

RSA $\sim 2^n$, $n \neq \text{bit}$
 $n \rightarrow \infty$
 шото = кохерентно coherent
 за суба на шотоа = декох. decoh.
 Теорие на измерване
 - квантови процесор.
 (квантови)
 възпр. квант. процесор
 Общавти системи \otimes

В това поле са снимки на дъските от дясната половина, на които са изписани потенциалните твърдения

Observables = $\{ \text{самопр. ел-ти } A \in \text{Mat}_N(\mathbb{C}) \mid (A=A^*) \}$
 $\rho: \text{Events} \xrightarrow{\text{Prob}} [0,1]$
 \cap
 Observables $\rightarrow \mathbb{R}$
 $\rho = \rho^* = \rho^2$
 $\rho(A) \equiv \langle A \rangle_\rho$; $\langle \rho \rangle_\rho = \text{Prob}_\rho(\rho)$
 (када.)
measurement - General
 $A = \text{Mat}_N(\mathbb{C})$

Проекц. измерване на функцията: $\rho \xrightarrow{Q=1} \rho'$
 $\rho'(P) (= \text{Prob}_\rho(P|Q)) = \frac{\rho(QPQ)}{\rho(Q)} = \frac{\text{Tr}(\rho QPQ)}{\text{Tr}(\rho Q)}$
 ax. \uparrow за квант. мис.
 Напомняне: $\rho(A) := \text{Tr}(\rho A)$
 наба. = $\langle A \rangle_\rho$ изг.
 Обз: $\hat{\rho} \mapsto \hat{\rho}' = \frac{Q \hat{\rho} Q}{\text{Tr}(\hat{\rho} Q)}$
 Обз: $\langle A \rangle_{\rho'} = \langle Q A Q \rangle_\rho / \rho(Q)$

Обз: Ако ρ е мисо ($\Leftrightarrow \hat{\rho} = |\psi\rangle\langle\psi|$)
 тогава ρ' е мисо ($\Leftrightarrow \hat{\rho}' = |\psi'\rangle\langle\psi'|$)
 $\psi' = Q\psi / \|Q\psi\|$

Знае ρ' е сводимо ?

Зад. PQP - не е проектор

$$(PQP)^* = P^* Q^* P^* = PQP$$

P_1, P_2 - функционират

($\Leftrightarrow P = P_1 + P_2$ е сводимо
и сводим $P = P_1 \vee P_2$)

$$\rho'(P_1 \vee P_2) = \rho'(P_1) + \rho'(P_2)$$

$$\rho'(P_1 + P_2) \stackrel{?}{=} \rho'(P_1) + \rho'(P_2)$$

$$\text{Зад. } \|Q\Psi\|^2 = \langle Q\Psi | Q\Psi \rangle = \langle \Psi | \underbrace{Q^* Q}_{\rho} \Psi \rangle = \langle \Psi | \rho \Psi \rangle = p(Q)$$

Проекция, изобразяваща на фон Койтман: $\rho \xrightarrow{Q=1} \rho'$

$$\rho'(P) (= \text{Prob}_\rho(P|Q)) = \frac{p(QPQ)}{p(Q)} \stackrel{\substack{\uparrow \\ \text{зв. квант. мис.}}}{=} \frac{\text{Tr}(\rho QPQ)}{\text{Tr}(\rho Q)}$$

Напомняне: $p(A) := \text{Tr}(\rho A)$
набл. = $\langle A \rangle_\rho$
чир.

$$\text{Зад. } \hat{\rho} \mapsto \hat{\rho}' = \frac{Q\hat{\rho}Q}{\text{Tr}(Q\hat{\rho}Q)}$$

$$\text{Сл. 1: } \langle A \rangle_{\rho'} = \langle Q A Q \rangle_\rho / p(Q)$$

Сл. 3: Ако ρ е чист ($\Leftrightarrow \hat{\rho} = |\Psi\rangle\langle\Psi|$)
тогава и ρ' е чист ($\Leftrightarrow \hat{\rho}' = |\Psi'\rangle\langle\Psi'|$)
 $\Psi' = Q\Psi / \|Q\Psi\|$

Док. на Сл. 3)

$$\hat{\rho}' \stackrel{?}{=} |\Psi'\rangle\langle\Psi'|$$

$$\text{Зв. } \Psi' = Q\Psi / \|Q\Psi\|$$

$$\text{По Сл. 2: } \hat{\rho}' = Q\hat{\rho}Q / \|Q\Psi\|^2$$

$$= Q |\Psi\rangle\langle\Psi| Q / \|Q\Psi\|^2$$

$$\underbrace{Q\Psi}_{\Psi} \underbrace{\langle\Psi|Q}_{\Psi^*} / \|Q\Psi\|^2$$

$$\underbrace{Q\Psi}_{\rho} \underbrace{(Q^*\Psi)^*}_{(Q\Psi)^*} / \|Q\Psi\|^2$$

$$= \Psi' \Psi'^* = |\Psi'\rangle\langle\Psi'|$$

Вероятност за преход:

$$\Psi \mapsto \Phi$$

$$|\langle\Psi|\Phi\rangle|^2$$

Сл. 4: Тим първене не

елементарно сводимо
кактова чист сводение:
чисто съв. колес свод. не
елем. сводение

Ком.: $\Psi = |\Psi\rangle$
 $\Psi^* = \langle\Psi|$

$\Rightarrow A|\Psi\rangle = |A\Psi\rangle$

до $\langle\Psi|A = \langle A^*\Psi|$
 $\Psi^*A \quad (A^*\Psi)^*$

$\rho \mapsto \rho' = \frac{Q|\Psi\rangle\langle\Psi|Q}{\|Q\Psi\|^2}$
 $\frac{|Q\Psi\rangle\langle Q\Psi|}{\|Q\Psi\|^2} = |\Psi'\rangle\langle\Psi'|$

Проекц. оператор на форткойма: $Q=1 \quad \rho \mapsto \rho'$

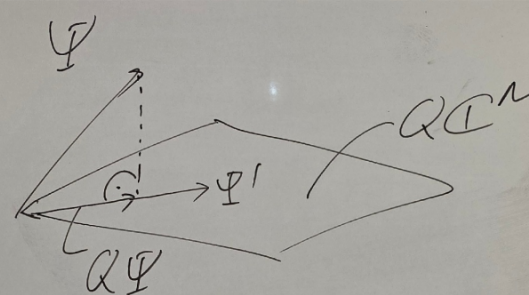
$\rho'(P) (= \text{Prob}_\rho(P|Q)) =$
 $\underset{\text{ох.}}{=} \frac{\rho(QPQ)}{\rho(Q)} \underset{\substack{\uparrow \\ \text{за кепр.} \\ \text{мис.}}}{=} \frac{\text{Tr}(\rho QPQ)}{\text{Tr}(\rho Q)}$

Напомине: $\rho(A) := \text{Tr}(\rho A)$
 Набл. = $\langle A \rangle_\rho$

Св. 2: $\hat{\rho} \mapsto \hat{\rho}' = \frac{Q\hat{\rho}Q}{\text{Tr}(\hat{\rho}Q)}$

Сл. 1: $\langle A \rangle_{\rho'} = \langle QAQ \rangle_\rho / \rho(Q)$

Сл. 3: Ако ρ е месо ($\Leftrightarrow \hat{\rho} = |\Psi\rangle\langle\Psi|$)
 тогава и ρ' е месо ($\Leftrightarrow \hat{\rho}' = |\Psi'\rangle\langle\Psi'|$)
 $\Psi' = Q\Psi / \|Q\Psi\|$



Класически случаи
 Q и P - комутират ($\Leftrightarrow PQ = QP$)

Тогава $QPQ = QP = PQ = QP$

$\rho'(P) = \frac{\rho(QPQ)}{\rho(Q)} = \text{Prob}_\rho(P|Q) = \frac{\text{Prob}_\rho(Q \wedge P)}{\text{Prob}_\rho(Q)}$

Вероятност за преход:

$\Psi \mapsto \Phi$

$|\langle\Psi|\Phi\rangle|^2$

Св. 4: Тим първене не
 елементарно събитие
 неговия месо състояние;
 чинно това, което съоб. на
 элем. събитие

$$\text{Prob}_\rho Q = |\langle \Psi | \Phi \rangle|^2$$

$$= \text{Prob}_{\hat{\rho}} P$$

$$\hat{\rho} \leftrightarrow \Phi, P \leftrightarrow \Psi$$

А какъв е преходът?

$$\hat{\rho} \xrightarrow{P} \hat{\rho}' = \hat{\eta}$$

$$\begin{matrix} \parallel & & \parallel \\ |\Psi\rangle\langle\Psi| & & |\Psi'\rangle\langle\Psi'| \end{matrix}$$

$$\Psi' = Q\Psi / \|Q\Psi\| = \text{const} \cdot \Phi$$

Проекц. оператор на фон Нойман: $Q=1$
 $\rho \mapsto \rho'$

$$\rho'(P) (= \text{Prob}_\rho(P|Q)) =$$

$$\underset{\text{ох.}}{=} \frac{\rho(QPQ)}{\rho(Q)} \underset{\substack{\uparrow \\ \text{за квант.} \\ \text{числ.}}}{=} \frac{\text{Tr}(\hat{\rho}QPQ)}{\text{Tr}(\hat{\rho}Q)}$$

Напомнене: $\rho(A) := \text{Tr}(\hat{\rho}A)$
 Набл. $= \langle A \rangle_\rho$
 числ.

Св.2: $\hat{\rho} \mapsto \hat{\rho}' = \frac{Q\hat{\rho}Q}{\text{Tr}(\hat{\rho}Q)}$

Св.1: $\langle A \rangle_{\rho'} = \langle QAQ \rangle_\rho / \rho(Q)$

Св.3: Ако ρ е чиста ($\Leftrightarrow \hat{\rho} = |\Psi\rangle\langle\Psi|$)
 тогава и ρ' е чиста ($\Leftrightarrow \hat{\rho}' = |\Psi'\rangle\langle\Psi'|$)

$$\Psi' = Q\Psi / \|Q\Psi\|$$

Док. на Св.4.

Изх. от Св.2:

$\hat{\rho}$ - е произв., но
 $Q = |\Phi\rangle\langle\Phi|$

$$\hat{\rho}' = \frac{Q\hat{\rho}Q}{\text{Tr} \hat{\rho} Q} =$$

$$= \frac{|\Phi\rangle\langle\Phi| \hat{\rho} |\Phi\rangle\langle\Phi|}{\text{Tr} \hat{\rho} |\Phi\rangle\langle\Phi|}$$

чисто
чисто

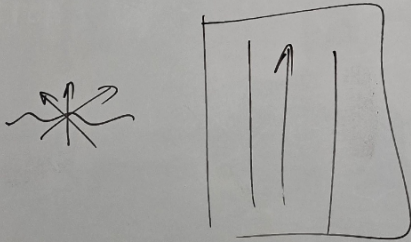
Вероятност за преход:

$$\Psi \mapsto \Phi$$

$$|\langle \Psi | \Phi \rangle|^2$$

Св.4: Тим първене не
 елементарно събитие
 настъпва само състояние;
 чиста съб., което съоб. на
 элем. събитие

$$= \frac{\langle \Phi | \hat{\rho} \Phi \rangle}{\langle \Phi | \hat{\rho} \Phi \rangle} |\Phi\rangle \langle \Phi|$$



Проекц. оператор на форт Койтър: $Q = | \Phi \rangle \langle \Phi |$

$$p'(P) (= \text{Prob}_p(P|Q)) =$$

$$\underset{\text{ох.}}{=} \frac{p(QPQ)}{p(Q)} \underset{\substack{\uparrow \\ \text{за кепр.} \\ \text{чис.}}}{=} \frac{\text{Tr}(\hat{\rho}QPQ)}{\text{Tr}(\hat{\rho}Q)}$$

Напомне: $p(A) := \text{Tr}(\hat{\rho}A)$
 Набл. $= \langle A \rangle_p$
 чис.

Св. 2: $\hat{\rho} \mapsto \hat{\rho}' = \frac{Q\hat{\rho}Q}{\text{Tr}(\hat{\rho}Q)}$

Св. 1: $\langle A \rangle_{p'} = \langle QAQ \rangle_p / p(Q)$

Св. 3: Ако p е чиста ($\Leftrightarrow \hat{\rho} = |\Psi\rangle \langle \Psi|$)
 тогава и p' е чиста ($\Leftrightarrow \hat{\rho}' = |\Psi'\rangle \langle \Psi'|$)
 $\Psi' = Q\Psi / \|Q\Psi\|$

$$\text{Prob}_p Q = |\langle \Psi | \Phi \rangle|^2$$

$$= \text{Prob}_{\hat{\eta}} P$$

$$\hat{\eta} \leftrightarrow \Phi, P \leftrightarrow \Psi$$

А какво е преход?

$$\hat{\rho} \xrightarrow{P} \hat{\rho}' = \hat{\eta}$$

" " " " " "

$$|\Psi\rangle \langle \Psi| \quad |\Psi'\rangle \langle \Psi'|$$

$$\Psi' = Q\Psi / \|Q\Psi\| = \text{const} \cdot \Phi$$

Вероятност за преход:


$$\Psi \mapsto \Phi$$

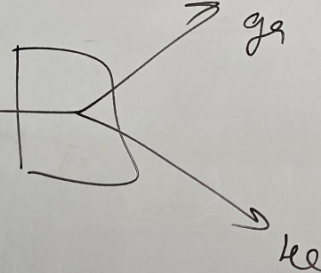
$$|\langle \Psi | \Phi \rangle|^2$$

Св. 4: Тим първене на

елементарно състояние
 неговия чиста състояние;
 чиста съба, което съоб. на
 элем. състояние

BB 84

→  g_1
 u_1

 g_2
 u_2

свогенератор
 делителен

g_1 "1" → u_1 "0"

g_1 "0" u_1 "1"

$\frac{1}{\sqrt{2}} e_1 \pm \frac{1}{\sqrt{2}} e_2 = f_{1,2}$

... 0 ... 1 ... 0 ...