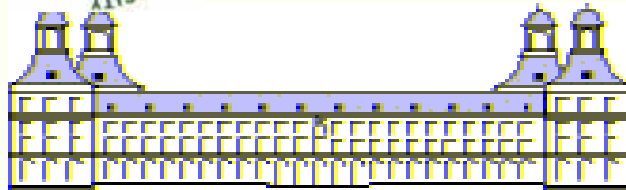


Theory of Quantum Entanglement

Shao-Ming Fei



Capital Normal University, Beijing



Universität Bonn, Bonn

Richard Feynman 1980

Certain quantum mechanical effects cannot be simulated efficiently on a classical computer

Peter Shor 1994

polynomial time quantum algorithm for factoring integers $15=3 \times 5$

Number of order 10^{130}

limit of current classical method

42 days, number field sieve, 10^{12} operations/second

Number of order 10^{260}

classically intractable (million years)

quantum algorithm: 8 times longer

Classical bit: 0 or 1

Quantum bit (qubit): 2-d complex vector

$$|\mathbf{1}\rangle = \begin{pmatrix} \mathbf{0} \\ \mathbf{1} \end{pmatrix} \quad |\mathbf{0}\rangle = \begin{pmatrix} \mathbf{1} \\ \mathbf{0} \end{pmatrix}$$

$$|\alpha\rangle = a|\mathbf{0}\rangle + b|\mathbf{1}\rangle = \begin{pmatrix} \mathbf{a} \\ \mathbf{b} \end{pmatrix}, \quad a, b \in \mathbb{C}, \quad |a|^2 + |b|^2 = 1$$

Quantum measurement:

$$\begin{cases} |\mathbf{1}\rangle : |\langle \mathbf{1} | \alpha \rangle|^2 = |a|^2 \\ |\mathbf{0}\rangle : |\langle \mathbf{0} | \alpha \rangle|^2 = |b|^2 \end{cases} \quad \langle \alpha | = (|\alpha\rangle)^\dagger$$

Cryptography

♠ Cryptography with private key

<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>	<i>E</i>	<i>X</i>	<i>Y</i>	<i>Z</i>	?	,	.	
00	01	02	03	04	23	24	25	26	27	28	29

<i>S</i>	<i>H</i>	<i>A</i>	<i>K</i>	<i>E</i>	<i>N</i>	<i>N</i>	<i>O</i>	<i>T</i>	<i>S</i>	<i>T</i>	<i>I</i>	<i>R</i>	<i>R</i>	<i>E</i>	<i>D</i>			
18	07	00	10	04	13	26	13	14	19	26	18	19	08	17	17	04	03	<i>Plaintext number (P)</i>
15	04	28	13	14	06	21	11	23	18	09	11	14	01	19	05	22	07	<i>Key numbers (K)</i>
03	11	28	23	18	19	17	24	07	07	05	29	03	09	06	22	26	10	<i>Code number (C)</i>

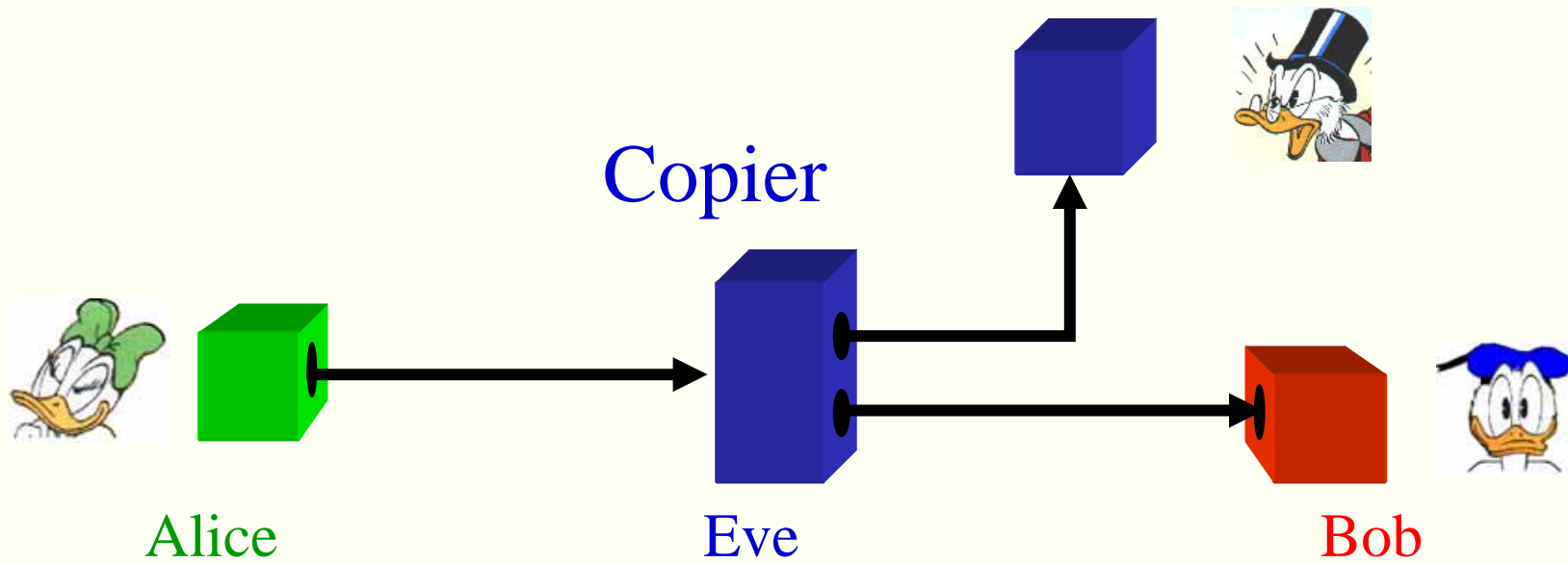
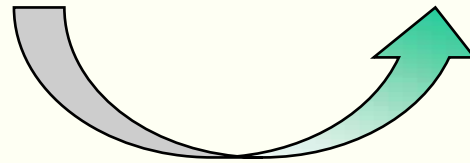
Key numbers: randomly selected from $0 \rightarrow 29$

$$C = P + K \pmod{30}$$

Alice sends C to Bob

Bob: decryption $C - K \pmod{30} = P$

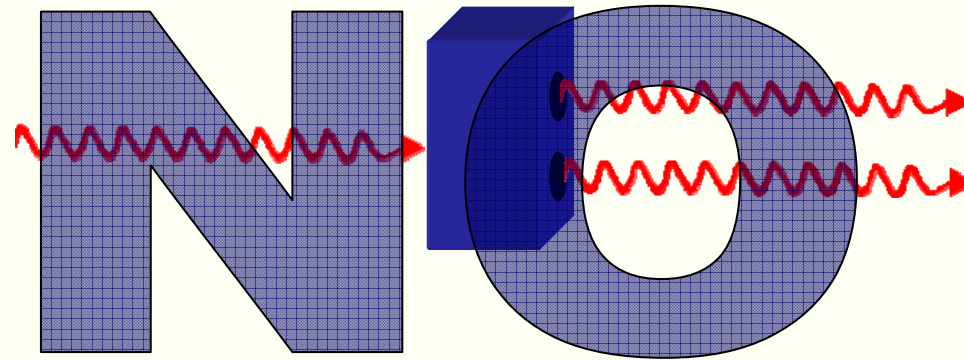
No private key: Alice ← Bob $N = P Q$



Impossible : Quantum Copier

No-Cloning

Copier:

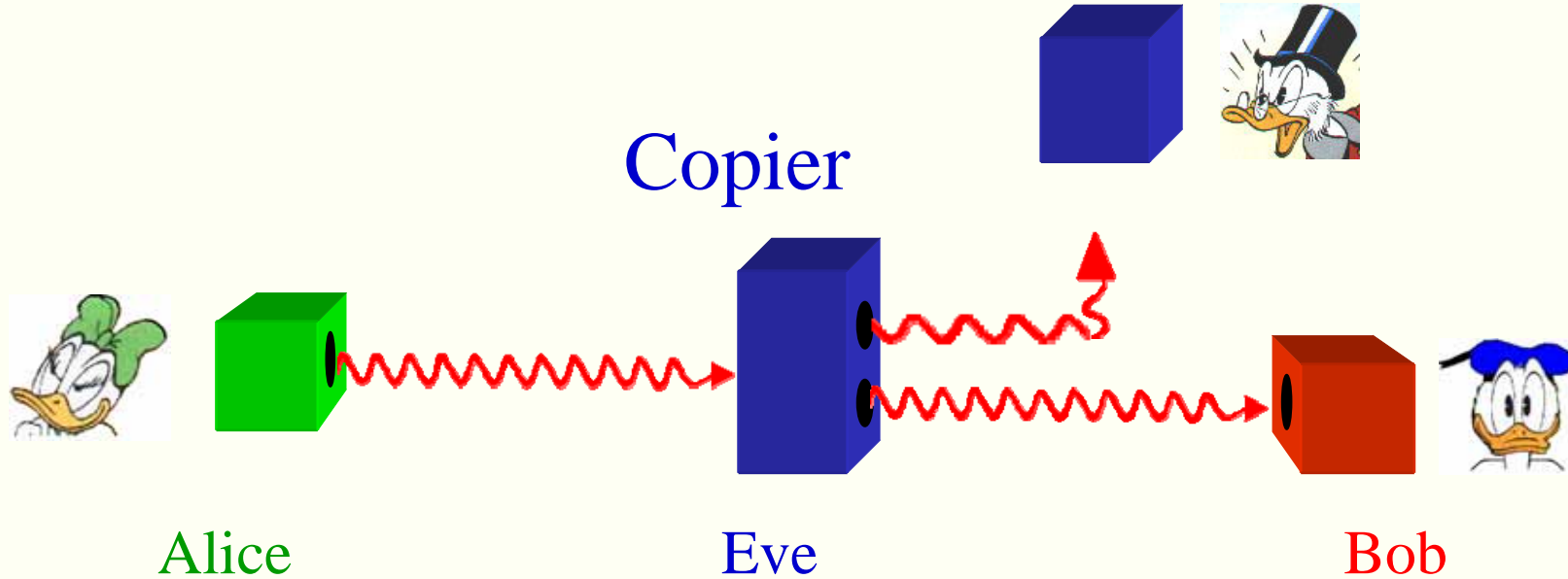


Quantum information is a
new kind of information

Application:

Quantum Cryptography

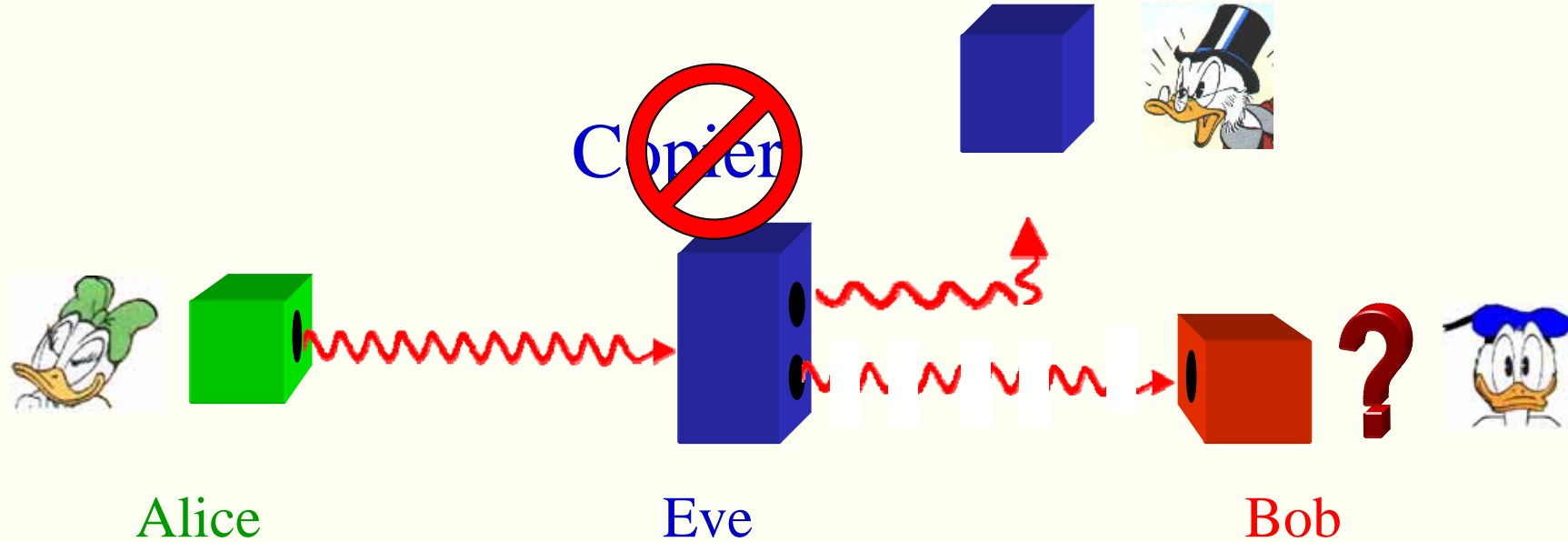
eavesdropping on quantum information ?



Application:

Quantum Cryptography

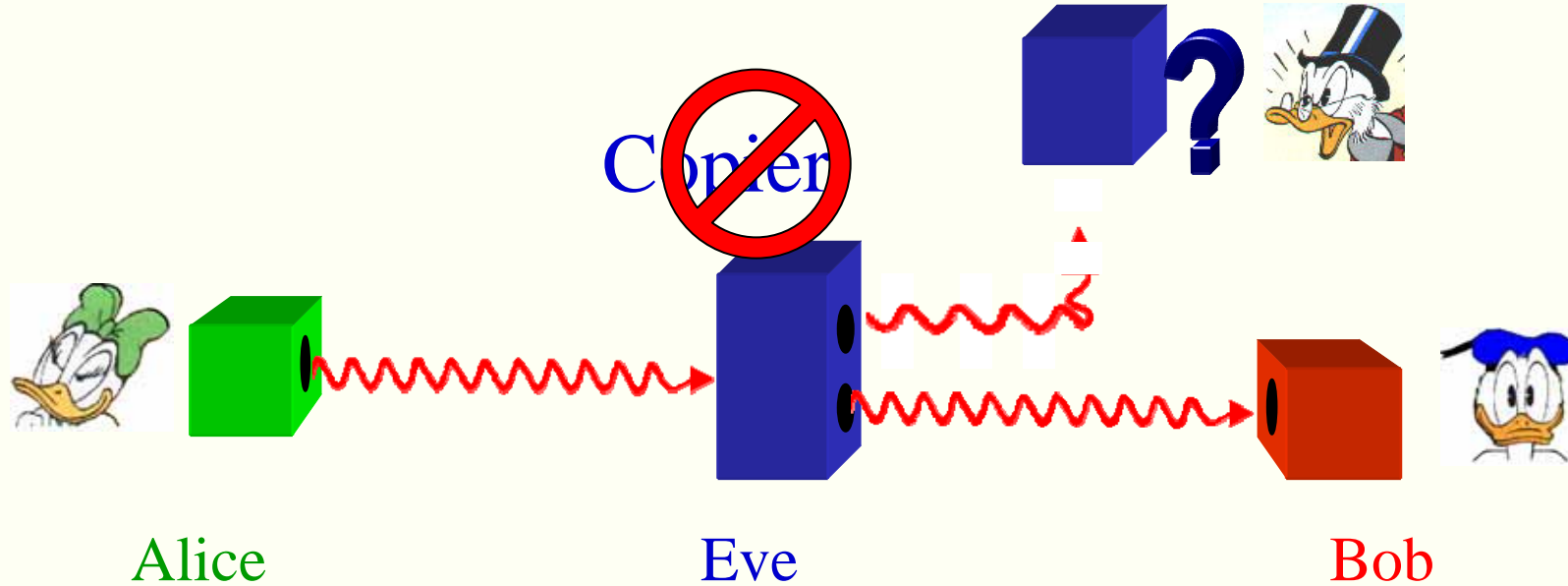
Detected eavesdropping on quantum information



Application:

Quantum Cryptography

Failed eavesdropping on quantum information

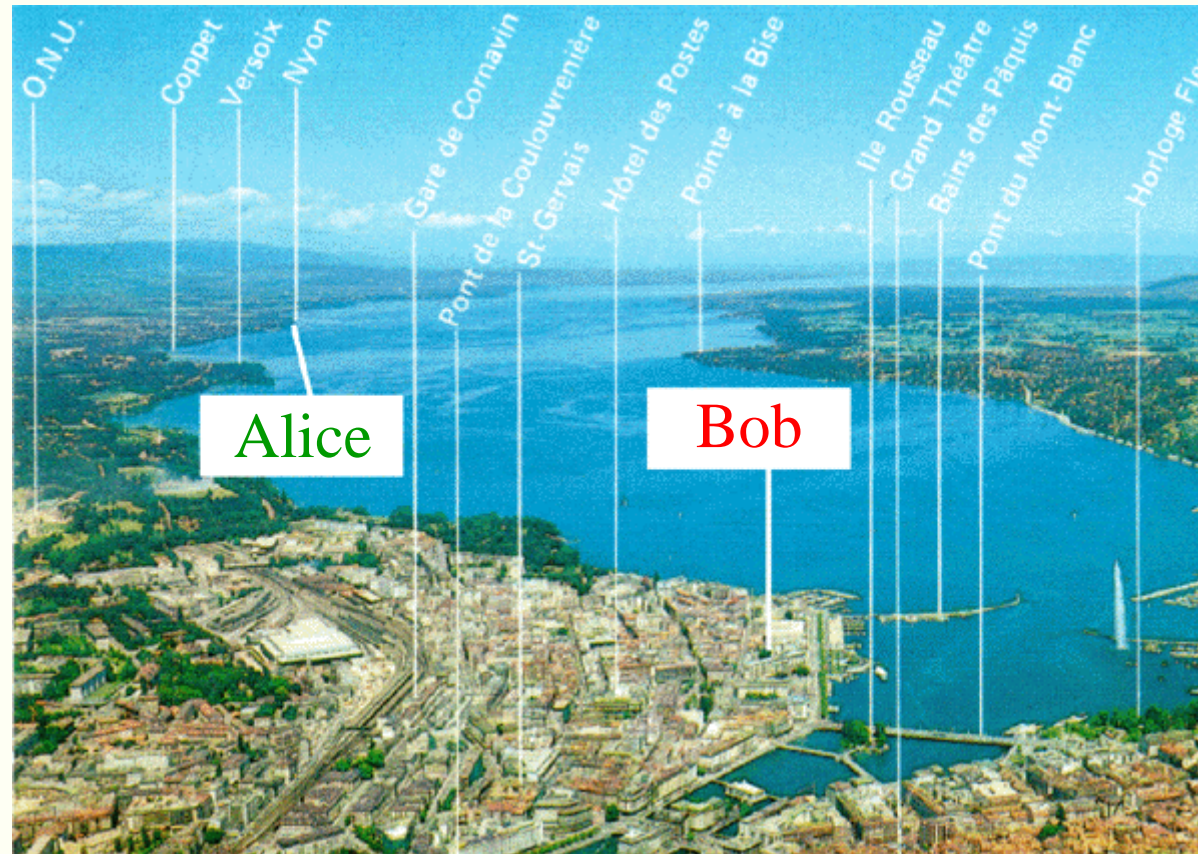


Suitable for key distribution

Experimental realization (among others)

by N. Gisin et al :

„A Plug and Play system for quantum cryptography“



23 km of standard optical fibre: supplied by



Multiqubits (qubit array):

$$\mathcal{H} \otimes \mathcal{H} \otimes \dots \otimes \mathcal{H}$$

two qubits: basis vector $|0\rangle_1 \otimes |1\rangle_2 \equiv |01\rangle, |10\rangle, |00\rangle, |11\rangle$

n qubits: 2^n basis vectors

Entangled states

$$|\alpha\rangle \neq (a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) \otimes \dots \otimes (a_n|0\rangle + b_n|1\rangle)$$

$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ EPR (Einstein, Podolsky and Rosen) pair

$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Separable state

Quantum gates: unitary transformations U

Single-qubit:

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} : |0\rangle \rightarrow |0\rangle, \quad |1\rangle \rightarrow |1\rangle$$
$$\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} : |0\rangle \rightarrow |1\rangle, \quad |1\rangle \rightarrow |0\rangle$$
$$\mathbf{Y} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} : |0\rangle \rightarrow |1\rangle, \quad |1\rangle \rightarrow -|0\rangle$$
$$\mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} : |0\rangle \rightarrow |0\rangle, \quad |1\rangle \rightarrow -|1\rangle$$

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

Controlled-NOT gate, C_{not} (on two qubits)

$$C_{\text{not}} : \begin{array}{l} |00\rangle \rightarrow |00\rangle \\ |01\rangle \rightarrow |01\rangle \\ |10\rangle \rightarrow |11\rangle \\ |11\rangle \rightarrow |10\rangle \end{array} \quad C_{\text{not}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Impossible : Quantum Copier

No-Cloning Theorem:

No U such that $U(|\alpha 0\rangle) = |\alpha\alpha\rangle, U(|\beta 0\rangle) = |\beta\beta\rangle$

[Proof] $|\gamma\rangle = (1/\sqrt{2})(|\alpha\rangle + |\beta\rangle)$

$$U(|\gamma 0\rangle) = U\left(\frac{1}{\sqrt{2}}(|\alpha 0\rangle + |\beta 0\rangle)\right) = \frac{1}{\sqrt{2}}(|\alpha\alpha\rangle + |\beta\beta\rangle)$$

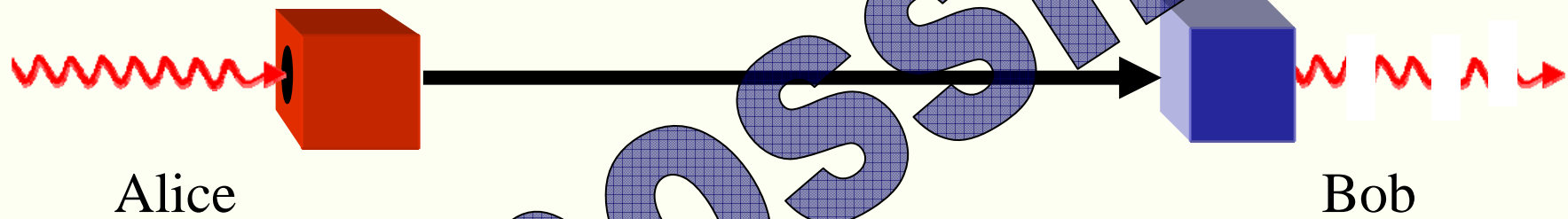
$$U(|\gamma 0\rangle) = |\gamma\gamma\rangle = \frac{1}{2}(|\alpha\alpha\rangle + |\alpha\beta\rangle + |\beta\alpha\rangle + |\beta\beta\rangle)$$

Optimal cloning: Unitary trans. \rightarrow best fidelity

(general case: d-dim. ; N to M copies)

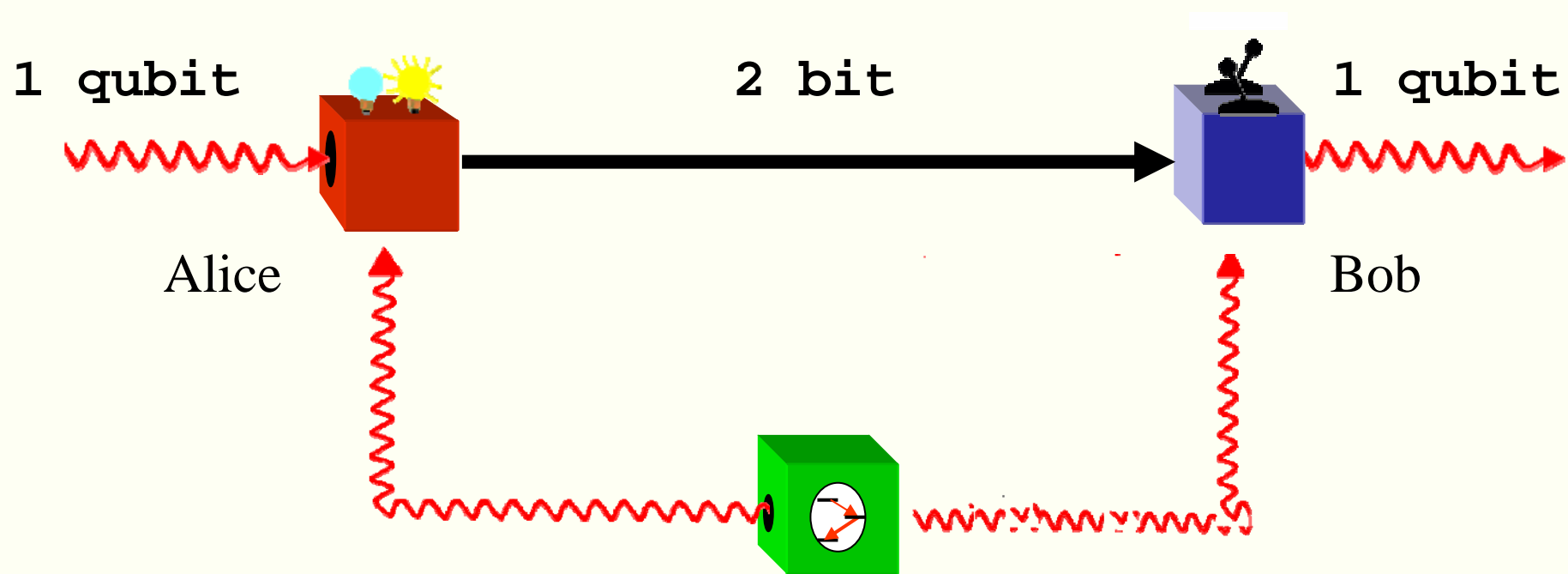
S. Albeverio, S.M. Fei, Euro. Phys. J. B 14(2000)669

Teleportation

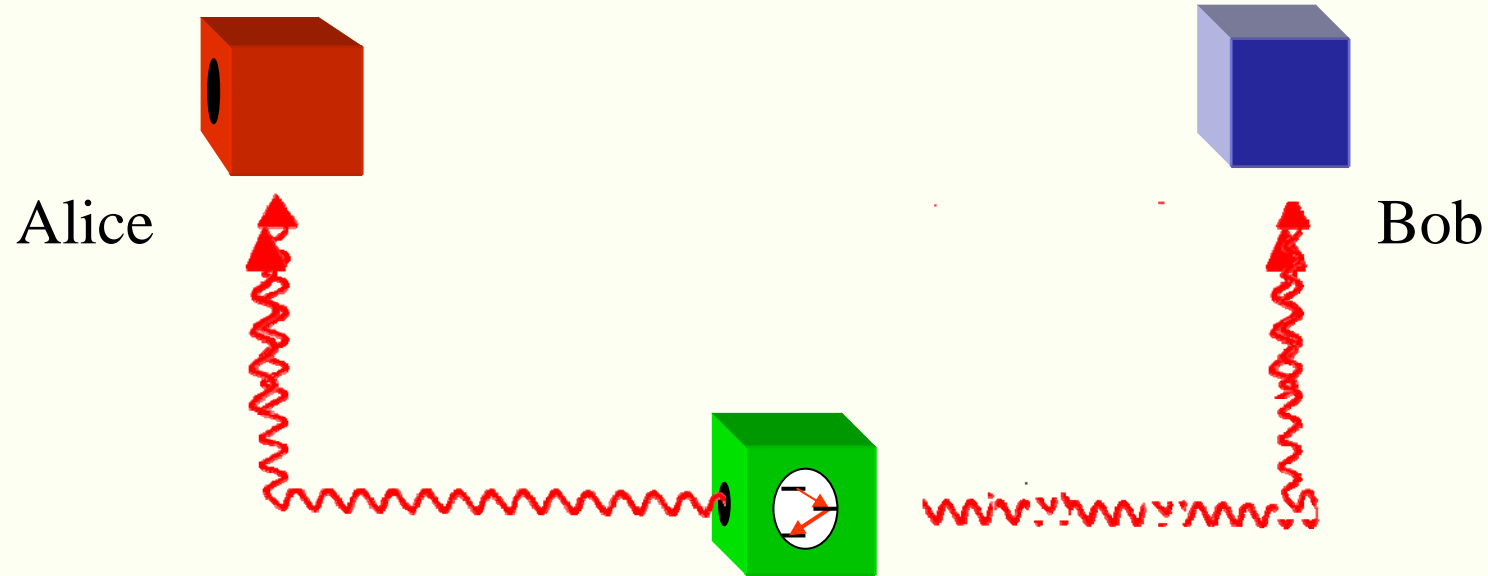


impossible

Entanglement enhanced Teleportation

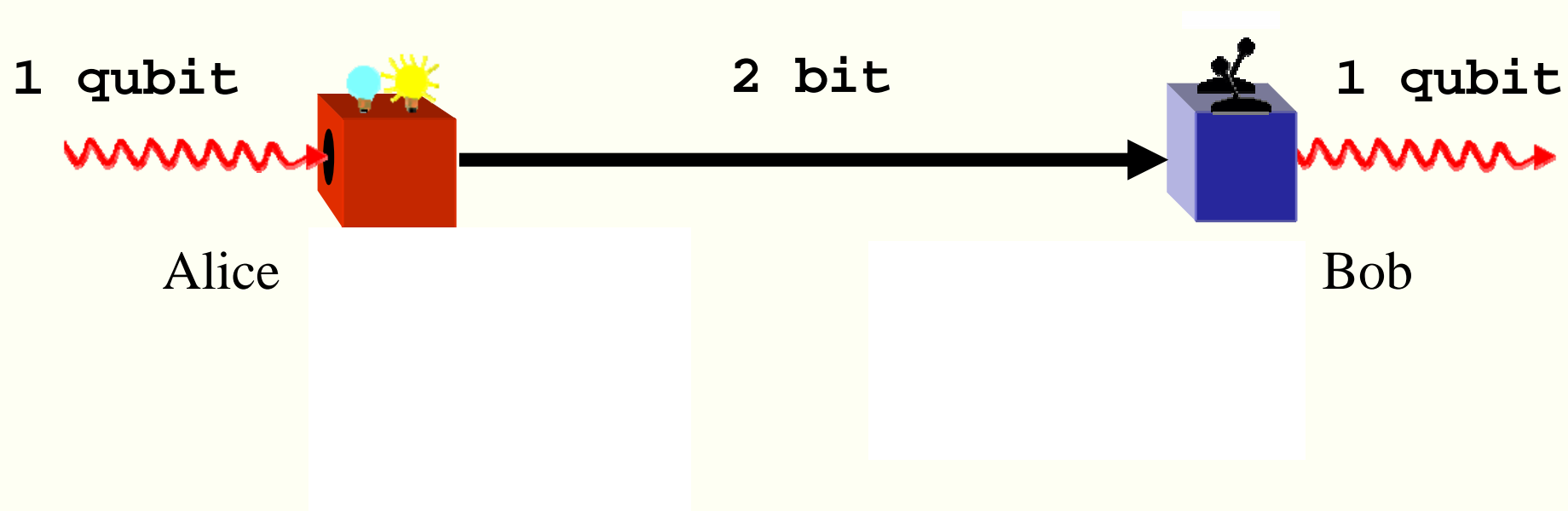


Entanglement enhanced Teleportation

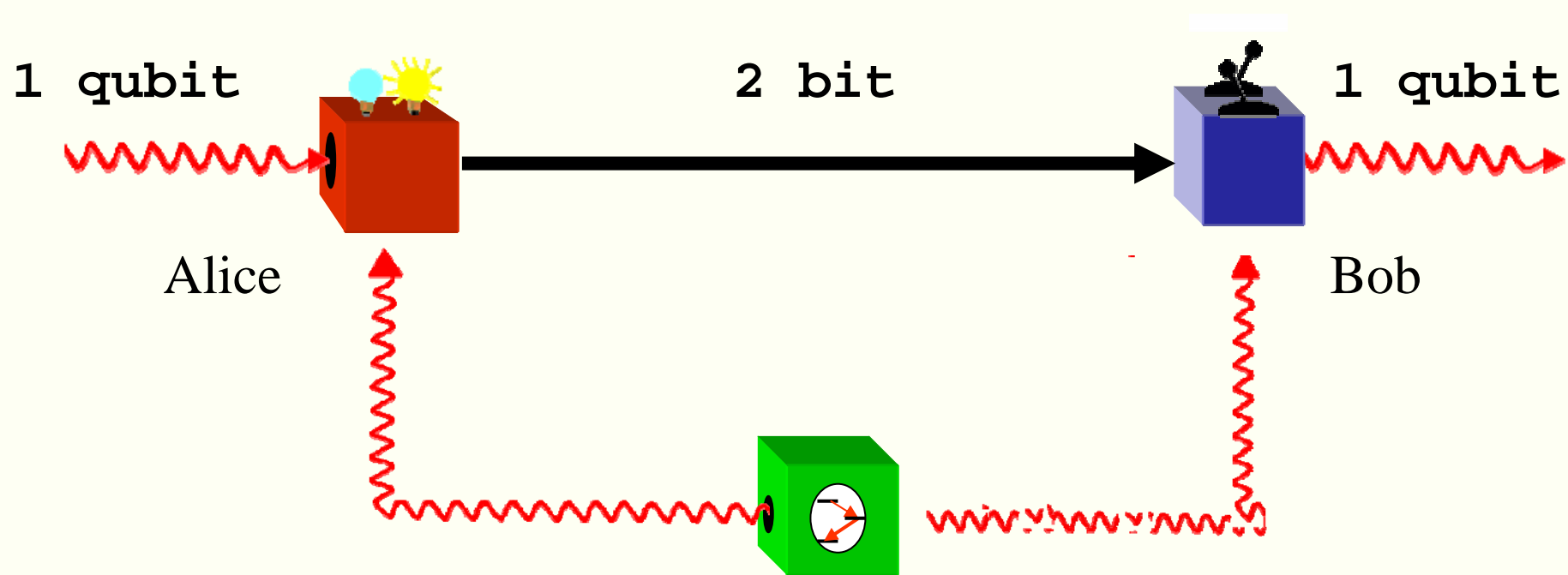


$$\frac{1}{\sqrt{2}} (|01\rangle - |10\rangle)$$

Entanglement enhanced Teleportation



Entanglement enhanced Teleportation



Alice:

$$\phi = a|0\rangle + b|1\rangle \quad \psi_0 = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$\phi \otimes \psi_0 = \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle)$$

$$(\mathbf{H} \otimes \mathbf{I} \otimes \mathbf{I})(\mathbf{C}_{\text{not}} \otimes \mathbf{I})(\phi \otimes \psi_0) =$$

$$\frac{1}{2}(|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) \\ + |10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle))$$

Alice
M

bits received	state	decoding
00	$a 0\rangle + b 1\rangle$	I
01	$a 1\rangle + b 0\rangle$	X
10	$a 0\rangle - b 1\rangle$	Z
11	$a 1\rangle - b 0\rangle$	Y

Bob
U

General case: d-dim.; mixed states; optimal

Optimal fidelity

$$f_{\max}(\chi) = \frac{n\mathcal{F}(\chi)}{n+1} + \frac{1}{n+1}$$

S. Albeverio, S.M. Fei, Phys. Lett. A 276(2000)8

S. Albeverio, S.M. Fei and W.L. Yang, Commun. Theor. Phys. 38 (2002) 301-304; Phys. Rev. A 66(2002)012301.

M. Horodecki, P. Horodecki and R. Horodecki, Phys. Rev. A 60, 1888 (1999).

Fully entangled fraction

$$\mathcal{F}(\chi) = \max\{\langle \Phi | (1 \otimes U^\dagger) \chi (1 \otimes U) | \Phi \rangle\}$$

$$|\Phi\rangle = 1/\sqrt{n} \sum_{i=0}^{n-1} |ii\rangle \quad (\text{Maximally entangled pure state})$$

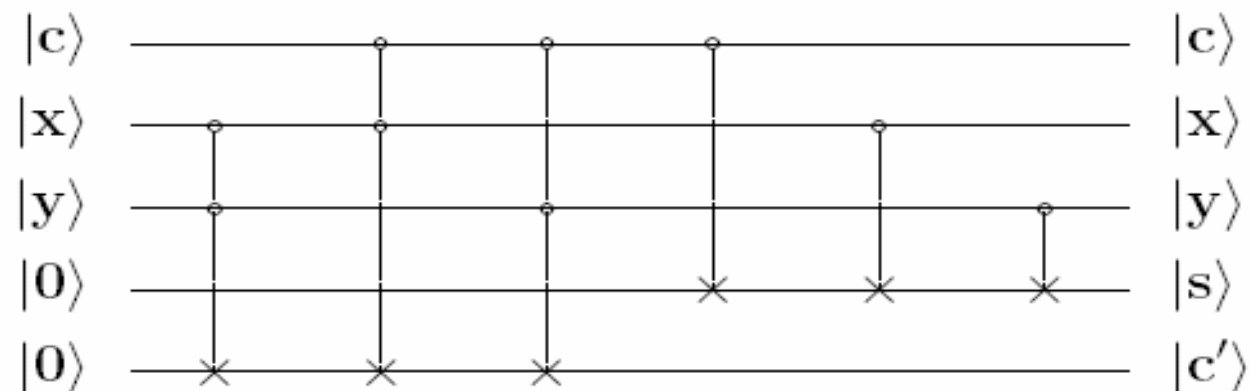
M. Li, S.M. Fei and Z.X. Wang, Phys. Rev. A, 78(2008)032332.

Quantum computation

Toffoli gate (Controlled-Controlled-NOT)

$$T = |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes C_{\text{not}}$$

Quantum circuit: a 1-bit full adder



x, y data bits, s sum (modulo 2), c (c') carry bit

Deutsch: possible to construct reversible quantum gates for any arbitrary classically computable function \mathbf{f}

$$U_f |x, 0\rangle \rightarrow |x, f(x)\rangle$$

Quantum Parallelism:

$$W : |00\dots 0\rangle \Rightarrow \frac{1}{\sqrt{2^n}} (|00\dots 0\rangle + |00\dots 1\rangle + \dots + |11\dots 1\rangle) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

$$U_f \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, 0\rangle \right) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} U_f(|x, 0\rangle) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, f(x)\rangle$$

Quantum algorithm: Manipulating quantum parallelism \Rightarrow desired results with high probability

Shor's factorisation algorithm

Period finding and quantum Fourier transform

$f(\mathbf{x})$, period \mathbf{r} : $f(\mathbf{x}) = f(\mathbf{x} + \mathbf{r})$

$f(\mathbf{x})$ can be efficiently computed from \mathbf{x} , $\mathbf{N}/2 < \mathbf{r} < \mathbf{N}$ for some \mathbf{N}

QC: $2\mathbf{n}$ qubits, $\mathbf{n} = \lceil 2 \log \mathbf{N} \rceil$

Two 'registers', \mathbf{X} and \mathbf{Y} , each \mathbf{n} qubits

Initially prepared in the state $|\mathbf{0}\rangle|\mathbf{0}\rangle$

H applies to each qubit in the **X** register:

$$\frac{1}{\sqrt{w}} \sum_{\mathbf{x}=0}^{w-1} |\mathbf{x}\rangle |\mathbf{0}\rangle, \quad w = 2^n$$

$$U_f |\mathbf{x}\rangle |\mathbf{0}\rangle = |\mathbf{x}\rangle |\mathbf{f}(\mathbf{x})\rangle$$

$$\frac{1}{\sqrt{w}} \sum_{\mathbf{x}=0}^{w-1} |\mathbf{x}\rangle |\mathbf{f}(\mathbf{x})\rangle$$

Measure **Y**: $\mathbf{f}(\mathbf{x}) = \mathbf{u}$

Y register state collapses onto $|\mathbf{u}\rangle$

$$\frac{1}{\sqrt{M}} \sum_{\mathbf{j}=0}^{M-1} |\mathbf{d}_u + \mathbf{j}\mathbf{r}\rangle |\mathbf{u}\rangle$$

$\mathbf{d}_u + \mathbf{j}\mathbf{r}$, $\mathbf{j} = 0, 1, 2 \dots M - 1$, all \mathbf{x} such that $\mathbf{f}(\mathbf{x}) = \mathbf{u}$, $M \simeq w/r$

Quantum Discrete Fourier transform:

$$U_{FT}|\mathbf{x}\rangle = \frac{1}{\sqrt{\mathbf{w}}} \sum_{\mathbf{k}=0}^{\mathbf{w}-1} e^{i2\pi\mathbf{k}\mathbf{x}/\mathbf{w}} |\mathbf{k}\rangle$$

$$U_{FT} \frac{1}{\sqrt{\mathbf{w}/\mathbf{r}}} \sum_{\mathbf{j}=0}^{\mathbf{w}/\mathbf{r}-1} |\mathbf{d}_u + \mathbf{j}\mathbf{r}\rangle = \frac{1}{\sqrt{\mathbf{r}}} \sum_{\mathbf{k}} \tilde{\mathbf{f}}(\mathbf{k}) |\mathbf{k}\rangle$$

$$|\tilde{\mathbf{f}}(\mathbf{k})| = \begin{cases} 1 & \text{if } \mathbf{k} \text{ is a multiple of } \mathbf{w}/\mathbf{r} \\ 0 & \text{otherwise} \end{cases}$$

Measure $\Rightarrow \nu = \lambda\mathbf{w}/\mathbf{r}$, λ unknown

$$\frac{\nu}{\mathbf{w}} = \frac{\lambda}{\mathbf{r}}$$

$$\mathbf{w} = 2^n$$

If λ and \mathbf{r} have no common factors, cancel ν/\mathbf{w} down to an irreducible fraction and thus obtain λ and \mathbf{r}

If λ and \mathbf{r} have a common factor (unlikely for large \mathbf{r}), algorithm fails, repeat the algorithm

repetitions no greater than $\sim \log \mathbf{r}$ (usually much less) probability of success is arbitrarily close to **1**

Take $f(x) = a^x \bmod N$

N the number to be factorized, $a < N$ is chosen randomly

Elementary number theory: for most choices of a , r is even

$$a^{r+x} = a^x \bmod N$$

$$a^r = 1 \bmod N$$

$$(a^{r/2} + 1)(a^{r/2} - 1) = 0 \bmod N$$

$a^{r/2} \pm 1$ shares a common factor with N

L. Grover quantum searching: $O(N/2) \rightarrow O(\sqrt{N})$

Quantum Information Processing

Initial State $|\psi\rangle_o \Rightarrow$ Final State $|\psi\rangle_t$

Unitary Transformations
+ Measurements

Quantum Entnglement:

- ✦ Quantum computation
 - ✦ Quantum teleportation
 - ✦ Dense coding
 - ✦ Quantum cryptography
 - ✦ Quantum error correction

Quantum Entanglement

\mathcal{H} : N-dim. complex Hilbert space, $|i\rangle$

Pure state (Vector) on $\mathcal{H} \otimes \mathcal{H} \otimes \dots \otimes \mathcal{H}$:

$$|\psi\rangle = \sum_{i,j,\dots,k=1}^N a_{ij\dots k} |ij\dots k\rangle, \quad a_{ij\dots k} \in \mathbb{C} \quad \in \mathcal{H} \otimes \mathcal{H} \otimes \dots \otimes \mathcal{H}$$
$$\rightarrow \left(\sum_{i=1}^N a_i |i\rangle \right) \otimes \left(\sum_{j=1}^N b_j |j\rangle \right) \otimes \dots \otimes \left(\sum_{k=1}^N c_k |k\rangle \right) \quad \text{Separable!}$$

$$\sum_{i,j,\dots,k=1}^N a_{ij\dots k} a_{ij\dots k}^* = \mathbf{1}$$

$$|ij\dots k\rangle \equiv |i\rangle \otimes |j\rangle \otimes \dots \otimes |k\rangle$$

Pure State : $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H} \otimes \dots \otimes \mathcal{H}$

Mean value of \mathbf{O} : $\langle \mathbf{O} \rangle = \langle \psi | \mathbf{O} | \psi \rangle = \text{Tr}(|\psi\rangle\langle\psi| \mathbf{O}) = \text{Tr}(\rho \mathbf{O})$

$$\langle \psi | = (|\psi\rangle)^\dagger \quad \rho = |\psi\rangle\langle\psi|$$

Mixed state:

$$\rho = \sum p_i |\psi_i\rangle\langle\psi_i|, \quad 0 < p_i \leq 1, \quad \sum p_i = 1$$

$\exists |\psi_i\rangle$ such that $|\psi_i\rangle$ are separable $\forall i$: ρ **Separable!**

$$\rho = \sum p_i \rho_1^i \otimes \rho_2^i \otimes \dots \otimes \rho_n^i \quad \text{Separable !}$$

Two qubits ($N=2$)

$$E(|\psi\rangle) = h\left(\frac{1 + \sqrt{1 - C^2}}{2}\right)$$

$$h(x) = -x \log_2 x - (1 - x) \log_2(1 - x)$$

Concurrence C : $|\psi\rangle = a_{11}|00\rangle + a_{12}|01\rangle + a_{21}|10\rangle + a_{22}|11\rangle$

$$C = 2|a_{11}a_{22} - a_{12}a_{21}|, \quad |a_{11}|^2 + |a_{12}|^2 + |a_{21}|^2 + |a_{22}|^2 = 1$$

$E \sim C$: monotonically increasing

$$E(|\psi\rangle) \implies E(C(|\psi\rangle)) \quad E(\rho) \implies E(C(\rho))$$

$$C(\rho) = \text{Max}\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}.$$

$$\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \lambda_4 : \quad \text{eigenvalue of } \sqrt{\rho\tilde{\rho}}$$

$$\tilde{\rho} = (\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y)$$

W. K. Wootters, Phys. Rev. Lett.
80, 2245 (1998)

High dimension $N > 2$: no general solution

Isotropic states: $\rho \rightarrow \mathbf{U} \otimes \mathbf{U}^* \rho (\mathbf{U} \otimes \mathbf{U}^*)^\dagger$

B.M. Terhal, K.H. Vollbrecht, Phys. Rev. Lett. 85, 2625 (2000)

If $\mathbf{A} \mathbf{A}^\dagger$ has only two non-zero eigenvalues
generalized concurrence

S.M. Fei, J. Jost, X.Q. Li-Jost, G.F. Wang,
Phys. Lett. A 310 (2003) 333

High dimensional construction:

S.M. Fei, X.Q. Li-Jost, Rep. Math. Phys. 53(2004)195

More non-zero eigenvalues

S.M. Fei, Z.X. Wang, H. Zhao, Phys. Lett. A 329 (2004) 414-419

Theory of Quantum Entanglement

(II)

4th Winter School on Quantum Information Sciences

Feb. 14, 2009

Lanyang Campus, Tamkang University, Yilan

Measure: Bipartite $\mathcal{H} \otimes \mathcal{H}$

Entanglement of Formation

Pure state $|\psi\rangle = \sum_{ij} a_{ij} |ij\rangle \in \mathcal{H} \otimes \mathcal{H}$

$$E(|\psi\rangle) = -\text{Tr}(\rho_1 \log_2 \rho_1) = -\text{Tr}(\rho_2 \log_2 \rho_2)$$

$$\rho_1 = \mathbf{A}\mathbf{A}^\dagger = \text{Tr}_2 |\psi\rangle\langle\psi|, \quad \rho_2 = (\mathbf{A}^\dagger \mathbf{A})^* = \text{Tr}_1 |\psi\rangle\langle\psi|, \quad (\mathbf{A})_{ij} = a_{ij}$$

Mixed
state

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \quad E(\rho) = \min \sum_i p_i E(|\psi_i\rangle)$$

Lower Bound for EoF

Partial transpose wrt subsystems

$$\rho \longrightarrow \rho^{T_1}$$

$$\langle ij | \rho^{T_1} | kl \rangle = \langle kj | \rho | il \rangle$$

$$\rho = \left(\begin{array}{cc|cc} \rho_{11} & \rho_{12} & \rho_{13} & \rho_{14} \\ \rho_{21} & \rho_{22} & \rho_{23} & \rho_{24} \\ \hline \rho_{31} & \rho_{32} & \rho_{33} & \rho_{34} \\ \rho_{41} & \rho_{42} & \rho_{43} & \rho_{44} \end{array} \right)$$

$$\rho^{T_1} = \left(\begin{array}{cc|cc} \rho_{11} & \rho_{12} & \rho_{31} & \rho_{32} \\ \rho_{21} & \rho_{22} & \rho_{41} & \rho_{42} \\ \hline \rho_{13} & \rho_{14} & \rho_{33} & \rho_{34} \\ \rho_{23} & \rho_{24} & \rho_{43} & \rho_{44} \end{array} \right)$$

Realignment:

Z: mxm block matrix with block size nxn

$$Z = \begin{pmatrix} Z_{11} & \dots & Z_{1m} \\ \vdots & \ddots & \vdots \\ Z_{m1} & \dots & Z_{mm} \end{pmatrix} \xrightarrow{\text{blue}} \tilde{Z} = \begin{pmatrix} \text{vec}(Z_{11})^T \\ \vdots \\ \text{vec}(Z_{m1})^T \\ \vdots \\ \text{vec}(Z_{1m})^T \\ \vdots \\ \text{vec}(Z_{mm})^T \end{pmatrix}$$

$$A = [a_{ij}] \xrightarrow{\text{green}} \text{vec}(A) = \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \\ \vdots \\ a_{1m} \\ \vdots \\ a_{mm} \end{pmatrix}$$

2x2 case

$$\rho = \begin{pmatrix} \rho_{11} & \rho_{12} & \rho_{13} & \rho_{14} \\ \rho_{21} & \rho_{22} & \rho_{23} & \rho_{24} \\ \rho_{31} & \rho_{32} & \rho_{33} & \rho_{34} \\ \rho_{41} & \rho_{42} & \rho_{43} & \rho_{44} \end{pmatrix} \xrightarrow{\text{blue}} \tilde{\rho} = \begin{pmatrix} \rho_{11} & \rho_{21} & \rho_{12} & \rho_{22} \\ \rho_{31} & \rho_{31} & \rho_{32} & \rho_{42} \\ \rho_{13} & \rho_{23} & \rho_{14} & \rho_{24} \\ \rho_{33} & \rho_{43} & \rho_{34} & \rho_{44} \end{pmatrix}$$

Pure state

$$|\psi\rangle = \sum_i \sqrt{\mu_i} |e_i f_i\rangle \quad \rho = |\psi\rangle\langle\psi|$$

$$\|\rho^{T_1}\| = \|\tilde{\rho}\| = \left(\sum_{k=1}^m \sqrt{\mu_k}\right)^2 = \lambda \quad \lambda \in [1, m]$$

$$R(\lambda) = \min_{\vec{\mu}} \left\{ E(\psi) \mid \left(\sum_{k=1}^m \sqrt{\mu_k}\right)^2 = \lambda \right\} = H_2[\gamma(\lambda)] + [1 - \gamma(\lambda)] \log_2(m - 1)$$

$$H_2(x) = -x \log_2 x - (1 - x) \log_2(1 - x) \quad \gamma(\lambda) = \frac{1}{m^2} [\sqrt{\lambda} + \sqrt{(m - 1)(m - \lambda)}]^2$$

Let $\mathcal{E} \leq E$ be a convex, monotonically increasing function

$$E(\rho) = \sum_i p_i E(\rho^i) \geq \sum_i p_i \mathcal{E}(\lambda^i) \geq \mathcal{E}\left(\sum_i p_i \lambda^i\right) \geq \begin{cases} \mathcal{E}(\|\rho^{T_1}\|) \\ \mathcal{E}(\|\tilde{\rho}\|) \end{cases}$$

$$\|\rho^{T_1}\| \leq \sum_i p_i \|(\rho^i)^{T_1}\| \quad \|\tilde{\rho}\| \leq \sum_i p_i \|\tilde{\rho}^i\|$$

$\mathcal{E}(\lambda) = \text{co}[R(\lambda)]$ “co” means the convex hull, which is the largest convex function that is bounded above by a given function

Theorem. — For any $m \otimes n$ ($m \leq n$) mixed quantum state ρ , the entanglement of formation $E(\rho)$ satisfies

$$E(\rho) \geq \begin{cases} 0, & \Lambda = 1, \\ H_2[\gamma(\Lambda)] + [1 - \gamma(\Lambda)] \log_2(m - 1), & \Lambda \in [1, \frac{4(m-1)}{m}], \\ \frac{\log_2(m-1)}{m-2} (\Lambda - m) + \log_2 m, & \Lambda \in [\frac{4(m-1)}{m}, m], \end{cases}$$

$$R(\Lambda) = H_2[\gamma(\Lambda)] + [1 - \gamma(\Lambda)] \log_2(m - 1) \quad \Lambda = \max(\|\rho^{T_1}\|, \|\tilde{\rho}\|)$$

$$\gamma(\Lambda) = \frac{1}{m^2} [\sqrt{\Lambda} + \sqrt{(m-1)(m-\Lambda)}]^2$$

$$H_2(x) = -x \log_2 x - (1-x) \log_2(1-x)$$

K. Chen, S. Albeverio, S.M. Fei, Phys. Rev. Lett. 95(2005)210501

S.M. Fei, X. Li-Jost, Phys. Rev. A 73(2006)024302

Lower Bound for Concurrence

$$C(|\psi\rangle) = \sqrt{2(1 - \text{Tr}\rho_1^2)}$$

Uhlmann 2000, Rungta et al, Albeverio and Fei 2001

$$\rho_1 = \text{Tr}_2(|\psi\rangle\langle\psi|) \quad C(\rho) \equiv \min_{\{p_i, |\psi_i\rangle\}} \sum_i p_i C(|\psi_i\rangle)$$

Theorem: For any $m \otimes n$ ($m \leq n$) mixed quantum state ρ , the concurrence $C(\rho)$ satisfies

$$C(\rho) \geq \sqrt{\frac{2}{m(m-1)}} \left(\max(\|\rho^{T_1}\|, \|\tilde{\rho}\|) - 1 \right)$$

K. Chen, S. Albeverio, S.M. Fei, Phys. Rev. Lett. 95(2005)040504

Example

3x3 Bound Entangled State

$$\begin{aligned} |\psi_0\rangle &= \frac{1}{\sqrt{2}}|0\rangle(|0\rangle - |1\rangle), & |\psi_1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|2\rangle \\ |\psi_2\rangle &= \frac{1}{\sqrt{2}}|2\rangle(|1\rangle - |2\rangle), & |\psi_3\rangle &= \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)|0\rangle \\ |\psi_4\rangle &= \frac{1}{3}(|0\rangle + |1\rangle + |2\rangle)(|0\rangle + |1\rangle + |2\rangle) \end{aligned}$$

$$\rho = \frac{1}{4} \left(Id - \sum_{i=0}^4 |\psi_i\rangle\langle\psi_i| \right)$$

$$\|\rho^{T_1}\| = 1$$

$$\|\mathcal{R}(\rho)\| = 1.087$$

$$C(\rho) \geq 0.05$$

the state is entangled !

Example

Isotropic states

$$\rho_F = \frac{1-F}{d^2-1} (Id - |\Psi^+\rangle\langle\Psi^+|) + F(|\Psi^+\rangle\langle\Psi^+|)$$

$$|\Psi^+\rangle \equiv \frac{1}{\sqrt{d}} \sum_{i=1}^d |ii\rangle \quad F > 1/d: \text{ entangled}$$

$$\|\rho_F^{T_1}\| = \|\rho_F\| = dF$$

Rudolph, quant-ph/0202121;

Vidal and Werner, PRA 65, 032314 (2002).

Concurrence

$$C(\rho_F) = \sqrt{\frac{2}{d(d-1)}} (dF - 1)$$

Rungta and Caves, PRA 67, 012307 (2003)

EOF

$$E(\rho_F) = \text{co}[R(dF)]$$

Terhal and Vollbrecht, PRL 85, 2625 (2000)

The lower bounds are *exact* for both concurrence and EOF !

Lower Bound for Concurrence of Tripartite States

$$|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C \quad \text{dim. } m, n, p$$

$$C(|\psi\rangle) = \sqrt{3 - \text{Tr}(\rho_A^2 + \rho_B^2 + \rho_C^2)}$$

$$C(\rho) \equiv \min_{\{p_i, |\psi_i\rangle\}} \sum_i p_i C(|\psi_i\rangle)$$

X.H. Gao, S.M. Fei and K. Wu, Phys. Rev. A 74
(Rapid Comm.)(2006)050303

Lower bound: covariance matrix approach ρ_{AB} $\mathcal{H}_d^A \otimes \mathcal{H}_d^B$.

A_k (resp. B_k) be d^2 observables on \mathcal{H}_d^A (resp. \mathcal{H}_d^B)

--- orthonormal normalized basis of the observable space

$$\{M_k\} = \{A_k \otimes I, I \otimes B_k\}$$

Covariance matrix

$$\gamma_{ij}(\rho_{AB}, \{M_k\}) = \frac{\langle M_i M_j \rangle + \langle M_j M_i \rangle}{2} - \langle M_i \rangle \langle M_j \rangle \quad \longrightarrow \quad \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}$$

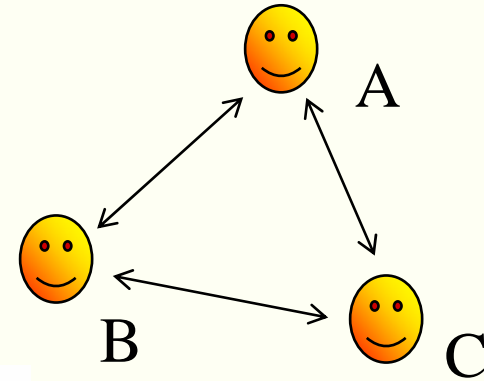
$$C_{ij} = \langle A_i \otimes B_j \rangle_{\rho_{AB}} - \langle A_i \rangle_{\rho_A} \langle B_j \rangle_{\rho_B}$$

$$C(\rho) \geq \frac{2\|C\|_{KF} - (1 - \text{Tr}\rho_A^2) - (1 - \text{Tr}\rho_B^2)}{\sqrt{2M(M-1)}} \quad \longrightarrow \quad \text{Multipartite}$$

M. Li, S.M. Fei and Z.X. Wang, J. Phys. A 41 (Fast track commun.)
(2008)202002

Monogamy relations

Pure three qubit state $|\phi\rangle_{ABC}$



Concurrence $C_{AB}^2 + C_{AC}^2 \leq C_{A(BC)}^2$

$$\rho_{AB} = \text{Tr}_C(|\phi\rangle_{ABC}\langle\phi|)$$

$$\rho_{AC} = \text{Tr}_B(|\phi\rangle_{ABC}\langle\phi|)$$

Negativity $\mathcal{N} = \|\rho^{T_A}\| - 1$

$$\mathcal{N}_{AB}^2 + \mathcal{N}_{AC}^2 \leq \mathcal{N}_{A(BC)}^2$$

High dimensional case

Y.C. Ou, H. Fan and S.M. Fei, Phys. Rev. A,
78(2008)012311.

Separability

Entanglement is invariant under local unitary tran.

$$|\Psi_2\rangle = \sum_{i,j=1}^N a_{ij} |ij\rangle \quad U_1 \otimes U_2$$

Invariants $I_\alpha = \text{Tr}(AA^\dagger)^\alpha, \quad \alpha = 1, \dots, N$

$$C_N^2 = \sqrt{\frac{N}{N-1}(I_1^2 - I_2)}$$

$$N = 2: \quad C_2^2 = C = 2|a_{11}a_{22} - a_{12}a_{21}|$$

$$C_N^2 = 0 \quad (1) \Leftrightarrow |\Psi_2\rangle \text{ separable (max.entangled)}$$

Multipartite

$$|\Psi_M\rangle = \sum_{\mathbf{i}_1, \dots, \mathbf{i}_M=1}^N \mathbf{a}_{\mathbf{i}_1, \dots, \mathbf{i}_M} |\mathbf{i}_1 \dots \mathbf{i}_M\rangle$$

Invariants: $\mathbf{I}_1 = \sum_{\mathbf{i}_1, \dots, \mathbf{i}_M=1}^N \mathbf{a}_{\mathbf{i}_1, \dots, \mathbf{i}_M} \mathbf{a}_{\mathbf{i}_1, \dots, \mathbf{i}_M}^* \equiv \mathbf{1}$

$$\mathbf{I}_{\alpha\beta} = \sum \mathbf{a}_{\alpha\beta} \mathbf{a}_{\alpha\beta'}^* \mathbf{a}_{\alpha'\beta'} \mathbf{a}_{\alpha'\beta}^*$$

$$C_N^M = \sqrt{\frac{N}{d(N-1)} (d \mathbf{I}_1^2 - \mathbf{I}_2 - \dots - \mathbf{I}_d)} \quad (d = 2^{M-1} - 1)$$

$$C_N^M = 0 \Leftrightarrow |\Psi_M\rangle \text{ separable}$$

S. Albeverio and S.M Fei, J. Opt. B: 3(2001)1

Separability of mixed states: no general criteria

$$\rho = \sum p_i |\psi_i\rangle \langle \psi_i|, \quad 0 < p_i \leq 1, \quad \sum p_i = 1$$

$\exists |\psi_i\rangle$ such that $|\psi_i\rangle$ are separable $\forall i$: ρ **Sep.**

$$\rho = \sum p_i \rho_1^i \otimes \rho_2^i \otimes \dots \otimes \rho_n^i \quad \text{Sep.}$$

a) Peres (PPT) criterion:

$$\rho \text{ separable} \implies \text{partial transpose } \rho^{T_1} \geq 0$$

Peres PRL **77**, 1413 (1996)

$$\text{Positive partial transpose (PPT): } \langle ij | \rho^{T_1} | kl \rangle = \langle kj | \rho | il \rangle$$

$$\rho = \sum p_i \rho_1^i \otimes \rho_2^i \otimes \dots \otimes \rho_n^i$$

2x2, 2x3: PPT \longleftrightarrow Separable

Horodeckis, Phys. Lett. A **223**,1 (1996)

b) Realignment:

Separable



$$\|\tilde{\rho}\| \leq 1$$

$\|M\|$: sum of all the singular values of M

Chen and Wu, Quant. Inf. Comp. 3, 193 (2003)

Rudolph, Quant. Inf. Proc. 4, 219 (2005)

Albeverio, Chen, Fei, Phys. Rev. A 68(2003)062313

c) Reduction:

$$\rho_1 = \text{Tr}_2 \rho, \rho_2 = \text{Tr}_1 \rho$$

$$\rho \text{ separable} \Rightarrow \rho_1 \otimes \mathbb{I} - \rho \geq 0, \mathbb{I} \otimes \rho_2 - \rho \geq 0$$

d) Majorization:

vector $\mathbf{x} = (x_1^\downarrow, x_2^\downarrow, \dots, x_d^\downarrow), x_1^\downarrow \geq x_2^\downarrow \geq \dots \geq x_d^\downarrow$

\mathbf{x} is majorized by \mathbf{y} : $\mathbf{x} \prec \mathbf{y}$ if

$$\sum_{j=1}^k x_j^\downarrow \leq \sum_{j=1}^k y_j^\downarrow \quad = (k=d)$$

$\mathbf{x} \prec \mathbf{y}$ if and only $\mathbf{x} = \mathbf{D}\mathbf{y}$ \mathbf{D} : stochastic matrix

$$\rho_{AB} \text{ separable} \Rightarrow \lambda_{AB} \prec \lambda_A \quad \lambda_{AB} \prec \lambda_B$$

$\lambda_{AB}, \lambda_A, \lambda_B$ eigenvalues of $\rho_{AB}, \rho_A, \rho_B$

e) Rank 2 (Necessary and sufficient condition)

ρ : a rank two state in $\mathcal{H} \otimes \mathcal{H}$,

$|\mathbf{E}_1\rangle, |\mathbf{E}_2\rangle$ Eigenvectors (non-zero)

S. Alberverio, S.M. Fei and D. Goswami, Phys. Lett. A286(2001)91

$$\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \dots \otimes \mathcal{H}_M$$

S.M. Fei, X.H. Gao, X.H. Wang, Z.X. Wang and K. Wu,
Phys. Lett. A300(2002)559;
Int. J. Quant. Inform. 1(2003)37

Multipartite Schmidt-correlated State

$$\rho = \sum_{m,n=0}^{N-1} a_{mn} |m \cdots m\rangle \langle n \cdots n|,$$

$$\sum_{m=0}^{N-1} a_{mm} = 1.$$

Fully separable \longleftrightarrow PPT

Fully separable (maximally entangled)

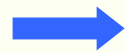


$$\|\tilde{\rho}\| = 1 (N)$$

M.J. Zhao, S.M. Fei and Z.X. Wang, Phys. Lett. A 372(2008)2552

Bell Inequalities

Separable



$$|\langle A_1 A_2 + A_1 B_2 + B_1 A_2 - B_1 B_2 \rangle| \leq 2$$

All generalized GHZ states $|\psi\rangle = \cos \alpha |0, \dots, 0\rangle + \sin \alpha |1, \dots, 1\rangle$
of many qubits violate the Bell inequality maximally

$$\frac{1}{2} |\langle \mathcal{B}_{N-1} (A_N + A'_N) + (A_N - A'_N) \rangle_{\text{LHV}}| \leq 1$$

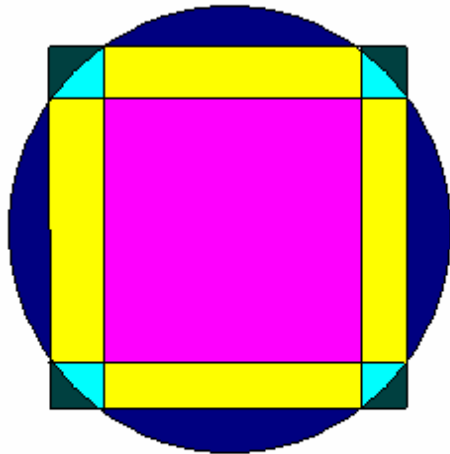
\mathcal{B}_{N-1} quantum mechanical Bell operator of
WWZB inequalities for N-1 particles

Only two measurement settings of each party

K. Chen, S. Albeverio and S.M. Fei, Phys. Rev. A (R)74(2006)050101

Tripartite

B.Z. Sun and S.M. Fei, Phys. Rev. A 74 (2006) 032335



For states ρ in S_{1-23} , S_{2-13} and S_{12-3} , respectively

$$|\langle \mathcal{D}_3^{(1)} \rangle_\rho| \leq \sqrt{2}, \quad |\langle \mathcal{D}_3^{(2)} \rangle_\rho| \leq 1, \quad |\langle \mathcal{D}_3^{(3)} \rangle_\rho| \leq 1.$$

$$|\langle \mathcal{D}_3^{(1)} \rangle_\rho| \leq 1, \quad |\langle \mathcal{D}_3^{(2)} \rangle_\rho| \leq \sqrt{2}, \quad |\langle \mathcal{D}_3^{(3)} \rangle_\rho| \leq 1$$

$$|\langle \mathcal{D}_3^{(1)} \rangle_\rho| \leq 1, \quad |\langle \mathcal{D}_3^{(2)} \rangle_\rho| \leq 1, \quad |\langle \mathcal{D}_3^{(3)} \rangle_\rho| \leq \sqrt{2}$$

$$\langle \mathcal{D}_3^{(1)} \rangle_\rho^2 + \langle \mathcal{D}_3^{(2)} \rangle_\rho^2 + \langle \mathcal{D}_3^{(3)} \rangle_\rho^2 \leq 3$$

Multi-mode states

Z.G. Li, S.M. Fei, Z.X. Wang and K. Wu, Phys. Rev. A 75(2007)012311

Classification under Local Unitary Transformations

$$\rho \Rightarrow (U_1 \otimes \dots \otimes U_M) \rho (U_1 \otimes \dots \otimes U_M)^{-1} \quad U_i U_i^\dagger = U_i^\dagger U_i = 1$$

Orbits (dimension , topology , geometry)

Equivalence criterion

$$\rho' = (U_1 \otimes U_2 \otimes \dots \otimes U_M) \rho (U_1 \otimes U_2 \otimes \dots \otimes U_M)^\dagger \quad \boxed{?}$$

Pure state:

$$|\Psi\rangle = \sum_{i,j,\dots,k} a_{ij\dots k} |ij\dots k\rangle$$

$$|\Psi'\rangle = \sum_{i,j,\dots,k} a'_{ij\dots k} |ij\dots k\rangle$$

$$|\Psi'\rangle = u_1 \otimes u_2 \otimes \dots \otimes u_M |\Psi\rangle \quad ?$$

Bipartite

$$|\Psi\rangle = \sum_{i,j} a_{ij} |ij\rangle$$

$$\mathbf{A}' = \mathbf{u}_1^t \mathbf{A} \mathbf{u}_2$$

Invariants:

$$\mathbf{I}_\alpha = \text{Tr}(\mathbf{A} \mathbf{A}^\dagger)^\alpha$$

$$\alpha = 1, 2, \dots, N$$

Multipartite:

S. Albeverio, L. Cattaneo, S.M. Fei, X.H. Wang, Rep. Math. Phys. 56 (2005)341-350; Int. J. Quant. Inform. 3 (2005) 603-609.

Z.H. Yu, X. Jost-Li, Q.Z. Li, J.T. Lv and S.M. Fei, Differential Geometry of Bipartite Quantum States, Rep. Math. Phys. 60(2007)125-133

X.H. Wang, S.M. Fei and K. Wu, J. Phys. A 41 (2008) 025305

Mixed state (bipartite): Equivalence criterion

I. Invariants under local unitary transformations

$$\rho = \sum_{i=1}^n \lambda_i |\nu_i\rangle \langle \nu_i|$$

$$|\nu_i\rangle = \sum_{k,l=1}^N a_{kl}^i |k\rangle \otimes |l\rangle, \quad a_{kl}^i \in \mathbb{C}, \quad \sum_{k,l=1}^N a_{kl}^i a_{kl}^{i*} = 1 \quad (A_i)_{kl} = a_{kl}^i$$

$$\rho_i = \text{Tr}_2 |\nu_i\rangle \langle \nu_i| = A_i A_i^\dagger, \quad \theta_i = (\text{Tr}_1 |\nu_i\rangle \langle \nu_i|)^* = A_i^\dagger A_i$$

$$\Omega(\rho)_{ij} = \text{Tr}(\rho_i \rho_j), \quad \Theta(\rho)_{ij} = \text{Tr}(\theta_i \theta_j).$$

Generic

$$\det(\Omega(\rho)) \neq 0 \quad \det(\Theta(\rho)) \neq 0$$

$$X(\rho)_{ijk} = \text{Tr}(\rho_i \rho_j \rho_k) \quad Y(\rho)_{ijk} = \text{Tr}(\theta_i \theta_j \theta_k)$$

Theorem: ρ Equiv. L.U. 

$$\mathbf{J}^s(\rho) = \text{Tr}_2(\text{Tr}_1 \rho^s), \quad s = 1, \dots, N^2$$

$$\Omega(\rho), \quad \Theta(\rho), \quad \mathbf{X}(\rho), \quad \mathbf{Y}(\rho)$$

S. Albeverio, S.M. Fei, P. Parashar, W.L. Yang,
Phys. Rev. A 68 (Rapid Comm.) (2003) 010303

Not full rank B.Z. Sun, S.M. Fei, X.Q. Li-Jost, Z.X. Wang, J. Phys. A39 (2006) L43

If ρ_1, θ_1 each of its eigenvalues has multiplicity one

S. Albeverio, S.M. Fei, D. Goswami, Phys. Lett. A 340(2005)37;
J. Phys. A 40(2007)11113

II. Matrix tensor product decomposition approach

$$\rho = \mathbf{X}\Lambda\mathbf{X}^\dagger, \quad \rho' = \mathbf{Y}\Lambda\mathbf{Y}^\dagger \quad \Lambda = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_{MN})$$

[Theorem]. If ρ and ρ' are not degenerate, they are equivalent under local unitary transformations if and only if $V = XDY^\dagger$, $D = \text{diag}(e^{i\theta_1}, e^{i\theta_2}, \dots, e^{i\theta_{MN}})$, contains a unitary tensor decomposable element for some $\theta_i \in \mathbb{R}$, $\text{rank}(\tilde{V}) = 1$.

$$(V = V_1 \otimes V_2 \quad \text{iff} \quad \text{rank}(\tilde{V}) = 1)$$

S.M. Fei, N.H. Jing, Phys. Lett. A 342(2005)77

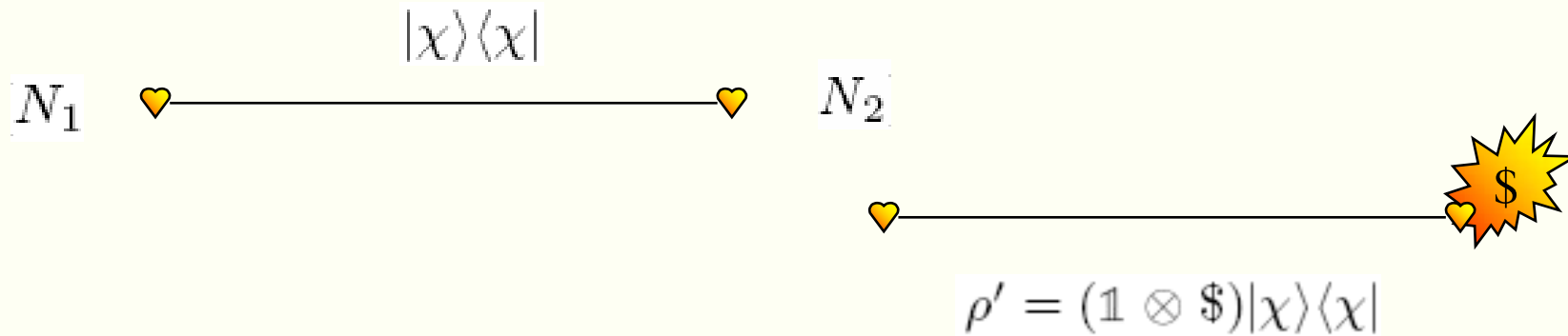
X.H. Gao, S. Albeverio, S.M. Fei, Z.X. Wang, Commun. Theor. Phys. 45 (2006) 267-270.

SLOCC

$$\rho_2 = (P \otimes Q)\rho_1(P \otimes Q)^\dagger$$

Evolution of quantum entanglement:

Bipartite system with one subsystem undergoes a noisy channel



$$C(\rho') \sim C[|\chi\rangle] ?$$

$$C[|\chi\rangle] = \sqrt{\sum_{\alpha=1}^{N_1(N_1-1)/2} \sum_{\beta=1}^{N_2(N_2-1)/2} |C_{\alpha\beta}|^2}$$

$$C_{\alpha\beta} = \langle\chi|(L_{\alpha} \otimes L_{\beta})|\chi^*\rangle$$

$$L_{\alpha}, \alpha = 1, \dots, N_1(N_1 - 1)/2$$

$$L_{\beta}, \beta = 1, \dots, N_2(N_2 - 1)/2$$

generators of $SO(N_1)$ and $SO(N_2)$ resp.

$$|\chi\rangle = (M_\chi \otimes \mathbb{1})|\phi\rangle$$

$$M_\chi = \sqrt{N_2} \sum_{i=1}^{N_1} \sum_{j=1}^{N_2} A_{ij} |i\rangle \langle j|$$

$$|\phi\rangle = \sum_{n=1}^{N_2} |n\rangle \otimes |n\rangle / \sqrt{N_2}$$

$$\rho' = (M_\chi \otimes \mathbb{1}) \rho_\$ (M_\chi^\dagger \otimes \mathbb{1})$$

$$\rho\$ = (\mathbb{1} \otimes \$) |\phi\rangle \langle \phi|$$

If $\rho\$$ is a pure state (e.g. channel \$ is unitary or stochastic quantum operation given by a local filter)

$$C[\rho'] = \sqrt{\sum_{\alpha=1}^{N_1(N_1-1)/2} \sum_{\beta=1}^{N_2(N_2-1)/2} |C'_{\alpha\beta}|^2}$$

$$C'_{\alpha\beta} = \frac{N_2}{2} \sum_{\gamma=1}^{N_2(N_2-1)/2} C_{\alpha\gamma}[|\chi\rangle] C_{\gamma\beta}[\rho\$_']$$

For $N_1 \otimes 2$ system: $C[\rho'] = C[|\chi\rangle] C[\rho\$]$

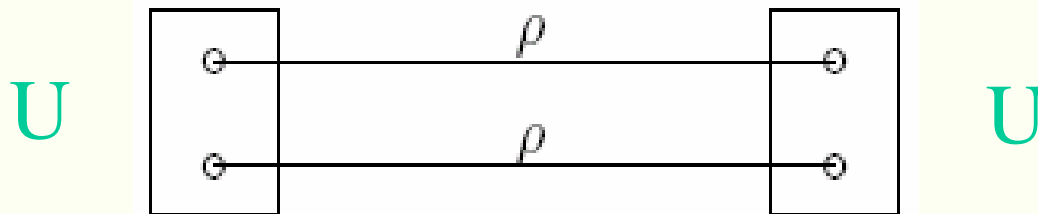
(2x2: Nature Physics 4, 99 (2008))

For general mixed initial state:

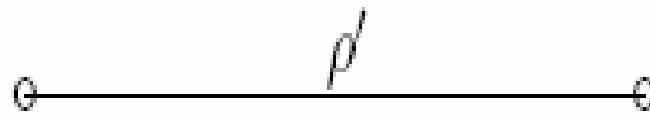
$$C[(\mathbb{1} \otimes \$)\rho_0] \leq \frac{N_2}{2} C(\rho_0) C[\rho\$]$$

Z.G. Li, S.M. Fei, Z.D. Wang and W.M. Liu, Phys. Rev. A, 79 (2009) 024303

Distillation:



Measurement

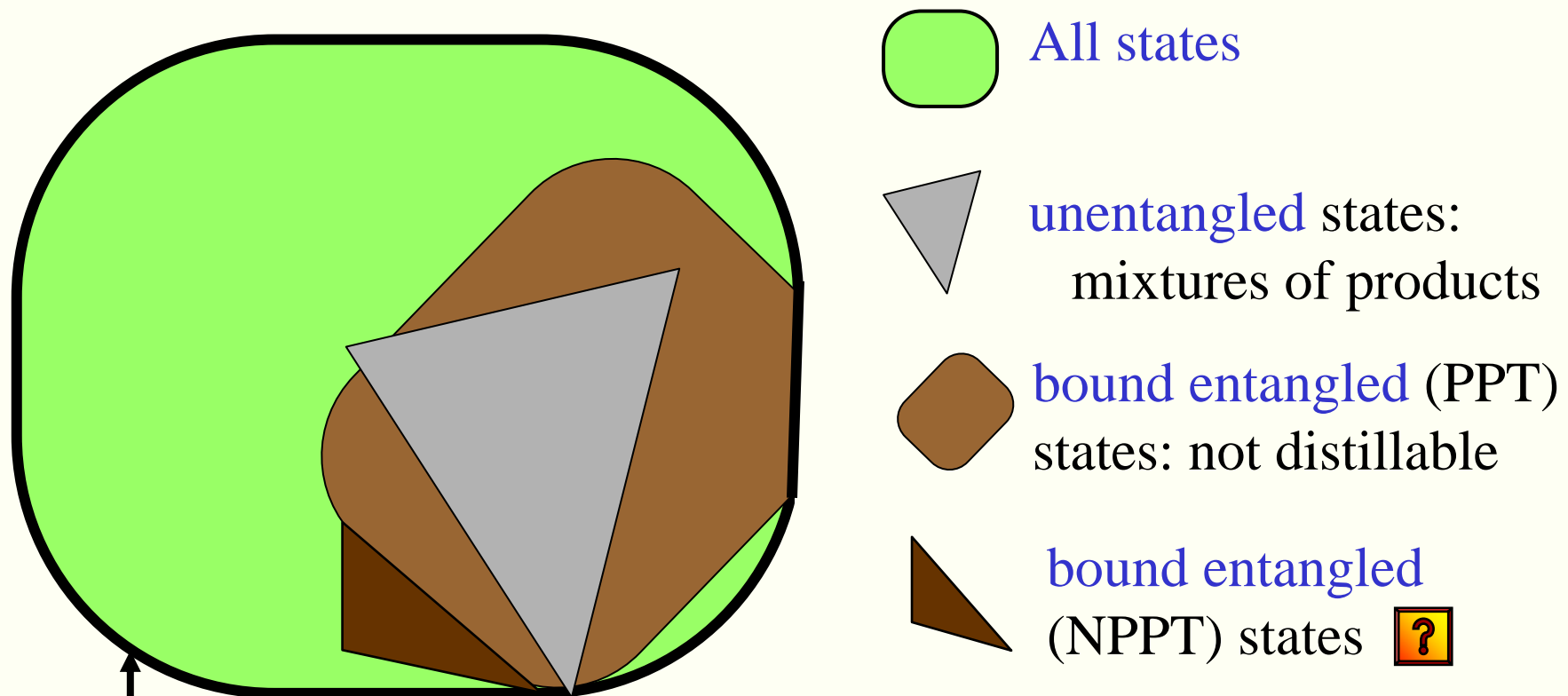


Entangled, but not distillable: Bound entangled

All PPT entangled states are bound entangled!

Entanglement

No Classical
Counterpart



pure states

Much remains to be clarified!

S.M. Fei, X.Q. Li-Jost, B.Z. Sun, Phys. Lett. A 352 (2006) 321

Thanks!