$$

1
10/0
P1
K.C.T

$$\|P_1 - P_2\|_{tr} = \max_{P \in E_m} |E(P) - E(P_2)|$$

2
sub miss
K.P.P.P
P.P.P.P
Gen
fidelity

$$F(P_1, P_2) = \min_{P \in E} F(E(P), E(P_2))$$

(Gen + P.M) iff E - C.P.P. B.B.B.B.C SC 2

$$\|E P_1 - E P_2\|_{tr} \leq \|P_1 - P_2\|_{tr}$$

$$F(E P_1, E P_2) \geq F(P_1, P_2)$$

$$F\left(\sum P_i P_i, \sum Q_i \sigma_i\right) \geq \sum \sqrt{P_i Q_i} F(P_i, \sigma_i)$$

.4

P.M

(9)

(10)

col flipping

P = 7/8 / c

1. $A \in \mathbb{R}^{2 \times 2}$ \rightarrow rank $A = 1$
 $Y_A = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ \rightarrow basis
 B is a permutation matrix \rightarrow rank

2. A is a permutation matrix \rightarrow rank $A = 2$

3. B is a permutation matrix \rightarrow rank $B = 2$
 \rightarrow rank $AB = 2$

4. Y_A is a permutation matrix \rightarrow rank $Y_A = 2$
 $Y_A A$ is a permutation matrix \rightarrow rank $Y_A A = 2$

1. $P_0 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ \rightarrow rank $P_0 = 2$

2. $P_0 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ $P_1 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$

$P_0 - P_1 = \begin{bmatrix} 1 & 0 \\ 0 & -2 \end{bmatrix}$ $\|P_0 - P_1\|_F = 1$

$P_0 \perp P_1 \Rightarrow \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} = \frac{2}{\sqrt{2}} = \sqrt{2}$

$P_0 \perp P_1$ \rightarrow rank $P_0 + P_1 = 2$

\rightarrow rank $P_0 + P_1 = 2$

(1) (1) \rightarrow rank $P_0 + P_1 = 2$

... A, B, C

1. הצגת פונקציה

הפונקציה ψ_a היא וקטור אורטונורמלי ב- $L^2(\mathbb{R})$.
 הפונקציה ψ_{1-a} היא וקטור אורטונורמלי ב- $L^2(\mathbb{R})$.

$$P = [\langle \psi_a, \psi_a \rangle \quad \langle \psi_a, \psi_{1-a} \rangle] = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

\downarrow \downarrow \downarrow
 1 1 $\langle \psi_a, \psi_{1-a} \rangle = 0$
 (אורטונורמלי) (אורטונורמלי) (אורטונורמלי)

2. הצגת פונקציה

$$\psi = \frac{1}{\sqrt{3}} \left(\frac{1}{\sqrt{2}} \psi_a + \frac{1}{\sqrt{2}} \psi_b + \frac{2}{\sqrt{2}} \psi_c \right)$$

$$\psi = \frac{\psi_0 + \psi_1}{\|\psi_0 + \psi_1\|}$$

הצגת A

$$\psi = \frac{1}{\sqrt{2}} \left(\frac{1}{\sqrt{2}} \psi_a + \frac{1}{\sqrt{2}} \psi_b + \frac{2}{\sqrt{2}} \psi_c \right)$$

הפונקציה ψ היא וקטור אורטונורמלי ב- $L^2(\mathbb{R})$.

הפונקציה ψ היא וקטור אורטונורמלי ב- $L^2(\mathbb{R})$.

$$P = [\langle \psi, \psi_0 \rangle \quad \langle \psi, \psi_1 \rangle] = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \frac{3}{4}$$

$$\langle \psi, \psi_0 \rangle = \frac{1}{\sqrt{2}} \left(\frac{1}{\sqrt{2}} \langle \psi_a, \psi_0 \rangle + \frac{1}{\sqrt{2}} \langle \psi_b, \psi_0 \rangle + \frac{2}{\sqrt{2}} \langle \psi_c, \psi_0 \rangle \right) = \frac{3}{4}$$