Quantum observations
talk 4

Vladimír Bužek
Research Center for Quantum Information, Bratislava, Slovakia

5 September 2012 **Sharif University of Technology, Tehran**

Quantum information: Distribution and manipulation

Bell Telephone & FLASH

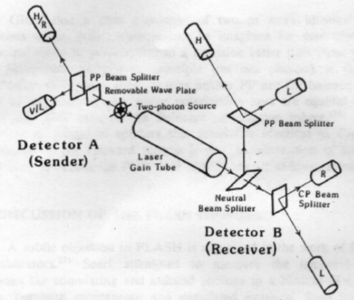


Fig. 1. The FLASH detection process. Photons in beam *B* (traveling to the right) are rendered either circularly unpolarized (CUP) or plane unpolarized (PUP) by positioning of the quarter wave plate in beam *A* (traveling to the left). Each *B* photon is amplified by a nonselective laser gain tube and the resulting isopolarized burst of light is examined for counting asymmetry in either the CP or PP channel.

Can quantum nonlocality of entangled states be used for super-luminal communication?

N.Herbert, *Found. Phys.* **12**, 1171 (1982)

Alphabet in Bell Telephone & Flash

- **Singlet states**

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|\psi\rangle_A |\psi^\perp\rangle_B - |\psi^\perp\rangle_A |\psi\rangle_B\right)$$

exhibits perfect quantum correlations for polarization measurement along orthogonal but *arbitrary* axes.

- **Alice and Bob have pair before any communication**

Alice might like to send a message to Bob. She performs a measurement on her particle in one of the two bases

$$\{|\uparrow\rangle, |\downarrow\rangle\} \text{ and } \{|\leftarrow\rangle, |\rightarrow\rangle\}$$

After Alice performs her measurement in one of the bases, say $\{|\uparrow\rangle, |\downarrow\rangle\}$

Then she can predict with certainty what Bob's result would be if he performs a measurement in the same basis.

$$\text{logical zero} = \text{basis } \{|\uparrow\rangle, |\downarrow\rangle\}$$
$$\text{logical one} = \text{basis } \{|\leftarrow\rangle, |\rightarrow\rangle\}$$

- Infinite (continuous) alphabet:

$$\{|\psi\rangle, |\psi^\perp\rangle\}$$

Question: Can we discriminate (reconstruct) quantum states based on results of measurements performed on a single quantum object?

Optimal reconstructions of qubits

- average fidelity of estimation

$$F = \frac{N+1}{N+2} = \frac{1}{2}\left[1 + \frac{N}{N+2}\right]$$

$$F = \frac{2}{3} = \frac{1}{2}\left(1 + \frac{1}{3}\right)$$

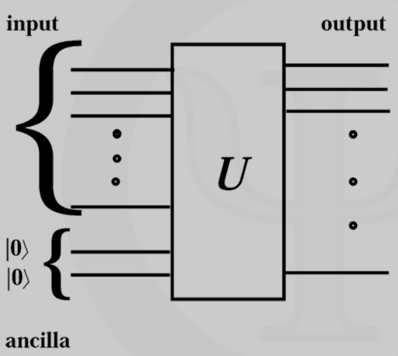
- Estimated density operator on average

$$\hat{\rho}_{est} = s\hat{\rho} + \frac{1-s}{2}\hat{I}; \qquad s = 2F - 1 = \frac{N}{N+2}$$

- Construction of optimal (& finite-dimensional) POVM's – maximize the fidelity *F*
- POVM via von Neumann projectors – Naimark theorem
- Optimal decoding of information
- Optimal preparation of quantum systems
- Recycling of q-information

S.Massar and S.Popescu, *Phys. Rev. Lett.* 74, 1259 (1995)
A.Latorre, P.Pascual, and R.Tarrach, *Phys. Rev. Lett.* 81, 1351 (1998)
R.Gill and S.Massar, *Phys. Rev. A* 61, 042312 (2000)
M.Hayashi, *Asymptotic Theory of Quantum Statistical Inference* (Academic Press, NY, 2005)

Naimark theorem



the optimal POVM can be physically realized via a quantum network and subsequent orthogonal measurement e.g. in the standard base

- number of auxiliary qbits is such that the space of all qbits with 2^q dimensions can accommodate $(N+1)^2$ orthogonal projectors

- the unitary transformation U reads:

$$|i\rangle \xrightarrow{U^\dagger} |\psi_i\rangle + \sum_{j=d+1}^{R} V_{ij}^* |\chi_j\rangle \qquad i=1,2,..R$$

$$|i\rangle \xrightarrow{U^\dagger} |i\rangle \qquad i=R+1,..\, 2^q$$

(for the meaning of symbols see the text)

Back to FLASH

- **Optimal Quantum Measurement:**

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

This does not allow for signaling – from a single shot measurement we are not able to discriminate between bases

$$\{|\uparrow\rangle, |\downarrow\rangle\} \text{ and } \{|\leftarrow\rangle, |\rightarrow\rangle\}$$

Herbert:

"a serious objection to FLASH concerns the noise… of the copying process"

- **Can we do better?**
- **Cloning quantum states?**

– active quantum detectors?

$$|\psi\rangle|0\rangle^{\otimes(N-1)} \to |\psi\rangle^{\otimes N}$$

$$F = \frac{N+1}{N+2}$$

N.Herbert, *Found. Phys.* **12**, 1171 (1982)

No-cloning Theorem

- Wigner 1961:

"the probability is zero for existence of self-reproducing states"

- Wootters & Zurek 1982:

"unkonwn pure states cannot be cloned perfectly"

- Condition for universal cloning

$$|\psi\rangle|0\rangle|S\rangle \xrightarrow{u} |\psi\rangle \otimes |\psi\rangle|S'\rangle$$
$$|\tilde{\psi}\rangle|0\rangle|S\rangle \xrightarrow{u} |\tilde{\psi}\rangle \otimes |\tilde{\psi}\rangle|S''\rangle$$

- Unitarity of the cloning operation:

$$\langle\tilde{\psi}|\psi\rangle = \left(\langle\tilde{\psi}|\psi\rangle\right)^2 \langle S'|S''\rangle$$

- $$\langle\tilde{\psi}|\psi\rangle = 0 \text{ or } \left|\langle\tilde{\psi}|\psi\rangle\right| = 1$$

Distinguishable states can be copied perfectly

E.Wigner, in The Logic of Personal Knowledge (The Free Press, 1961), p.231.
W.K.Wootters and W.H.Zurek, *Nature* **299**, 802 (1982).
H.Yuen, *Phys. Lett. A* **113**, 405 (1986)

Copying of unkown states?

- Mandel 1983:

$$H_I = g\sum_{s=1}^{2}\left[\left(\sigma_a^- \vec{\mu}_a + \sigma_b^- \vec{\mu}_b\right)\cdot \vec{\varepsilon}_s^{\,*} a_s^+ + h.c.\right]$$

Orthogonal transition dipole moments: $\vec{\mu}_x = |\mu|\vec{\varepsilon}_x$

Polarization vectors: $\vec{\varepsilon}_x$

Initial state $\left|1_{\vec{\varepsilon}_1}, 0_{\vec{\varepsilon}_2}\right\rangle$

$$\rho_{\vec{\varepsilon}_1,\vec{\varepsilon}_2} = \frac{2}{3}\left|2_{\vec{\varepsilon}_1}, 0_{\vec{\varepsilon}_2}\right\rangle\left\langle 2_{\vec{\varepsilon}_1}, 0_{\vec{\varepsilon}_2}\right| + \frac{1}{3}\left|1_{\vec{\varepsilon}_1}, 1_{\vec{\varepsilon}_2}\right\rangle\left\langle 1_{\vec{\varepsilon}_1}, 1_{\vec{\varepsilon}_2}\right|$$

L.Mandel, *Nature* **304**, 188 (1983)

- Stimulated vs spontaneous emission

Each "perfect clone" is accompanied by one randomly polarized photon

- Amplification & noise
- Optimal strategy

Universal quantum cloners

- Input: $|\psi\rangle$
- Outputs are identical $\rho_a^{(out)} = \rho_b^{(out)}$
- $F\left(\rho_x^{(out)};\rho_x^{(id)}\right) = \max\left\{F^{(U)}\left(\rho_x^{(out)};\rho_x^{(id)}\right);\forall U\right\}$

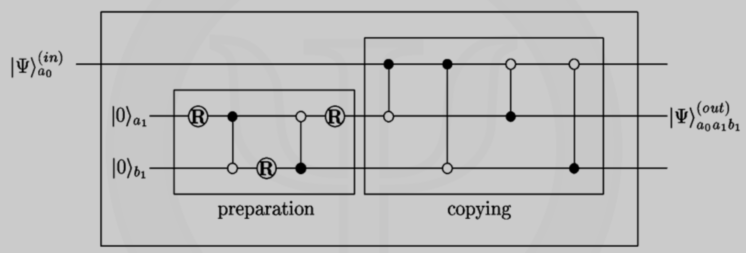
$$\boxed{|\psi\rangle_a |\Xi\rangle_{bc} \rightarrow \sqrt{\frac{2}{3}}|\psi,\psi\rangle_{ab}|\psi^\perp\rangle_c - \frac{1}{\sqrt{3}}\left|\{\psi^\perp,\psi\}\right\rangle_{ab}|\psi\rangle_c}$$

$$\left|\{\psi^\perp,\psi\}\right\rangle_{ab} = \left(|\psi\rangle_a|\psi^\perp\rangle_b + |\psi^\perp\rangle_a|\psi\rangle_b\right)/\sqrt{2}$$

$$\rho_j^{(out)} = s\rho + \frac{1-s}{2}I; \quad s = \frac{2}{3}$$

Quantum logical network for UQM

$$\rho_j^{(out)} = s\rho + \frac{1-s}{2} I; \quad s = \frac{2}{3}$$



quantum copier

$$F = 5/6 \text{ compare with measurement } F = 4/6$$

V.Bužek and M.Hillery, *Phys. Rev. A* **54**, 1844 (1996)
N.Gisin and S.Massar, *Phys. Rev. Lett.* **79**, 2153 (1997)
R.F.Werner, *Phys.Rev. A* **58**, 1827 (1998)

Bounds on cloning due to no-signaling

- Input qubit:

$$\rho_a = \frac{1}{2}\left(1 + \vec{\sigma}\cdot\vec{m}\right) = \left|+\vec{m}\right\rangle\left\langle+\vec{m}\right|$$

- Linearity implies no-signaling; output: $\rho_{ab}(\vec{m})$

linear in $\vec{m}$

- Universality (covariance) condition

$$\rho_{ab}\left(U\vec{m}\right) = U \otimes U \rho_{ab}\left(\vec{m}\right) U^{+} \otimes U^{+}$$

- *U*: $\forall$ single-qubit unitary operations

- Basis:

$$\left\{ I \otimes I, I \otimes \sigma_i, \sigma_i \otimes I, \sigma_i \otimes \sigma_k \right\}$$

$$\rho_{ab}\left(\vec{m}\right) = \frac{1}{4}\left(I \otimes I + \eta_1 \vec{m}\vec{\sigma} \otimes I + \eta_2 I \otimes \vec{m}\vec{\sigma} + t\vec{\sigma} \otimes \vec{\sigma} + t_{xy}\vec{m}\left(\vec{\sigma} \wedge \vec{\sigma}\right)\right)$$

Bounds on cloning due to no-signaling

$$\rho_{ab}\left(\vec{m}\right)=\frac{1}{4}\left(I\otimes I+\eta_1\vec{m}\vec{\sigma}\otimes I+\eta_2 I\otimes\vec{m}\vec{\sigma}+t\vec{\sigma}\otimes\vec{\sigma}+t_{xy}\vec{m}\left(\vec{\sigma}\wedge\vec{\sigma}\right)\right)$$

$1\to 2$ cloning

- η_1,η_2,t,t_{xy} are real parameters
- $\rho\left(\vec{m}\right)$ – non-negative eigenvalues

$$1+t\pm\left(\eta_1+\eta_2\right)\geq 0$$

$$1-t\pm\sqrt{4t^2+4t_{xy}^2+\left(\eta_1-\eta_2\right)^2}\geq 0$$

- Optimize the fidelity $F=\mathrm{Tr}\left[\rho_{ab}\left(\vec{m}\right)P_{\vec{m}}\otimes I\right]$
- $P_{\vec{m}}=\left|+\vec{m}\right\rangle\left\langle+\vec{m}\right|,$ assuming $\eta_1=\eta_2\equiv\eta$
- Optimal values $t_{xy}=0,\ t=1/3,\ \eta=2/3\to F=\frac{5}{6}$
- Generalization to 1 toN cloning

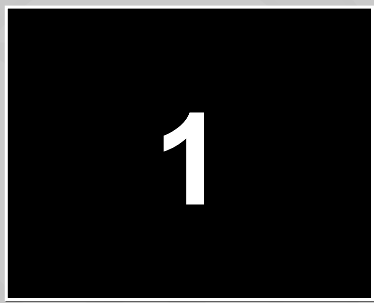
No-signaling and QM give the same fidelity!

N.Gisin, *Phys.Lett. A* **143**, 1 (1990)
C.Simon, V.Bužek, and N.Gisin, *Phys. Rev. Lett.* **87**, 170405 (2001)

Flipping a bit – NOT gate

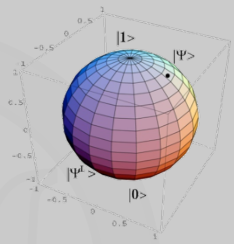
0

Flipping a Bit – NOT gate



Universal NOT gate: Problem

$\left|\psi^{\perp}\right\rangle$ **is antipode of** $\left|\psi\right\rangle$



- Spin flipping is an inversion of the Poincare sphere
- This inversion preserves angels
- The Wigner theorem - spin flip is either unitary or anti-unitary operation
- Unitary operations are equal to proper rotations of the Poincare sphere
- Anti-unitary operations are orthogonal transformations with det=-1
- Spin flip operation is anti-unitary and is not CP
- In the unitary world the ideal universal NOT gate which would flip a qubit in an arbitrary (unknown) state does not exist

Measurement-based vs quantum scenario

Measurement-based scenario: **optimally measure and estimate the state then on a level of classical information perform flip and prepare the flipped state of the estimate**

Quantum scenario**: try to find a unitary operation on the qubit and ancillas that at the output generates the best possible approximation of the spin-flipped state. The fidelity of the operation should be state independent (universality of the U-NOT)**

Measurement-based flipping of qubit

- Estimated density operator when just a single qubit is available

$$\hat{\rho}_{est} = \frac{1}{3}\hat{\rho} + \frac{1}{3}\hat{I}$$

- Flipping based on this estimation

$$\hat{\rho}^{\perp}_{meas} = \frac{1}{3}\hat{\rho}^{\perp} + \frac{1}{3}\hat{I}$$

R.Derka, V.Bužek, and A.K.Ekert, *Phys. Rev. Lett* 80, 1571 (1998)

Theorem: Optimal universal NOT gate

Among all completely positive trace preserving maps

$$T : S\left(H_{+}^{\otimes N}\right) \to S\left(H\right)$$

The measurement-based U-NOT scenario attains the highest possible fidelity, namely

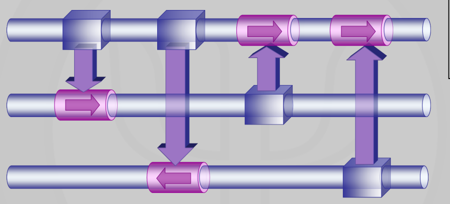
$$F = \left(N+1\right)/\left(N+2\right).$$

H.Bechmann-Pasquinucci and N.Gisin, Phys. Rev, A 59, 4238 (1999)
V.Bužek, M.Hillery, and R.F.Werner *Phys. Rev. A* 60, R2626 (1999)
N.Gisin and S.Popescu *Phys. Rev. Lett.* 83, 432 (1999)

Approximate U-NOT gate

$\left|\psi\right\rangle_a$

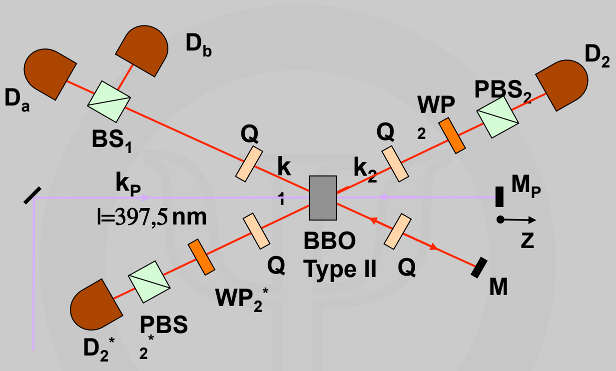
$\left|\Xi\right\rangle_{bc}$

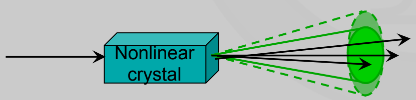


$$\rho_c^{(out)} = \frac{1}{3}\rho^{\perp} + \frac{1}{3}I$$

W.Wootters and W.H.Zurek, *Nature* 299, 802 (1982)
V.Bužek and M.Hillery, *Phys. Rev. A* 54, 1844 (1996)
S.L.Braunstein, V.Bužek, M.Hillery, and D.Bruss, *Phys. Rev. A* 56, 2153 (1997)

U-NOT via optical parametric amplifier





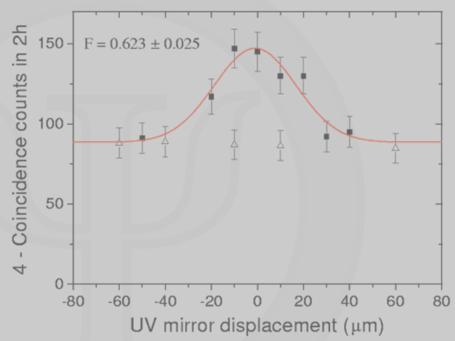
$$H_I = i\chi\hbar\left[a^+_\psi b^+_{\psi\perp} - a^+_{\psi\perp} b^+_\psi\right] + h.c.$$

$$\left|\psi\right\rangle = a^+_\psi \left|0,0\right\rangle_{k_1} = \left|1,0\right\rangle_{k_1}$$

A.Lamas-Linares, C.Simon, J.C.Howell, and D.Bouwmeester, *Science* 296, 712 (2002)
F.DeMartini, V.Bužek, F.Sciarino, and C.Sias, *Nature* 419, 815 (2002)

Optimal universal-NOT gate

$$F = \frac{R}{R+1}$$



There is something in this network

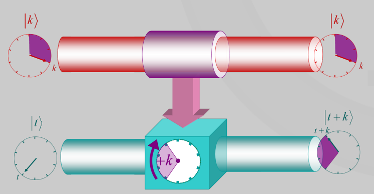
$$|\psi\rangle_1 = \sum_{k=0}^{N-1} c_k |x_k\rangle_1$$

$$\hat{x}|x_k\rangle = x_k|x_k\rangle \qquad x_k = L\sqrt{\frac{2\pi}{N}}k$$

$$\hat{p}|p_l\rangle = p_l|p_l\rangle \qquad p_l = \frac{1}{L}\sqrt{\frac{2\pi}{N}}l$$

$$|x_k\rangle = \frac{1}{\sqrt{N}}\sum_{l=0}^{N-1}\exp\left(-i\frac{2\pi}{N}kl\right)|p_l\rangle$$

$$|\langle x_k \mid p_l\rangle|^2 = \frac{1}{N}$$

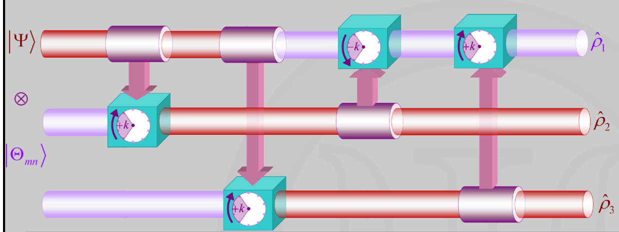


$$\widehat{D}_{ab}: |k\rangle_a|l\rangle_b \to |k\rangle_a|(l+k)\bmod N\rangle_b$$

$$\widehat{D}_{ab} = \exp\left[-i\hat{x}_a\hat{p}_b\right]$$

S.L.Braunstein, V.Bužek, and M.Hillery, *Phys. Rev. A* 63, 052313 (2001)

Quantum information distributor



$$\rho_1^{(out)} = \left(\alpha^2 + \frac{2\alpha\beta}{N}\right)\rho + \frac{\beta^2}{N}I$$

$$\rho_2^{(out)} = \left(\beta^2 + \frac{2\alpha\beta}{N}\right)\rho + \frac{\alpha^2}{N}I$$

$$\rho_3^{(out)} = \frac{2\alpha\beta}{N}\rho^T + \frac{(N-2\alpha\beta)}{N^2}I$$

$$\widehat{U} = \exp\left[-i(\hat{x}_3-\hat{x}_2)\hat{p}_1\right]\exp\left[-i\hat{x}_1(\hat{p}_2-\hat{p}_3)\right]$$

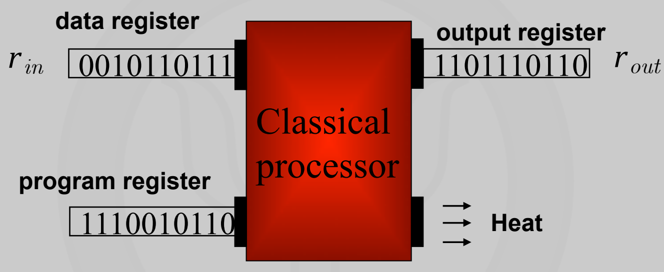
$$|\Theta(s)\rangle_{23} = \alpha\frac{1}{\sqrt{N}}\sum_{k}^{N-1}|x_k\rangle_2|x_k\rangle_3 + \beta|x_0\rangle_2|p_0\rangle_3$$

$$\alpha^2+\beta^2+\frac{2\alpha\beta}{N}=1$$

- Covariant device with respect to SU(2) operations
- POVM measurements
- eavesdropping

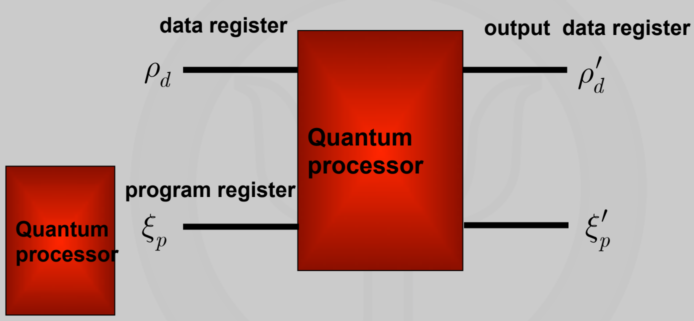
S.L.Braunstein, V.Bužek, and M.Hillery, *Phys. Rev. A* 63, 052313 (2001)

Model of classical processor



$$\rho_{out} = T[\rho_{in}]$$

Quantum processor



Quantum processor – fixed unitary transformation U_{dp}

$\mathcal{H}_d$ – data system, $S(\mathcal{H}_d)$ – data states

$\mathcal{H}_p$ – program system, $S(\mathcal{H}_p)$ – program states

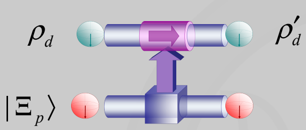
Two scenarios

- **Measurement-based strategy - estimate the state of program**

$$\boxed{F = \frac{N+1}{N+d}}$$

- **Quantum strategy – use the quantum program register**
  conditional (probabilistic) processors
  unconditional processors

C-NOT as unconditional q-processor



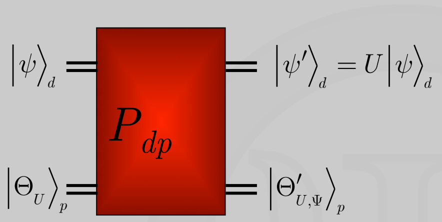
$$\text{CNOT } |\psi\rangle|0\rangle = |\psi\rangle|0\rangle$$
$$\text{CNOT } |\psi\rangle|1\rangle = \sigma_x|\psi\rangle \otimes |1\rangle$$

- program state $|0\rangle \Rightarrow \mathbf{1}$ implemented, i.e. $\rho_d \to \rho'_d = \rho_d$
- program state $|1\rangle \Rightarrow \sigma_x$ implemented, i.e. $\rho_d \to \rho'_d = \sigma_x \rho_d \sigma_x$
- general pure state $|\Xi_p\rangle = \alpha|0\rangle_p + \beta|1\rangle_p \Rightarrow \rho_d \mapsto \rho'_d = |\alpha|^2 \rho_d + |\beta|^2 \sigma_x \rho_d \sigma_x$
- unital operation, since $\Phi[\mathbf{1}] = |\alpha|^2 \mathbf{1} + |\beta|^2 \sigma_x \mathbf{1} \sigma_x = \mathbf{1}$
- program state is **2-d** and we can apply **2** unitary operations

Question

Is it possible to build a *universal* programmable quantum gate array which take as input a quantum state specifying a quantum program and a data register to which the unitary operation is applied ?

No-go theorem



$$P_{dp}\left(|\psi\rangle_d \otimes |\Theta_U\rangle_p\right) = \left(U|\psi\rangle\right) \otimes |\Theta'_{U,\psi}\rangle$$

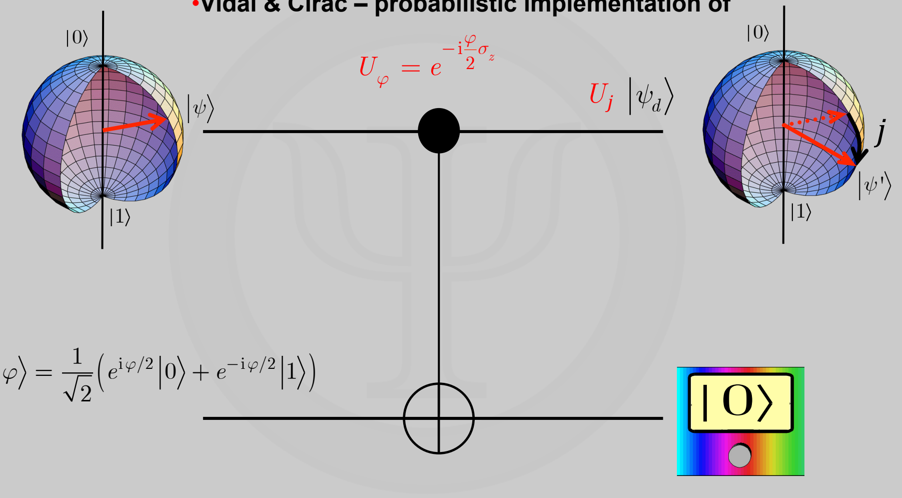
- **no universal deterministic quantum array of finite extent can be realized**
- **on the other hand – a program register with *d* dimensions can be used to implement *d* unitary operations by performing an appropriate sequence of controlled unitary operations**

M.A.Nielsen & I.L.Chuang, *Phys. Rev. Lett* 79, 321 (1997)

C-NOT: probabilistic q-processor

• Vidal & Cirac – probabilistic implementation of

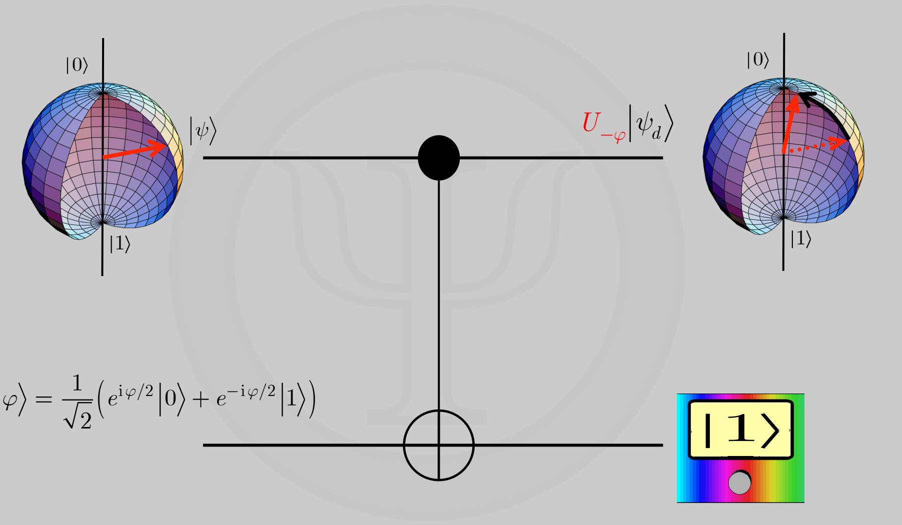
$$U_{\varphi} = e^{-i\frac{\varphi}{2}\sigma_z}$$



$$|\varphi\rangle = \frac{1}{\sqrt{2}}\left(e^{i\varphi/2}|0\rangle + e^{-i\varphi/2}|1\rangle\right)$$

G.Vidal and J.I.Cirac, Los Alamos arXiv *quant-ph/0012067* (2000)
G.Vidal, L.Mesanes, and J.I.Cirac, Los Alamos arXiv *quant-ph/0102037* (2001).

C-NOT: probabilistic q-processor



$$|\varphi\rangle = \frac{1}{\sqrt{2}}\left(e^{i\varphi/2}|0\rangle + e^{-i\varphi/2}|1\rangle\right)$$

Correction of the error – new run of the processor with $|2\varphi\rangle$

Description of q-processors

- **definition of U_{dp} via "Kraus operators"** $A_{kl} := {}_p\langle l|U_{dp}|k\rangle_p$

$$U_{dp}\left(|\psi\rangle_d \otimes |k\rangle_p\right) = \sum_l \left(A_{kl}|\psi\rangle_d\right)\otimes|l\rangle_p$$

- **normalization condition** $\sum_l A^\dagger_{k_1 l}A_{k_2 l} = \delta_{k_1 k_2}\mathbf{1}_d$
- **induced quantum operation** $\rho_d \mapsto \rho'_d = \Phi_k[\rho_d] = \sum_l A_{kl}\rho_d A^\dagger_{kl}$
- **general pure program state** $|\Xi\rangle_p = \sum_k \alpha_k |k\rangle_p$

$$\rho_d \mapsto \rho'_d = \Phi_\Xi[\rho_d] = \sum_l A_l(\Xi)\rho_d A_l^\dagger(\Xi)$$

$$A_l(\Xi) = {}_p\langle l|U_{dp}|\Xi\rangle_p = \sum_k \alpha_k A_{kl}$$

- **can be generalized for mixed program states**

Universal probabilistic processor

- Quantum processor U_{dp}
- Data register r_d, dim $H_d = D$
- Quantum programs U_k = program register r_p, dim $H_p = N = D^2$

- Nielsen & Chuang:
  - N programs Þ N orthogonal states
  - Universal quantum processors do not $\exists$
- Bužek-Hillery-Ziman:
  - Probabilistic implementation
  - $\{U_k\}$ operator basis,

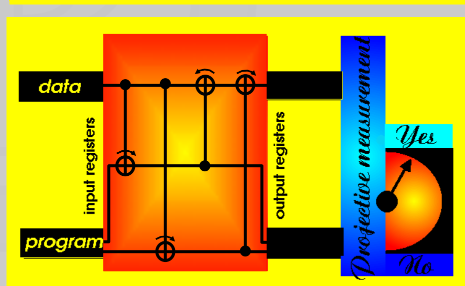
    $U = \sum_k \alpha_k U_k, \quad \alpha_k = \frac{1}{D}\mathbf{Tr}U_k^+ U$
  - program state

    $|\psi_U\rangle = \sum_k \alpha_k |\psi_k\rangle$

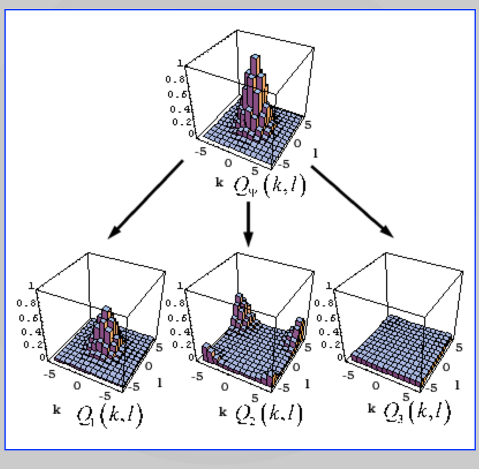
Example:
Data register = qudit, program register = 2 qudits

$$U_k \equiv U^{(mn)} = \sum_{s=0}^{D-1}\exp\left(-\frac{2\pi i s m}{N}\right)|s-n\rangle\langle s|$$

$$|\psi_k\rangle \equiv |\Xi_{mn}\rangle = \frac{1}{\sqrt{D}}\sum_{s=0}^{D-1}\exp\left(-\frac{2\pi i s m}{N}\right)|s\rangle|s-n\rangle$$



POVM Measurement



V.Bužek, M.Roško, and M.Hillery, ***unpublished***