Title: Quantum Theory - Lecture 14

Date: Sep 28, 2011 03:15 PM

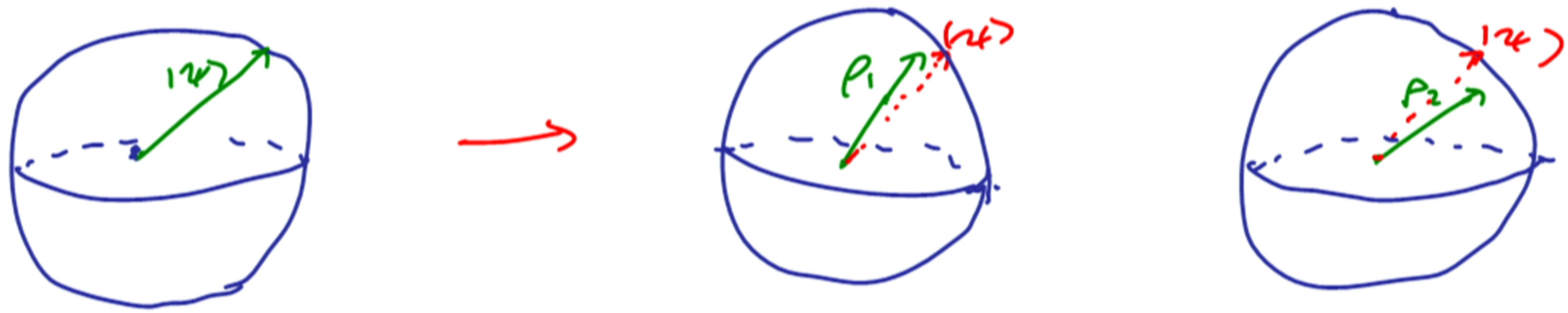
URL: http://pirsa.org/11090056

Abstract:

File Edit View Insert Actions Tools Help Reading View

Extending the no-cloning theorem II

What about **approximate** quantum cloning?



reduced density matrices

$$\mathrm{Tr}_2(\rho) = \rho_1 \quad , \quad \mathrm{Tr}_1(\rho) = \rho_2$$

ρ_1, ρ_2 close to $|\psi\rangle\langle\psi|$.

We need a measure of closeness: a natural one is the fidelity $\langle\psi|\rho_i|\psi\rangle$ which gives the probability of outcome "yes" if we measure $|\psi\rangle\langle\psi|$ on ρ_i.

89 / 131

$$|\psi\rangle |R_0\rangle |M\rangle \longrightarrow |\psi'\rangle$$

qubit qubit $\mathbb{C}^d$

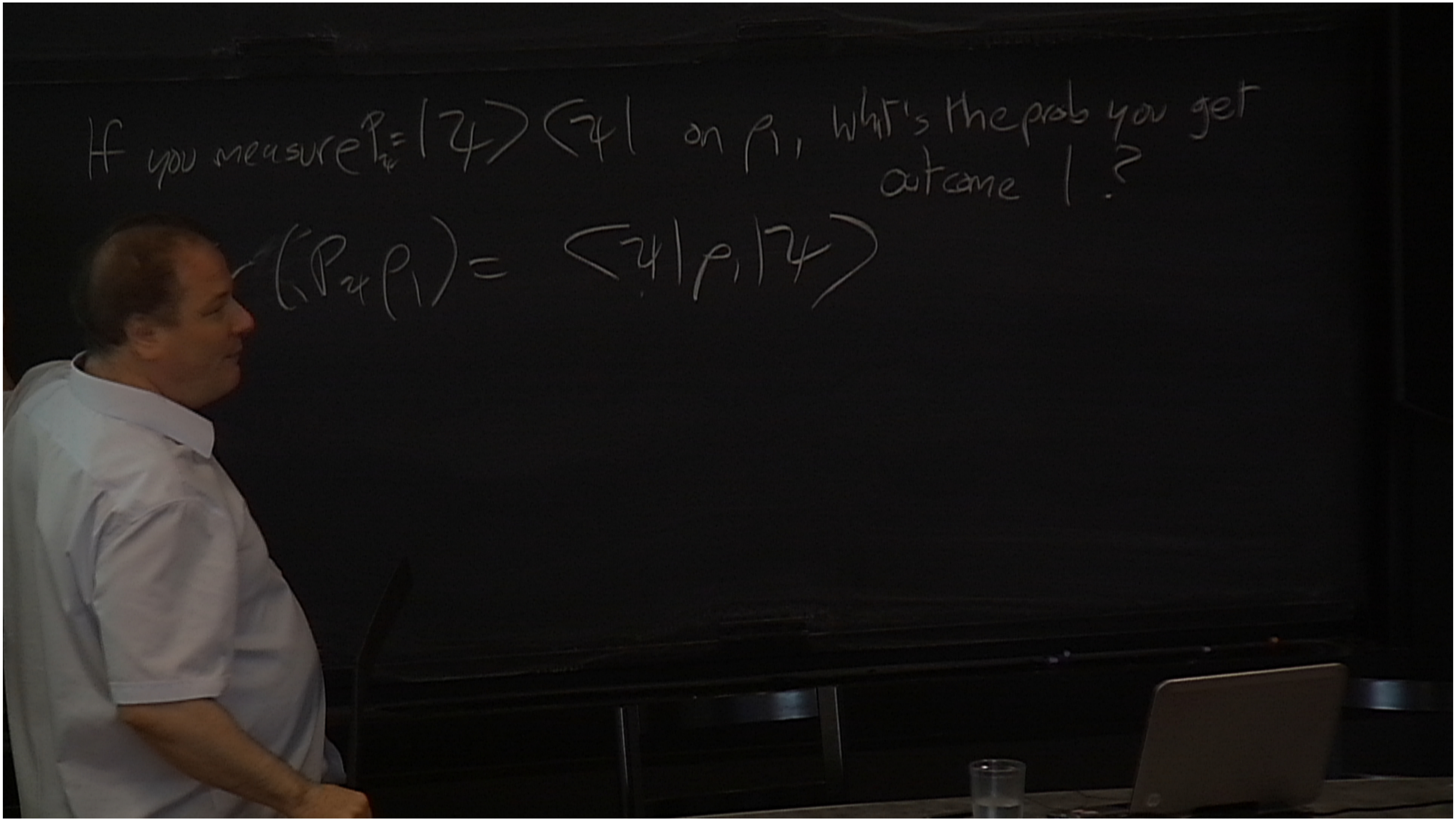
entangled state

$\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^d$

$H_1 \otimes H_2 \otimes H_M$

$$\rho_1 = \mathrm{Tr}_{H_2 \otimes H_M}\left(|\psi'\rangle\langle\psi'|\right)$$

$$\rho_2 = \mathrm{Tr}_{H_1 \otimes H_M}\left(|\psi'\rangle\langle\psi'|\right)$$


If you measure $P_\psi = |\psi\rangle\langle\psi|$ on ρ_1, what's the prob you get outcome 1?
$(P_\psi \rho_1) = \langle\psi|\rho_1|\psi\rangle$

Effectively:

reduced density matrices

$|\psi\rangle|R_0\rangle|M\rangle \to \underbrace{|\psi'\rangle}$

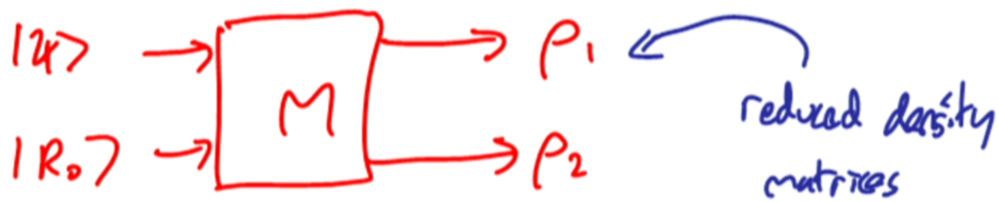
Full picture:

state of all 3, maybe entangled.

Could we arrange that $|\langle\psi|\rho_1|\psi\rangle| \geq 1-\varepsilon$, $|\langle\psi|\rho_2|\psi\rangle| \geq 1-\varepsilon$

for all possible inputs $|\psi\rangle$?

And can we arrange this for any $\varepsilon > 0$?



Could we arrange that $|\langle\psi|\rho_1|\psi\rangle| \geq 1-\varepsilon$, $|\langle\psi|\rho_2|\psi\rangle| \geq 1-\varepsilon$

for all possible inputs $|\psi\rangle$?

And can we arrange this for any $\varepsilon > 0$?

The no-signalling argument – remember Herbert's F.L.A.S.H. scheme – implies <u>not</u>. We can distinguish the mixtures $\frac{1}{2}(|\uparrow\rangle|\uparrow\rangle\langle\uparrow|\langle\uparrow| + |\downarrow\rangle|\downarrow\rangle\langle\downarrow|\langle\downarrow|)$

$\frac{1}{2}(|\rightarrow\rangle|\rightarrow\rangle\langle\rightarrow|\langle\rightarrow| + |\leftarrow\rangle|\leftarrow\rangle\langle\leftarrow|\langle\leftarrow|)$

So by continuity we must be able to distinguish mixtures of sufficiently close approximations.

If you measure $P_\psi = |\psi\rangle\langle\psi|$ on ρ_1, what's the prob you get outcome 1?

$$F = \mathrm{Tr}(P_\psi \rho_1) = \langle\psi|\rho_1|\psi\rangle$$

$$\sigma_1 = \frac{1}{2}\left(|\uparrow\rangle|\uparrow\rangle\langle\uparrow|\langle\uparrow| + |\downarrow\rangle|\downarrow\rangle\langle\downarrow|\langle\downarrow|\right)$$

$$\sigma_2 = \frac{1}{2}\left(|\rightarrow\rangle|\rightarrow\rangle\langle\rightarrow|\langle\rightarrow| + |\leftarrow\rangle|\leftarrow\rangle\langle\leftarrow|\langle\leftarrow|\right)$$

If you measure $P_\psi = |\psi\rangle\langle\psi|$ on ρ_1, what's the prob you get outcome 1?

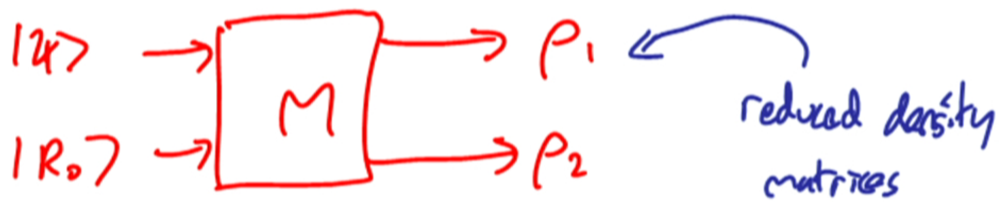
$$F = \mathrm{Tr}(P_\psi \rho_1) = \langle\psi|\rho_1|\psi\rangle$$

approx cloner produces

$$\sigma_1^\varepsilon \approx \sigma_1 = \frac{1}{2}\left(|\uparrow\rangle|\uparrow\rangle\langle\uparrow|\langle\uparrow| + |\downarrow\rangle|\downarrow\rangle\langle\downarrow|\langle\downarrow|\right)$$

$$\sigma_2^\varepsilon \approx \sigma_2 = \frac{1}{2}\left(|\rightarrow\rangle|\rightarrow\rangle\langle\rightarrow|\langle\rightarrow| + |\leftarrow\rangle|\leftarrow\rangle\langle\leftarrow|\langle\leftarrow|\right)$$

so $\sigma_1^\varepsilon \neq \sigma_2^\varepsilon$ for small ε. $\quad \sigma_1 \neq \sigma_2$.



Could we arrange that $|\langle\psi|\rho_1|\psi\rangle| \geq 1-\epsilon$, $|\langle\psi|\rho_2|\psi\rangle| \geq 1-\epsilon$

for all possible inputs $|\psi\rangle$?

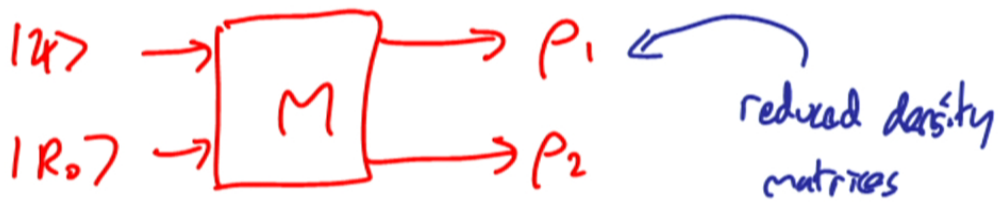
And can we arrange this for any $\epsilon > 0$?

The no-signalling argument – remember Herbert's F.L.A.S.H. scheme – implies <u>not</u>. We can distinguish the mixtures $\frac{1}{2}(|\uparrow\rangle|\uparrow\rangle\langle\uparrow|\langle\uparrow| + |\downarrow\rangle|\downarrow\rangle\langle\downarrow|\langle\downarrow|)$

$\frac{1}{2}(|\rightarrow\rangle|\rightarrow\rangle\langle\rightarrow|\langle\rightarrow| + |\leftarrow\rangle|\leftarrow\rangle\langle\leftarrow|\langle\leftarrow|)$

So by continuity we must be able to distinguish mixtures of sufficiently close approximations.

91 / 131



OK, we can't achieve $\langle\psi|\rho_1|\psi\rangle = \langle\psi|\rho_2|\psi\rangle = 1$.

Nor can we achieve $\langle\psi|\rho_1|\psi\rangle = \langle\psi|\rho_2|\psi\rangle = (1-\varepsilon)$

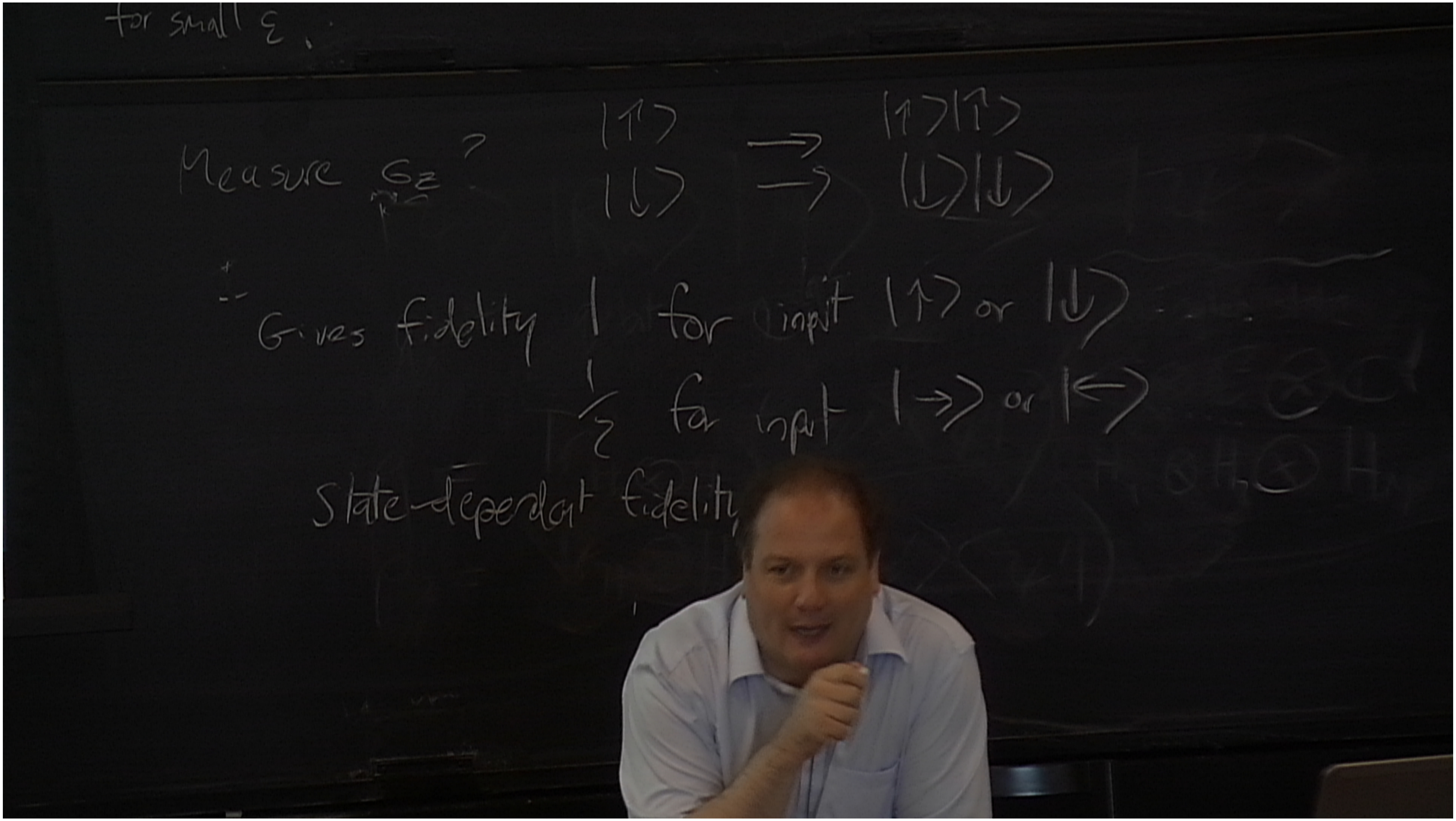
for arbitrary $\varepsilon > 0$.

Can we achieve anything that can sensibly be called approximate cloning?

$$\langle\psi|\rho_1|\psi\rangle = \langle\psi|\rho_2|\psi\rangle = \eta \quad \text{for } \eta > 0\,?$$

$$\eta > \tfrac{1}{2}\,?$$

$$\ldots$$


for small ε.
Measure σ_z?
$|\uparrow\rangle \longrightarrow |\uparrow\rangle|\uparrow\rangle$
$|\downarrow\rangle \longrightarrow |\downarrow\rangle|\downarrow\rangle$
Gives fidelity 1 for input $|\uparrow\rangle$ or $|\downarrow\rangle$
$\frac{1}{2}$ for input $|\rightarrow\rangle$ or $|\leftarrow\rangle$
State-dependent fidelity

File Edit View Insert Actions Tools Help Reading View

Simple (trivial?) cloning strategies ① random measurement.

Initial state $|\psi\rangle = \frac{1}{2}(1 + \underline{a}.\underline{\sigma}) \equiv |\underline{a}\rangle$

Choose random axis $\underline{b}$ for measurement of $(\underline{\sigma}.\underline{b})$

Make 2 copies of the outcome state $|+\underline{b}\rangle|\pm\underline{b}\rangle$ or $|-\underline{b}\rangle|-\underline{b}\rangle$

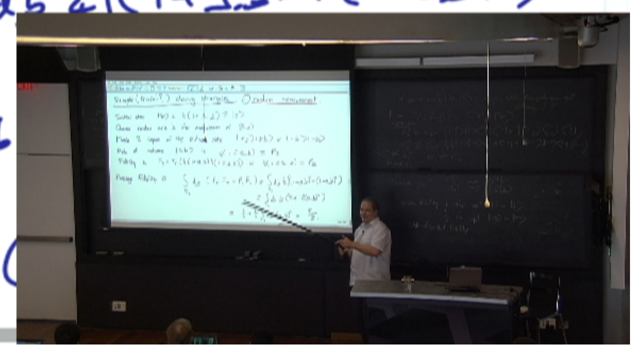
Prob of outcome $|\pm b\rangle$ is $\frac{1}{2}(1 \pm \underline{a}.\underline{b}) = P_\pm$

Fidelity is $F_\pm = \mathrm{Tr}\left(\frac{1}{2}(1+\underline{a}.\underline{\sigma})\frac{1}{2}(1 \pm \underline{b}.\underline{\sigma})\right) = \frac{1}{2}(1 \pm \underline{a}.\underline{b}) = P_\pm$

Average fidelity is $\int_{S_2} d\underline{b}\,(P_+F_+ + P_-F_-) = \int_{S_2} d\underline{b}\,\frac{1}{4}\left((1+\underline{a}.\underline{b})^2 + (1-\underline{a}.\underline{b})^2\right)$

$= \int_{S_2} d\underline{b}$

$= \frac{1}{2} + \frac{1}{2}\int_{S_2} d\underline{b}\,($



File Edit View Insert Actions Tools Help

Reading View

Simple (trivial) approximate cloning strategies: (2) add a random qubit

Initial state $|\psi\rangle = \frac{1}{2}(1 + \underline{a} \cdot \underline{\sigma})$

New state $|\psi'\rangle = \frac{1}{2}(1 + \underline{b} \cdot \underline{\sigma})$ (random $\underline{b}$)

"Flip a coin" to mix them: prepare $\frac{1}{\sqrt{2}}(|0\rangle|\psi\rangle|\psi'\rangle + |1\rangle|\psi'\rangle|\psi\rangle)$

$$\rho_1 = \rho_2 = \frac{1}{2}(|\psi\rangle\langle\psi| + |\psi'\rangle\langle\psi'|)$$

Averaged over $\underline{b}$, fidelity $\langle\psi|\rho_i|\psi\rangle = \frac{1}{2} + \frac{1}{4} = \frac{3}{4}$.

Could we do better? What is the max possible?

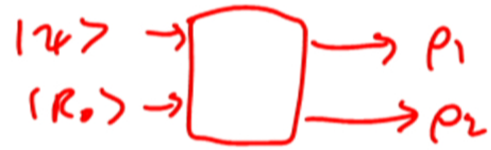
95 / 131

File Edit View Insert Actions Tools Help

Reading View

Firming up the no-signalling bound on approximate cloning (Gisin, 1998)

Let's focus on cloning qubits:



} reduced density matrices

We can assume symmetric cloning: $\langle\psi|\rho_1|\psi\rangle = \langle\psi|\rho_2|\psi\rangle$

(if not, randomize outputs).

We can also assume universal cloning: $\langle\psi|\rho_1|\psi\rangle = F$ independent of $|\psi\rangle$.

(For if we have a non-universal machine, we can rotate the input and output states by a randomly chosen U and U^{-1}, making a universal cloner.)

It can be shown this also makes the outputs rotationally invariant functions of the inputs.

$$\psi = \tfrac{1}{2}(1 + \underline{a}\cdot\underline{\sigma}) \Rightarrow \rho_i = \tfrac{1}{2}(1 + \eta\, \underline{a}\cdot\underline{\sigma})$$

where the fidelity $F = \tfrac{1}{2}(1+\eta)$

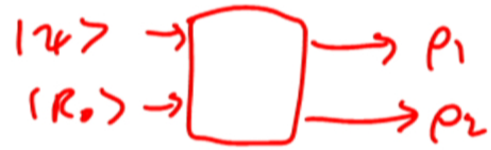
Bloch sphere "shrinking"

96 / 131

File Edit View Insert Actions Tools Help Reading View

Firming up the no-signalling bound on approximate cloning (Gisin, 1998)

Let's focus on cloning qubits:



} reduced density matrices

We can assume symmetric cloning: $\langle\psi|\rho_1|\psi\rangle = \langle\psi|\rho_2|\psi\rangle$

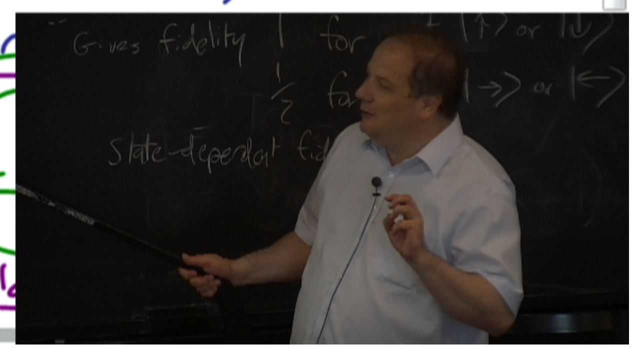
(if not, randomize outputs).

We can also assume universal cloning: $\langle\psi|\rho_i|\psi\rangle = F$ independant of $|\psi\rangle$.

(For if we have a non-universal machine, we can rotate the input and output states by a randomly chosen U and U^{-1}, making a universal cloner.)

It can be shown this also makes the outputs rotationally invariant

$$\boxed{\psi = \tfrac{1}{2}(1 + \underline{a}\cdot\underline{\sigma}) \Rightarrow \rho_i = \tfrac{1}{2}(1 + \eta\, \underline{a}\, \underline{\sigma}) \quad \text{where the fidelity } F = \tfrac{1}{2}(1+\eta)}$$



Firming up the no-signalling bound on approximate cloning (Gisin, 1998)

Let's focus on cloning qubits:

$|\psi\rangle \rightarrow \boxed{} \rightarrow \rho_1$
$|R_0\rangle \rightarrow \boxed{} \rightarrow \rho_2$

$\left.\begin{matrix}\rho_1\\ \rho_2\end{matrix}\right\}$ reduced density matrices

We can assume symmetric cloning: $\langle\psi|\rho_1|\psi\rangle = \langle\psi|\rho_2|\psi\rangle$

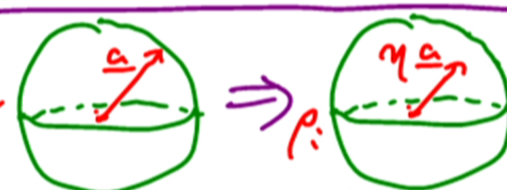
(if not, randomize outputs).

We can also assume universal cloning: $\langle\psi|\rho_1|\psi\rangle = F$ independant of $|\psi\rangle$.

(For if we have a non-universal machine, we can rotate the input and output states by a randomly chosen U and U^{-1}, making a universal cloner.)

It can be shown this also makes the outputs rotationally invariant functions of the inputs.

$$\boxed{\psi = \tfrac{1}{2}(1 + \underline{a}\cdot\underline{\sigma}) \Rightarrow \rho_i = \tfrac{1}{2}(1 + \eta\,\underline{a}\,\underline{\sigma})}$$

ψ  $\Rightarrow \rho_i$

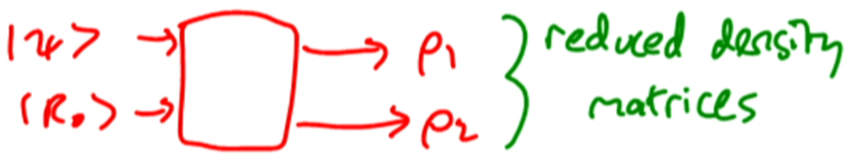
where the fidelity $F = \tfrac{1}{2}(1+\eta)$

Bloch sphere "shrinking"

File Edit View Insert Actions Tools Help

Reading View

Summary (1) We analyse machines for approximately cloning qubits:



(2) Symmetry arguments allow us to restrict attention to machines of a quite restricted type: $\rho_1 = \rho_2$ and ρ_i have the same Bloch vector as ψ, up to a scaling factor. The machine outputs are "noisy" copies of ψ: mixtures of ψ and the uniformly mixed state $\frac{1}{2}I$.

$$\psi = \tfrac{1}{2}(1 + \underline{a}.\underline{\sigma}) \Rightarrow \rho_i = \tfrac{1}{2}(1 + \eta\, \underline{a}\, \underline{\sigma})$$

where the fidelity $F = \frac{1}{2}(1+\eta)$

Bloch sphere "shrinking"

97 / 131

File Edit View Insert Actions Tools Help

Reading View

$$\rho_{out}(\underline{m}) = \tfrac{1}{4}\Big(I\otimes I + \eta\big(\underline{m}\cdot\underline{\sigma}\otimes I + I\otimes\underline{m}\cdot\underline{\sigma}\big) + \sum_{jk=1}^{3} t_{jk}\,\sigma_j\otimes\sigma_k\Big)$$

We can constrain the t_{jk} and η using (1) rotational invariance,

To see this explicitly, consider e.g. $\rho_{out}(\uparrow)$. Rotational invariance about z axis means $t_{xz} = t_{yz} = t_{zx} = t_{zy} = 0$, $t_{xx} = t_{yy}$, $t_{xy} = -t_{xy}$ (think of t as a 3-d tensor invariant under rotations about $\underline{z}$)

So
$$\rho_{out}(\uparrow) = \tfrac{1}{4}\Big(I\otimes I + \eta(\sigma_z\otimes I + I\otimes\sigma_z) + t_{xx}(\sigma_x\otimes\sigma_x + \sigma_y\otimes\sigma_y) + t_{zz}(\sigma_z\otimes\sigma_z) + t_{xy}(\sigma_x\otimes\sigma_y - \sigma_y\otimes\sigma_x)\Big).$$

and
$$\rho_{out}(\uparrow) + \rho_{out}(\downarrow) = \tfrac{1}{2}\Big(I\otimes I + t_{xx}(\sigma_x\otimes\sigma_x + \sigma_y\otimes\sigma_y) + t_{zz}(\sigma_z\otimes\sigma_z)\Big)$$

Next we consider (2) no-signalling: $\rho_{out}(\uparrow) + \rho_{out}(\downarrow) = \rho_{out}(\rightarrow) + \rho_{out}(\leftarrow)$

99 / 131

File Edit View Insert Actions Tools Help

Reading View

② non-signalling $\rho_{out}(\uparrow)+\rho_{out}(\downarrow)=\rho_{out}(\rightarrow)+\rho_{out}(\leftarrow)$ (*)

$$\rho_{out}(\uparrow)+\rho_{out}(\downarrow)=\tfrac{1}{2}\left(I\otimes I+t_{xx}(\sigma_x\otimes\sigma_x+\sigma_y\otimes\sigma_y)+t_{zz}(\sigma_z\otimes\sigma_z)\right)$$

and similarly $\rho_{out}(\rightarrow)+\rho_{out}(\leftarrow)=\tfrac{1}{2}\left(I\otimes I+t_{xx}(\sigma_y\otimes\sigma_y+\sigma_z\otimes\sigma_z)+t_{zz}(\sigma_x\otimes\sigma_x)\right)$

So (*) implies $t_{xx}=t_{zz}=t$

We now have

$$\rho_{out}(\uparrow)=\tfrac{1}{4}\Big(I\otimes I+m(\sigma_z\otimes I+I\otimes\sigma_z)+\overset{t}{\cancel{t_{xx}}}(\sigma_x\otimes\sigma_x+\sigma_y\otimes\sigma_y)$$
$$+\overset{t}{\cancel{t_{zz}}}(\sigma_z\otimes\sigma_z)+t_{xy}(\sigma_x\otimes\sigma_y-\sigma_y\otimes\sigma_x)\Big)$$

$$=\tfrac{1}{4}\Big(I\otimes I+m(\sigma_z\otimes I+I\otimes\sigma_z)+t(\sigma_x\otimes\sigma_x+\sigma_y\otimes\sigma_y+\sigma_z\otimes\sigma_z)$$
$$+t_{xy}(\sigma_x\otimes\sigma_y-\sigma_y\otimes\sigma_x)\Big)$$

Finally we consider ③ non-negativity – all eigenvalues ≥ 0

100 / 131

File Edit View Insert Actions Tools Help

Reading View

$$\rho_{out}(\uparrow) = \frac{1}{4}\Big(I \otimes I + \eta\,(\sigma_z \otimes I + I \otimes \sigma_z) + t\,(\sigma_x \otimes \sigma_x + \sigma_y \otimes \sigma_y + \sigma_z \otimes \sigma_z) + t_{xy}\,(\sigma_x \otimes \sigma_y - \sigma_y \otimes \sigma_x)\Big)$$

Finally we consider (3) non-negativity – all eigenvalues ≥ 0

$\rho_{out}(\uparrow)$ has eigenvalues

$$\frac{1}{4}(1 \pm 2\eta + t) \implies \eta \leq \frac{t+1}{2}$$

$$\frac{1}{4}\left(1 - t \pm 2(t^2 + t_{xy}^2)^{1/2}\right) \implies 2(t^2 + t_{xy}^2)^{1/2} \leq 1 - t$$

To maximize η we need to maximize t, which gives

$$t_{xy} = 0$$

$$t = \frac{1}{3}$$

$$\eta = \frac{2}{3}$$

$$F = \left(\frac{1+\eta}{2}\right) = \frac{5}{6}$$

QED

101 / 131

$|\psi\rangle \rightarrow \boxed{} \rightarrow \rho_1$
$|R_0\rangle \rightarrow \phantom{\boxed{X}} \rightarrow \rho_2$ } reduced density matrices

Bloch sphere shrinking

$$\psi = \tfrac{1}{2}(1 + \underline{a}\cdot\underline{\sigma}) \Rightarrow \rho_i = \tfrac{1}{2}(1 + \eta\,\underline{a}\,\underline{\sigma})$$

where the fidelity $\boxed{F = \tfrac{1}{2}(1+\eta) \leq 5/6}$

So, no-signalling gives us an upper bound : a cloning scheme cannot reliably produce 2 copies both with fidelity $> 5/6$.

Can we achieve this bound? Yes!! Buzek – Hillery (1996) gave an explicit construction of a fidelity $5/6$ universal cloner.

The Buzek-Hillery approximate cloning machine

a machine defined by just 1 qubit!

Let
$$|0\rangle|R_0\rangle|M_0\rangle \to \sqrt{\tfrac{2}{3}}\,|0\rangle|0\rangle|1\rangle - \sqrt{\tfrac{1}{3}}\,|\Psi^+\rangle|0\rangle$$
$$|1\rangle|R_0\rangle|M_0\rangle \to -\sqrt{\tfrac{2}{3}}\,|1\rangle|1\rangle|0\rangle + \sqrt{\tfrac{1}{3}}\,|\Psi^+\rangle|1\rangle$$

where $|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle + |1\rangle|0\rangle\right)$.

Then
$$(a|0\rangle + b|1\rangle)|R_0\rangle|M_0\rangle \to \sqrt{\tfrac{2}{3}}\,a|0\rangle|0\rangle|1\rangle + \sqrt{\tfrac{1}{3}}\,a|\Psi^+\rangle|0\rangle - \sqrt{\tfrac{2}{3}}\,b|1\rangle|1\rangle|0\rangle + \sqrt{\tfrac{1}{3}}\,b|\Psi^+\rangle|1\rangle$$

$$|\psi\rangle = a|0\rangle + b|1\rangle$$
$$|\psi^\perp\rangle = a^*|1\rangle - b^*|0\rangle$$

$$= \dots = \sqrt{\tfrac{2}{3}}\,(a|0\rangle + b|1\rangle)(a|0\rangle + b|1\rangle)(a^*|1\rangle - b^*|0\rangle) - \sqrt{\tfrac{1}{6}}\Big((a|0\rangle + b|1\rangle)(a^*|1\rangle - b^*|0\rangle) + (a^*|1\rangle - b^*|0\rangle)(a|0\rangle + b|1\rangle)\Big)(a|0\rangle + b|1\rangle)$$

$$= \sqrt{\tfrac{2}{3}}\,|\psi\rangle|\psi\rangle|\psi^\perp\rangle - \sqrt{\tfrac{1}{6}}\Big(\big(|\psi\rangle|\psi^\perp\rangle + |\psi^\perp\rangle|\psi\rangle\big)|\psi\rangle\Big)$$

So as promised
$$\langle\psi|\rho_1|\psi\rangle = \langle\psi|\rho_2|\psi\rangle = 5/6$$

File Edit View Insert Actions Tools Help Reading View

The Buzek-Hillery approximate cloning machine

a machine defined by just 1 qubit!

Let $|0\rangle|R_0\rangle|M_0\rangle \to \sqrt{\frac{2}{3}}\,|0\rangle|0\rangle|1\rangle - \sqrt{\frac{1}{3}}\,|\Psi^+\rangle|0\rangle$

$|1\rangle|R_0\rangle|M_0\rangle \to -\sqrt{\frac{2}{3}}\,|1\rangle|1\rangle|0\rangle + \sqrt{\frac{1}{3}}\,|\Psi^+\rangle|1\rangle$

where $|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle + |1\rangle|0\rangle\right).$

Then $(a|0\rangle + b|1\rangle)|R_0\rangle|M_0\rangle \to \sqrt{\frac{2}{3}}\,a|0\rangle|0\rangle|1\rangle + \sqrt{\frac{1}{3}}\,a|\Psi^+\rangle|0\rangle$

$- \sqrt{\frac{2}{3}}\,b|1\rangle|1\rangle|0\rangle + \sqrt{\frac{1}{3}}\,b|\Psi^+\rangle|1\rangle$

$\boxed{|\psi\rangle = a|0\rangle + b|1\rangle \quad |\psi^\perp\rangle = a^*|1\rangle - b^*|0\rangle}$

$= \dots = \sqrt{\frac{2}{3}}\,(a|0\rangle + b|1\rangle)(a|0\rangle + b|1\rangle)(a^*|1\rangle - b^*|0\rangle)$

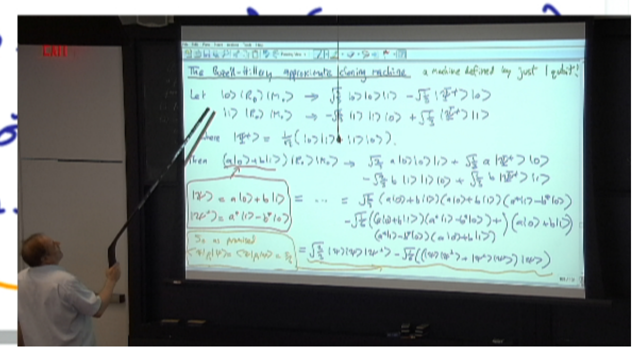
$-\sqrt{\frac{1}{6}}\Big((a|0\rangle + b|1\rangle)(a^*|1\rangle \ldots$

$(a^*|1\rangle - b^*|0\rangle)(a|0 \ldots$

So as promised

$\langle\psi|\rho_1|\psi\rangle = \langle\psi|\rho_2|\psi\rangle = 5/6$

$= \sqrt{\frac{2}{3}}\,|\psi\rangle|\psi\rangle|\psi^\perp\rangle - \sqrt{\frac{1}{6}}\Big(\big(|\psi\rangle|\psi^\perp \ldots$



File Edit View Insert Actions Tools Help

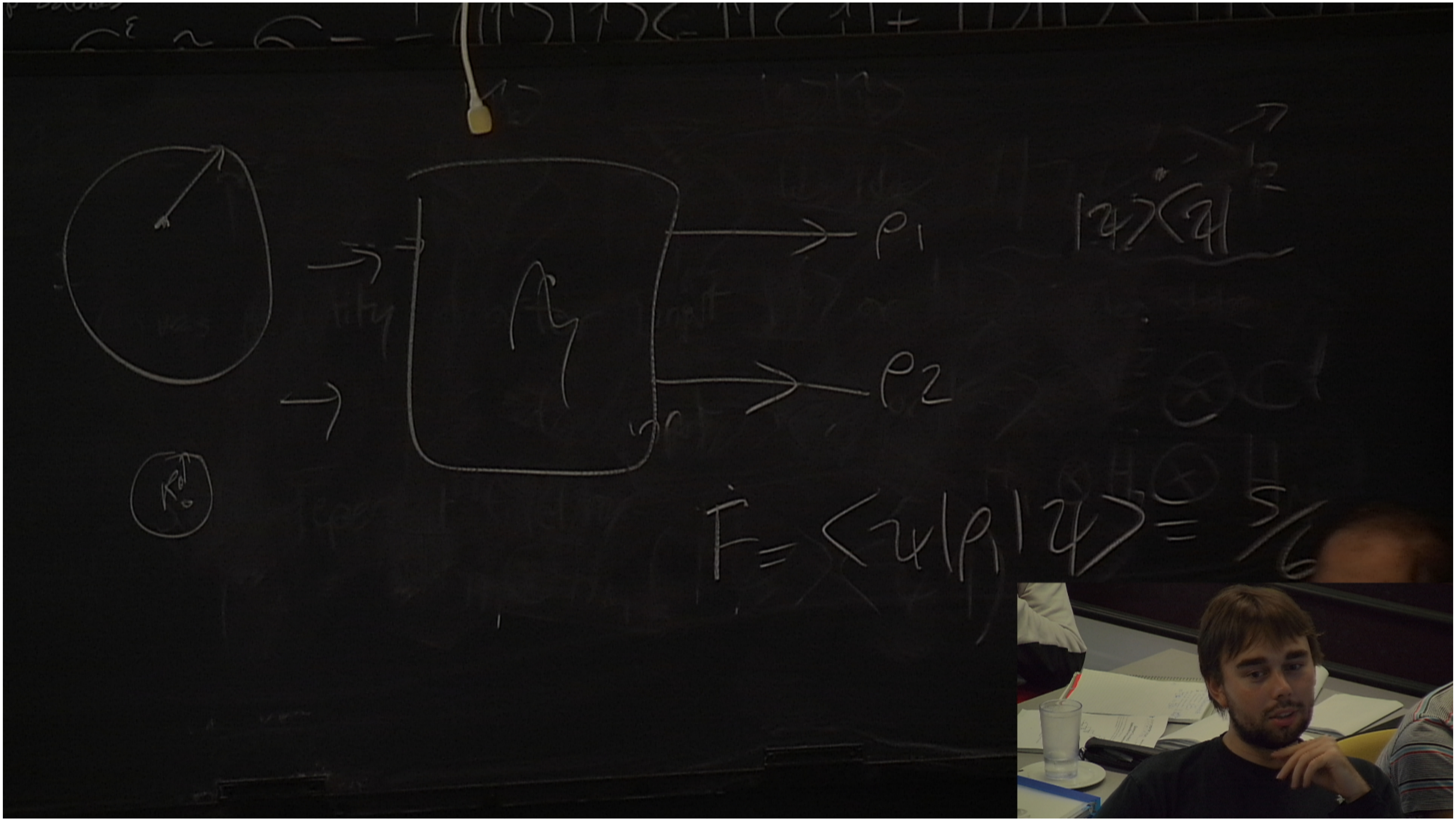
Reading View

Note that while the Buzek-Hillery optimal universal cloner is simple and elegant, and while it's satisfying that it achieves precisely the no-signalling bound, it's not that much better than the trivial add-a-random-qubit cloner ($F = 5/6$ compared to $F = 3/4$).

This turns out to be generally true: in higher dimensions, or $M \to N$ copy cloning, you can do a bit better than trivial strategies, but not much.

(Bad news if you're thinking of cloning as a way of "backing up" your quantum states. But good news if you want to ensure that other people can't copy them!)

105 / 131

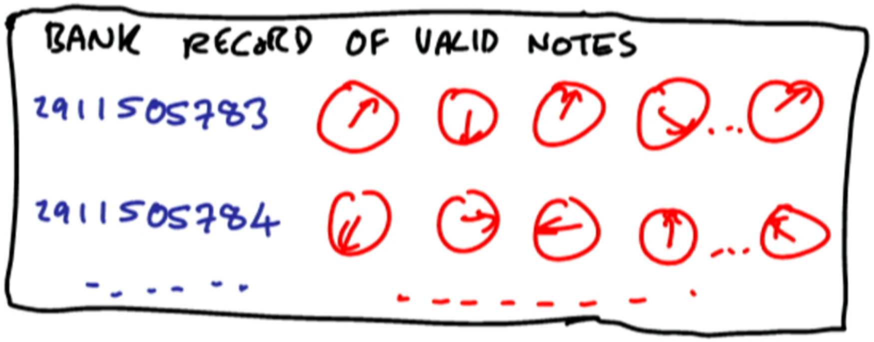

ρ1
ρ2
|ψ⟩⟨ψ|
F = ⟨ψ|ρ1|ψ⟩ = 5/6

Quantum Money (Wiesner c. 1970, unpublished till 1983)

Classical money is basically classical information: it is copiable (forgeable) with arbitrary precision. A sufficiently skilled forger can make any number of copies.

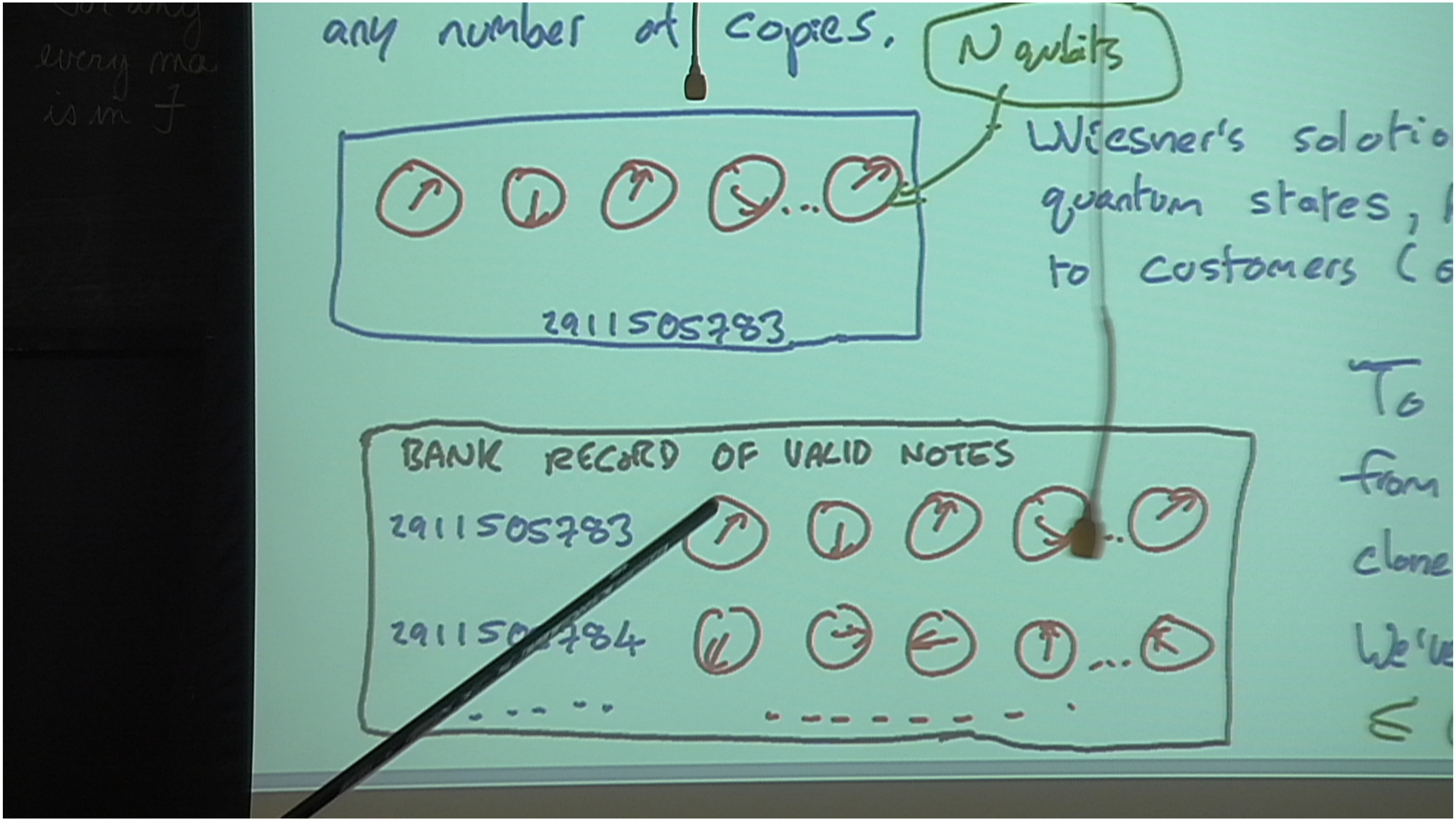
N qubits

Wiesner's solution: incorporate randomly chosen quantum states, known to the bank but not to customers (or forgers)



To create even two valid notes from one, the forger needs to try to clone N unknown qubits.

We've seen her success probability is $\leq (5/6)^N$. I.E. SECURE FOR LARGE N


any number of copies.
N qubits
Wiesner's solutio
quantum states,
to customers (
2911505783
BANK RECORD OF VALID NOTES
2911505783
To
from
clone