Methods of Quantum Information Processing

(with an emphasis on optical implementations)

Adam Miranowicz
e-mail: miran@amu.edu.pl
http://zon8.physd.amu.edu.pl/∼miran

summer semester 2008

Keywords

- quantum logic gates
- quantum entanglement
- quantum cryptography
- quantum teleportation
- quantum algorithms
- quantum error correction
- quantum tomography
- solid-state implementations of quantum computing

Basic textbook:

1. *Quantum Computation and Quantum Information*
   by Michael A. Nielsen and Isaac L. Chuang (Cambridge, 2000)

Review articles on quantum-optical computing:

1. *Linear optical quantum computing*,
   P. Kok, W.J. Munro, K. Nemoto, T.C. Ralph, J. P. Dowling, G.J. Milburn,
   free downloads at http://arxiv.org/quant-ph/0512071.
2. *Linear optics quantum computation: an overview,* C.R. Myers, R. Laflamme,
   free downloads at http://arxiv.org/quant-ph/0512104.
3. *Quantum optical systems for the implementation of quantum information processing*, T.C. Ralph, free downloads at http://arxiv.org/quant-ph/0609038.
4. *Quantum mechanical description of linear optics*
   J. Skaar, J.C.G. Escartin, H. Landro,
   Am. J. Phys. **72**, 1385-1391 (2005).

Other Textbooks on Quantum Computing

1. *Quantum Computing* by Joachim Stolze, Dieter Suter
2. *Approaching Quantum Computing*
   by Dan C. Marinescu, Gabriela M. Marinescu
3. *Introduction to Quantum Computation and Information*
   edited by Hoi-Kwong Lo, Tim Spiller, Sandu Popescu
4. *Quantum Computing* by Mika Hirvensalo
5. *Explorations in Quantum Computing*
   by Colin P. Williams, Scott H. Clearwater
6. *Quantum Information Processing*
   edited by Gerd Leuchs, Thomas Beth
7. *Quantum Computing* by Josef Gruska
8. *Quantum Computing and Communications*
   by Sandor Imre, Ferenc Balazs

9. *An Introduction to Quantum Computing Algorithms*
by Arthur O. Pittenger

10. *Quantum Computing* by M. Nakahara, Tetsuo Ohmi

11. *Principles of Quantum Computation and Information* - *Vol.1*
by Giuliano Benenti, Giulio Casati, Giuliano Strini

12. *Principles of Quantum Computation And Information: Basic Tools And Special Topics* by Giuliano Benenti

13. *Quantum Optics for Quantum Information Processing*
edited by Paolo Mataloni

14. *Lectures on Quantum Information*
edited by Dagmar Bruß, Gerd Leuchs

15. *A Short Introduction to Quantum Information and Quantum Computation*
by Michel Le Bellac

16. *Quantum Computation and Quantum Communication* by Mladen Pavicic

17. *Scalable Quantum Computers: Paving the Way to Realization*
edited by Samuel L. Braunstein, Hoi-Kwong Lo

18. *Fundamentals of Quantum Information* edited by Dieter Heiss

19. *Experimental Aspects of Quantum Computing*
edited by Henry O. Everitt

20. *Quantum Computing: Where Do We Want to Go Tomorrow*
edited by Samuel L. Braunstein

21. *Quantum Information* by Gernot Alber et al.

22. *The Physics of Quantum Information*
edited by Dirk Bouwmeester, Artur K. Ekert, Anton Zeilinger

23. *Temple of Quantum Computing* by Riley T. Perry
(free downloads at www.toqc.com)

24. *Quantum Computation* edited by Samuel J. Lomonaco, Jr.
(free downloads at www.cs.umbc.edu/∼lomonaco)

25. *Lecture Notes for Physics: Quantum Information and Computation*
by John Preskill
(free downloads at www.theory.caltech.edu/people/preskill/ph229).

a two-level atom/system

$|g\rangle$ - ground state

$|e\rangle$ - excited state

– physical notation

$$|g\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad |e\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

– information notation

$$|g\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |e\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

- **Pauli matrices**

$$\hat{\sigma}_x \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \hat{\sigma}_y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \hat{\sigma}_z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

- rasing ($\hat{\sigma}^\dagger$) and lowering ($\hat{\sigma}$) energy operators,

= atomic-transition operators

$$\hat{\sigma}^\dagger = \frac{\hat{\sigma}_x + i\hat{\sigma}_y}{2} = |e\rangle\langle g|, \quad \hat{\sigma} = \frac{\hat{\sigma}_x - i\hat{\sigma}_y}{2} = |g\rangle\langle e|, \quad \hat{\sigma}_z = \hat{\sigma}^\dagger\hat{\sigma} - \hat{\sigma}\hat{\sigma}^\dagger = |e\rangle\langle e| - |g\rangle\langle g|$$

qubit = quantum bit

- the smallest unit of quantum information
- physically realized by a 2-level quantum system
whose two basic states are conventionally labelled $|0\rangle$ and $|1\rangle$
- By contrast to classical bits,
a qubit can be in an arbitrary superposition of '0' and '1':

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

with normalization condition $|\alpha|^2 + |\beta|^2 = 1.$

- **matrix representation** of qubit states:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

qudits = qunits

d-dimensional quantum states, generalized qubits

$$|\psi\rangle_d = \sum_{n=0}^{d-1} c_n |n\rangle$$

with normalization condition

$$\sum_{n=0}^{d-1} |c_n|^2 = 1$$

special cases

2D qudit = qubit

3D qudit = qutrit

4D qudit = (qu)quartit = ququart

5D qudit = (qu)quintit

...

optical qudits are spanned in d-dimensional Fock space

quantum (logic) gates

basic quantum circuits
operating on a small number of qubits

they are for quantum computers what
classical logic gates are in conventional computers

Pauli $\hat{X}$ gate = quantum NOT gate = bit flip

$$\hat{X} \equiv \hat{\sigma}_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\hat{X}|k\rangle = |1 \oplus k\rangle, \quad k = 0, 1$$

examples

$$\hat{X}|1\rangle = \hat{X}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

$$\hat{X}(\alpha|0\rangle + \beta|1\rangle) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix} = \beta|0\rangle + \alpha|1\rangle$$

Pauli $\hat{Z}$ gate = phase flip

$$\hat{Z} \equiv \hat{\sigma}_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\hat{Z}|k\rangle = (-1)^k|k\rangle, \quad k = 0, 1$$

example

$$\hat{Z}(\alpha|0\rangle + \beta|1\rangle) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ -\beta \end{bmatrix} = \alpha|0\rangle - \beta|1\rangle$$

Pauli $\hat{Y}$ gate = phase flip + bit flip

$$\hat{Y} \equiv \hat{\sigma}_X = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$\hat{Y}|k\rangle = i(-1)^k|1 \oplus k\rangle, \quad k = 0, 1$$

example

$$\hat{Y}(\alpha|0\rangle + \beta|1\rangle) = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = i\begin{bmatrix} -\beta \\ \alpha \end{bmatrix} = -i\beta|0\rangle + i\alpha|1\rangle$$

phase gate

$$\hat{S} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

Hadamard gate

$$\hat{H} = \tfrac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

examples

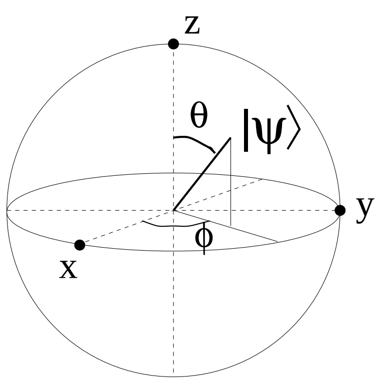
$$\hat{H}|0\rangle = \tfrac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \tfrac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \equiv |+\rangle$$

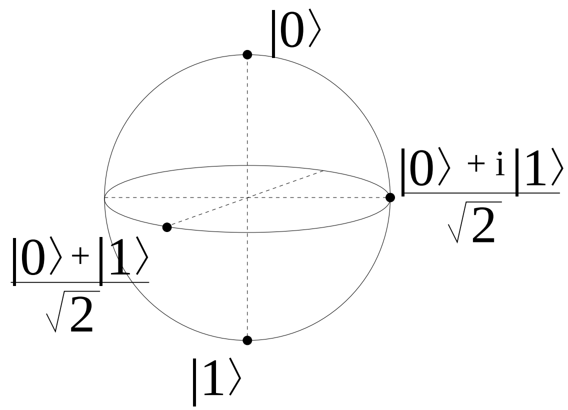
$$\hat{H}|1\rangle = \tfrac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \tfrac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \equiv |-\rangle$$

$$\hat{H}|+\rangle = \tfrac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\tfrac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \tfrac{1}{2}\begin{bmatrix} 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

$$\hat{H}|-\rangle = |1\rangle$$

Bloch representation/sphere





$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

qubit rotations

- **rotations on Bloch sphere**

$$\begin{aligned}\hat{R}_{\mathbf{n}}(2\theta) &\equiv \exp\left(-i\theta\mathbf{n}\cdot\hat{\boldsymbol{\sigma}}\ \right)\\ &= \hat{\sigma}_I\cos\theta - i\mathbf{n}\cdot\hat{\boldsymbol{\sigma}}\sin\theta\\ &= \hat{\sigma}_I\cos\theta - i(n_x\hat{\sigma}_x + n_y\hat{\sigma}_y + n_z\hat{\sigma}_z)\sin\theta,\end{aligned}$$

- **Pauli matrices** (and identity matrix)

$$\hat{\sigma}_x \equiv \begin{bmatrix} 0 & 1\\ 1 & 0\end{bmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|,$$

$$\hat{\sigma}_y \equiv \begin{bmatrix} 0 & -i\\ i & 0\end{bmatrix} = -i|0\rangle\langle 1| + i|1\rangle\langle 0|,$$

$$\hat{\sigma}_z \equiv \begin{bmatrix} 1 & 0\\ 0 & -1\end{bmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|,$$

$$\hat{\sigma}_I \equiv \hat{I} = \begin{bmatrix} 1 & 0\\ 0 & 1\end{bmatrix} = |0\rangle\langle 0| + |1\rangle\langle 1|$$

$$\hat{\boldsymbol{\sigma}} = (\hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z)$$

- **rotations about $k = x, y, z$ axes** – special cases of $\hat{R}_{\mathbf{n}}(\theta)$

$$\hat{R}_k(\theta) = \exp\left(-i\tfrac{\theta}{2}\hat{\sigma}_k\right) = \hat{\sigma}_I\cos\tfrac{\theta}{2} - i\hat{\sigma}_k\sin\tfrac{\theta}{2}$$

or explicitly

$$\hat{X}(\theta) \equiv \hat{R}_x(\theta) = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2}\\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{bmatrix}$$

$$\hat{Y}(\theta) \equiv \hat{R}_y(\theta) = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2}\\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{bmatrix}$$

$$\hat{Z}(\theta) \equiv \hat{R}_z(\theta) = \begin{bmatrix} e^{-i\theta/2} & 0\\ 0 & e^{i\theta/2}\end{bmatrix}$$

- **Do we need all XYZ-rotations? No!**

e.g. we can omit Z-rotation as

$$\hat{Z}(\theta) = \hat{X}(\tfrac{\pi}{2})\hat{Y}(\theta)\hat{X}(-\tfrac{\pi}{2}) = \hat{Y}(\tfrac{\pi}{2})\hat{X}(-\theta)\hat{Y}(-\tfrac{\pi}{2}).$$

- **any single-qubit gate**

can be written as a decomposition ZY (or, equivalently, XY or XZ)

$$\hat{U} = e^{i\alpha}\hat{R}_{\mathbf{n}}(\theta) = e^{i\alpha}\hat{Z}(\theta_1)\hat{Y}(\theta_2)\hat{Z}(\theta_3)$$

Bloch vector (Pauli vector) for a qubit

- **in any pure state**

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

we have

$$\mathbf{r}_{\text{Bloch}} \equiv (r_x, r_y, r_z) = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$$

- **in any mixed state**

$$\begin{aligned}\hat{\rho} &= \begin{bmatrix} \rho_{11} & \rho_{12}\\ \rho_{21} & \rho_{22}\end{bmatrix}\\ &= \tfrac{1}{2}(\hat{\sigma}_I + \mathbf{r}_{\text{Bloch}}\cdot\hat{\boldsymbol{\sigma}}) \quad \text{(so-called } \textbf{Pauli basis}\text{)}\\ &= \tfrac{1}{2}(\hat{\sigma}_I + r_x\hat{\sigma}_x + r_y\hat{\sigma}_y + r_z\hat{\sigma}_z)\end{aligned}$$

we get

$$\begin{aligned}\mathbf{r}_{\text{Bloch}} &= \langle\hat{\boldsymbol{\sigma}}\rangle\\ &= \mathrm{Tr}[\hat{\rho}\hat{\boldsymbol{\sigma}}]\\ &= (\mathrm{Tr}[\hat{\rho}\hat{\sigma}_x], \mathrm{Tr}[\hat{\rho}\hat{\sigma}_y], \mathrm{Tr}[\hat{\rho}\hat{\sigma}_z])\\ &= (2\mathrm{Re}\rho_{21}, 2\mathrm{Im}\rho_{21}, \rho_{11} - \rho_{22})\end{aligned}$$

- **Exemplary proof**:

$$\begin{aligned}\mathrm{Tr}[\hat\rho\hat\sigma_x] &= \mathrm{Tr}[\tfrac{1}{2}(\hat\sigma_I + r_x\hat\sigma_x + r_y\hat\sigma_y + r_z\hat\sigma_z)\hat\sigma_x] \\ &= \tfrac{1}{2}\mathrm{Tr}[\hat\sigma_I\hat\sigma_x + r_x\hat\sigma_x\hat\sigma_x + r_y\hat\sigma_y\hat\sigma_x + r_z\hat\sigma_z\hat\sigma_x] \\ &= \tfrac{1}{2}(\mathrm{Tr}[\hat\sigma_I\hat\sigma_x] + r_x\mathrm{Tr}[\hat\sigma_x\hat\sigma_x] + r_y\mathrm{Tr}[\hat\sigma_y\hat\sigma_x] + r_z\mathrm{Tr}[\hat\sigma_z\hat\sigma_x]) \\ &= \tfrac{1}{2}(\mathrm{Tr}[\hat\sigma_x] + r_x\mathrm{Tr}[\hat\sigma_I] + r_y\mathrm{Tr}[-i\hat\sigma_z] + r_z\mathrm{Tr}[i\hat\sigma_y]) \\ &= \tfrac{1}{2}(0 + 2r_x + 0 + 0) \\ &= r_x\end{aligned}$$

moreover

$$\begin{aligned}\mathrm{Tr}[\hat\rho\hat\sigma_x] &= \mathrm{Tr}\left(\begin{bmatrix}\rho_{11} & \rho_{12}\\ \rho_{21} & \rho_{22}\end{bmatrix}\cdot\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\right) \\ &= \mathrm{Tr}\begin{bmatrix}\rho_{12} & \rho_{11}\\ \rho_{22} & \rho_{21}\end{bmatrix} \\ &= \rho_{12} + \rho_{21} = \rho_{21}^* + \rho_{21} = 2\mathrm{Re}\,\rho_{21} = 2\mathrm{Re}\,\rho_{12}\end{aligned}$$

- **Properties**:

$|\mathbf{r}_{\mathrm{Bloch}}| = 1$ – for pure state,
$|\mathbf{r}_{\mathrm{Bloch}}| < 1$ – for mixed state

Kronecker tensor product

let

$$A = \begin{bmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix}, \quad B = \begin{bmatrix}b_{11} & b_{12}\\ b_{21} & b_{22}\end{bmatrix}$$

then

$$A\otimes B = \begin{bmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix}\otimes\begin{bmatrix}b_{11} & b_{12}\\ b_{21} & b_{22}\end{bmatrix}$$

$$= \begin{bmatrix} a_{11}\begin{bmatrix}b_{11} & b_{12}\\ b_{21} & b_{22}\end{bmatrix}, & a_{12}\begin{bmatrix}b_{11} & b_{12}\\ b_{21} & b_{22}\end{bmatrix} \\ a_{21}\begin{bmatrix}b_{11} & b_{12}\\ b_{21} & b_{22}\end{bmatrix}, & a_{22}\begin{bmatrix}b_{11} & b_{12}\\ b_{21} & b_{22}\end{bmatrix}\end{bmatrix}$$

$$= \begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{11}b_{12} & a_{22}b_{11} & a_{12}b_{12} \\ a_{21}b_{21} & a_{11}b_{22} & a_{22}b_{21} & a_{12}b_{22}\end{bmatrix}$$

two-qubit pure states

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

notation of two-mode states

$$|\psi\rangle = |\psi'\rangle_A \otimes |\psi''\rangle_B \equiv |\psi'\rangle_A|\psi''\rangle_B \equiv |\psi'\psi''\rangle_{AB} \equiv |\psi'\psi''\rangle$$

matrix representation

$$|00\rangle = \begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix},$$

$$|01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}, |10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix},$$

matrix representation

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

$$= \alpha\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix} + \beta\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix} + \gamma\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix} + \delta\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}$$

$$= \alpha\begin{bmatrix}1\\0\\0\\0\end{bmatrix} + \beta\begin{bmatrix}0\\1\\0\\0\end{bmatrix} + \gamma\begin{bmatrix}0\\0\\1\\0\end{bmatrix} + \delta\begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

$$= \begin{bmatrix}\alpha\\ \beta\\ \gamma\\ \delta\end{bmatrix}$$

Universal set of gates for quantum computing

- rotations of single qubits
- any nontrivial two-qubit gate (e.g., CNOT, NS, CZ)

CZ and CNOT gates

CZ = controlled phase gate (CPhase)

= controlled sign gate (CSign)

control bit	target bit	CZ	CNOT
$\|0\rangle$	$\|0\rangle$	$\|0,0\rangle$	$\|0,0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0,1\rangle$	$\|0,1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1,0\rangle$	$\|1,1\rangle$
$\|1\rangle$	$\|1\rangle$	$-\|1,1\rangle$	$\|1,0\rangle$

or equivalently

$$\mathrm{CZ}:|q_1,q_2\rangle \;\to\; (-1)^{q_1 q_2}|q_1,q_2\rangle$$

$$\mathrm{CNOT}:|q_1,q_2\rangle \;\to\; |q_1,q_1\oplus q_2\rangle$$

where $q_k = 0,1$ and $q_1 \oplus q_2 = \mod(q_1+q_2,2)$.

Introduction to quantum-optical cryptography

basic cryptographic terms

Vernam protocol

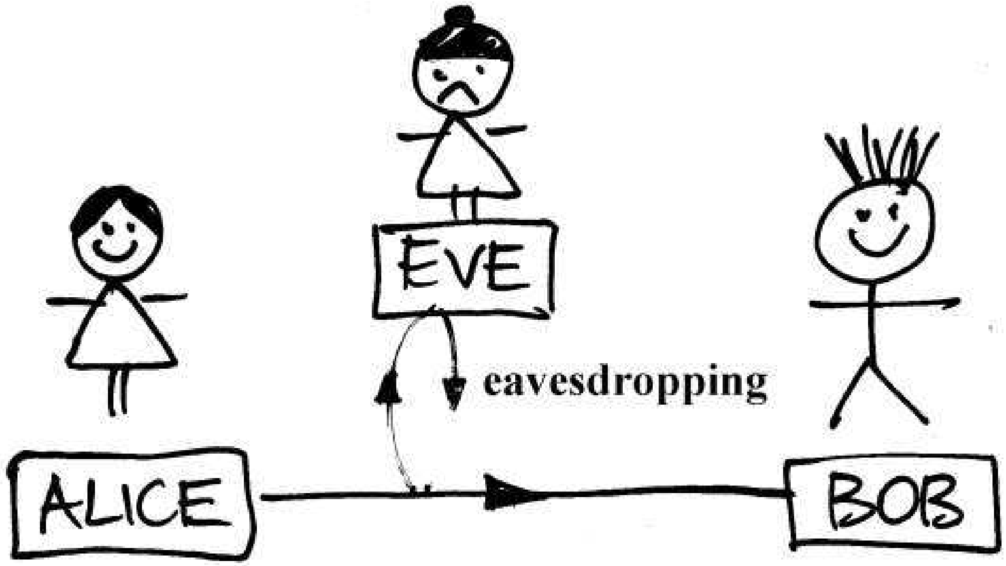
quantum key distribution

BB84 protocol

security and no-cloning theorem

a note

quantum cryptography is, probably,
the most important application of quantum optics nowadays



basic cryptographic terms (I)

Plaintext

a string of numbers (letters) of our digital alphabet

Encryption

a computation which is usually quick and easy to perform

Decryption

quick and easy computation is only when some additional information is available
otherwise it is very long and time consuming computation

Key

a set of instructions to encrypt and decrypt a message,
e.g., randomly chosen series of numbers known
to Alice and Bob only

basic cryptographic terms (II)

cipher
1. encryption scheme
   = cryptographic algorithm
   = math. function for encryption and decryption
   using a key
2. encrypted message = ciphertext = cryptogram

cryptosystem = cryptographic algorithm
+ all keys + all cryptograms + all cleartexts

cryptology = cryptography + cryptoanalysis

exemplary digital alphabet

01 A	02 Ą	03 B	04 C	05 Ć
06 D	07 E	08 Ę	09 F	10 G
11 H	12 I	13 J	14 K	15 L
16 Ł	17 M	18 N	19 Ń	20 O
21 Ó	22 P	23 Q	24 R	25 S
26 Ś	27 T	28 U	29 V	30 W
31 X	32 Y	33 Z	34 Ż	35 Ź
36 _	37 -	38 ?	39 ,	40 .

cleartext: A D A M
plaintext: 01060117

symmetric algorithms

cleartext
↓
plaintext
↓ Encryption using key k
ciphertext ↓ key distribution
↓ Decryption using the same key k
plaintext
↓
cleartext

asymmetric algorithms = public-key algorithms

cleartext
↓
plaintext
↓ Encryption using key k_1 (public key)
ciphertext
↓ Decryption using key k_2 (private key)
plaintext
↓
cleartext

first paper on quantum cryptography

1983 (1970 !)

by Stephen Wiesner

first description of quantum coding

- How to print banknotes, which cannot be counterfeited
- How to combine two messages such that by reading one of them, the other is automatically destroyed

eavesdropping on classical system

two steps:

1. Eve makes a copy (clone) of the information carrier
2. and reads information from the copy

passive monitoring of classical information is possible

eavesdropping on quantum system

Eve cannot clone the information as she does not know the state of the „carrier” of information

monitoring disturbs quantum information

no-cloning theorem

It is impossible to make a copy of an unknown quantum state.

[Wootters, Żurek and Dieks (1982)]

This is one of the most fundamental theorems of quantum mechanics and quantum information

- quantum cryptography is secure
- superluminal communication by using entangled states is impossible
- quantum teleportation seems to be also impossible ???

Heisenberg uncertainty principle

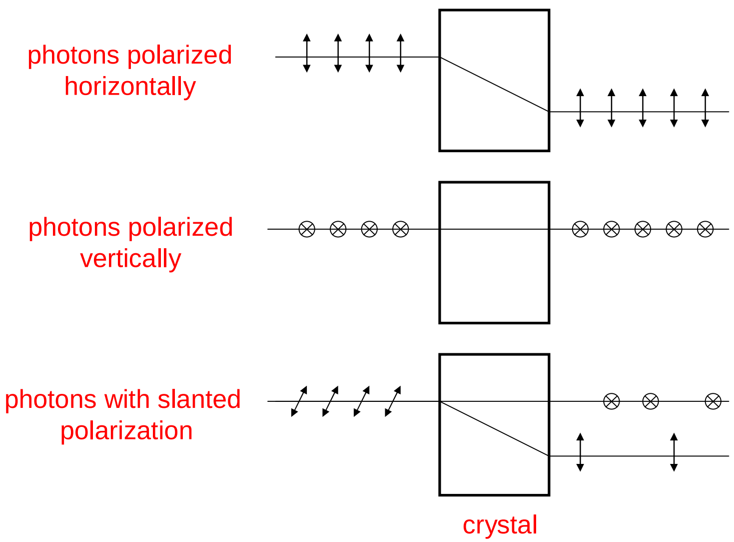
➡ passive eavesdropping is impossible

1. It is possible to disinguish two polarizations at $\alpha = 0^o$ and 90^o
2. It is possible to disinguish two polarizations at $\alpha = 45^o$ and 135^o
3. It is possible to change quickly polarization (e.g. by Pockels cell)
4. BUT it is impossible to measure simultaneously four polarizations at $\alpha=0^o, 90^o, 45^o, 135^o$

a birefringent crystal

for example Iceland spar (calcite) or BBO

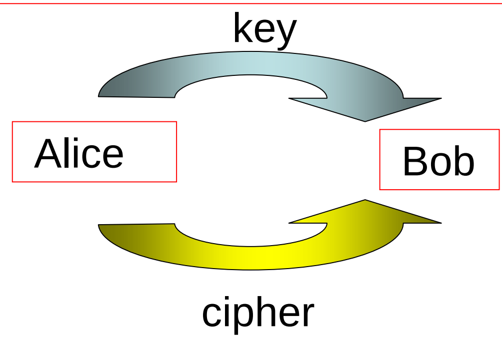
enables discrimination of polarizations perpendicular to each other



scheme of Bennett & Brassard (1984) = BB84 protocol

two channels:

1. quantum private for key distribution
2. classical public (e.g. internet) for cipher transmission



BB84

2 stages:

1. quantum key distribution
2. classical encryption e.g.Vernam protocol

PROBLEM:

How can Alice and Bob establish their common key?

Vernam cipher/protocol (1918)
= Che Guevara cipher
= one-time pad

algorithm

addition modulo N (e.g. 40)

key

1. a series of randomly chosen number
2. physically safe
3. not shorter than the length of message

Vernam cipher is unbreakable
if the above conditions are satisfied.

example of Vernam protocol

Key is a series of random numbers:

```
16 19 24 03 13 24 07 25 10 23 20 19 22 38 14 16 12 16 11
```

cleartext:

```
A  D  A  M  _  M  I  R  A  N  O  W  I  C  Z  _  Z  O  N
```

plaintext:

```
01 06 01 17 36 17 12 24 01 18 20 30 12 04 33 36 33 20 18
-----------------------------------------------------------
```

Sum:

```
17 25 25 20 49 41 19 49 11 41 40 49 34 42 47 52 45 36 29
```

Sum mod (40):

```
17 25 25 20 09 01 19 09 11 01 40 09 34 02 07 12 05 36 29
```

cipher

BB84 (1)

convention

| ($\alpha = 90^o$) and \ ($\alpha = 135^o$) => bit 1

\- ($\alpha = 0^o$) and / ($\alpha = 45^o$) => bit 0

1. Alice sends photons

```
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
+  +  x  +  x  x  x  +  x  +  +  x  x  +  x   base
|  -  \  |  /  /  \  |  /  -  |  \  \  -  \   polarization
1  0  1  1  0  0  1  1  0  0  1  1  1  0  1   bit
```

BB84 (2)

2. Bob randomly chooses the measurement base

```
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
|  -  \  |  /  /  \  |  /  -  |  \  \  -  \   polarization of Alice's photons

+  x  +  +  x  x  +  +  x  +  x  x  +  +  x   Bob's base
|  \  -  |  /  /  |  |  /  -  /  \  -  -  \   polarization of photons after measurement
```

BB84 (3)

3. Alice and Bob publicly compare bases

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
Alice's bases	+	+	x	+	x	x	x	+	x	+	+	x	x	+	x
Bob's bases	+	x	+	+	x	x	+	+	x	+	x	x	+	+	x
test	y	n	n	y	y	y	n	y	y	y	n	y	n	y	y

BB84 (4)

4. Alice and Bob keep only those results obtained for the same bases

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
Alice's series	1	.	.	1	0	0	.	1	0	0	.	1	.	0	1
Bob's series	1	.	.	1	0	0	.	1	0	0	.	1	.	0	1

BB84 (5)

5. Alice and Bob publicly check results for some photons say 1, 5, 10, 14th.

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
Alice's series	1	.	.	1	0	0	.	1	0	0	.	1	.	0	1
Bob's series	1	.	.	1	0	0	.	1	0	0	.	1	.	0	1
	OK				OK					OK				OK	

BB84 (6)

6. They reject the bits for the tested photons

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
Alice's series	*	.	.	1	*	0	.	1	0	*	.	1	.	*	1
Bob's series	*	.	.	1	*	0	.	1	0	*	.	1	.	*	1

thus the secret key known only to Alice and Bob is

1 0 1 0 1 1

Test of agreement

1. Alice and Bob compare arbitrary subset of their data.
   (Obviously, the tested subset is then not used for the key.)
2. Methods:
   (a) **testing bit after bit**
   (b) **testing parity**
   e.g 20 times $\Rightarrow (1/2)^{20} \sim 0.000001$
3. If the subset reveals eavesdropping, all the data of Alice and Bob are rejected and the BB84 protocol is repeated.
4. **privacy amplification**
   via e.g. Bennett-Brassard-Robert, Ekert et al. or Horodecki et al. schemes

strategy of eavesdropping

	Alice	Eve	Bob	
	+	+	+	
		1/2		= 1/2
	Alice	Eve	Bob	
Base	+	x	+	
Polarization	|	/	|	
Probability		1/2*1/2	1/2	= 1/8
	Alice	Eve	Bob	
	+	x	+	
	|	\	|	
		1/2*1/2	1/2	= 1/8

Eve's strategy of eavesdropping (I)

Eve measures a photon sent by Alice
(e.g. by using another calcite crystal)

QUESTION

What is the probability that a single photon was measured by Eve, but Alice and Bob have not realized it?

ANSWER

$P = \frac{3}{4}$

the probability is surprisingly high!

security of BB84

for 1 photon P_1=3/4
so for n photons $P_n=(3/4)^n$
e.g.
$P_2=(3/4)^2 \sim 0.56$
$P_{10}=(3/4)^{10} \sim 0.06$
$P_{20}=(3/4)^{20} \sim 0.003$
$P_{100}=(3/4)^{100} \sim 10^{-13}$
and for 1000 photons
$P_{1000}=(3/4)^{1000} \sim 10^{-125}$

famous protocols of quantum key distribution

1984 Bennett-Brassard protocol (BB84)

1991 Ekert protocol based Bell's inequality (E91)

1992 Bennett-Brassard-Mermin protocol
a la Ekert protocol but without Bell's inequality

1992 Bennett protocol using any two
nonorthogonal states (B92)

2004 Englert et al. protocol claimed to be the
most efficient nowadays (Singapore protocol)

information is physical

„Information is inevitably tied to
a physical representation and
therefore to restrictions and possibilities
related to the laws of physics"
[R. Landauer]

classical cryptography is
a branch of mathematics

quantum cryptography is
a branch of physics
- mainly of quantum optics

quantum algorithms and cryptography

1985 Deutsch (Deutsch-Jozsa / DJ) algorithm:
How to see both sides of a coin simultaneously?

1994 Shor algorithm for number factorization:
How to break cryptosystems of
RSA, Rabin, Williams, Blum-Goldwasser,…?

1994 Shor algorithm for finding discrete logarithms:
How to break ElGamal cryptosystem?

1997 Grover algorithm for searching databases:
How to search the keys more effectively?

quantum entanglement
= inseparability
= Verschränkung = entwinement
(Schrödinger 1935)

it is a quantum phenomenon in which
the quantum states of two or more objects (possibly spatially separated)
have to be described with reference to each other.

definition

A bipartite pure state is
separable if $|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$
entangled if $|\psi_{AB}\rangle \neq |\psi_A\rangle \otimes |\psi_B\rangle$

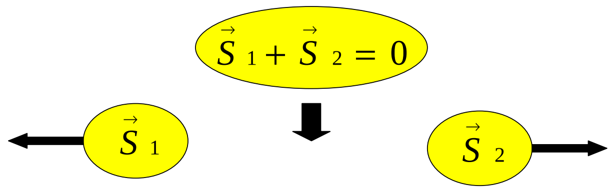
A bipartite mixed state is
separable if $\rho_{AB} = \sum_i p_i \rho_A^i \otimes \rho_B^i$
entangled if $\rho_{AB} \neq \sum_i p_i \rho_A^i \otimes \rho_B^i$
where $\sum_i p_i = 1$ and $p_i \geq 0$ for all i.

quantum entanglement & Einstein-Podolsky-Rosen paradox

How to ‘violate’ uncertainty relation ?

Can we measure exactly both compontents of spin?

$$\operatorname{var} S_{1x} \operatorname{var} S_{1y} \geq \frac{\hbar^2}{4}\left|\langle S_{1z}\rangle\right|^2$$



$$\underline{\underline{S_{1x}}} + S_{2x} = 0, \quad S_{1y} + \underline{\underline{S_{2y}}} = 0$$

So let’s measure S_{1x} i S_{2y} to determine S_{2x} i S_{1y}

Bell states (EPR states)

maximally entangled two-qubit states

$$|\Phi_A\rangle = |\Psi^{(-)}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_x|1\rangle_y - |1\rangle_x|0\rangle_y\right)$$ singlet state

$$|\Phi_B\rangle = |\Psi^{(+)}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_x|1\rangle_y + |1\rangle_x|0\rangle_y\right)$$ one of the triplet states

$$|\Phi_C\rangle = |\Phi^{(-)}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_x|0\rangle_y - |1\rangle_x|1\rangle_y\right)$$

$$|\Phi_D\rangle = |\Phi^{(+)}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_x|0\rangle_y + |1\rangle_x|1\rangle_y\right)$$

maximally? entangled states of 3 qubits

GHZ (Greenberger-Horne-Zeilinger) states

$$\left|\Psi'_{\mathrm{GHZ}}\right\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle \pm |111\rangle\right) \qquad \left|\Psi''_{\mathrm{GHZ}}\right\rangle = \frac{1}{\sqrt{2}}\left(|001\rangle \pm |110\rangle\right)$$

$$\left|\Psi'''_{\mathrm{GHZ}}\right\rangle = \frac{1}{\sqrt{2}}\left(|010\rangle \pm |101\rangle\right) \qquad \left|\Psi^{iv}_{\mathrm{GHZ}}\right\rangle = \frac{1}{\sqrt{2}}\left(|100\rangle \pm |011\rangle\right)$$

W states

$$|\Phi_W\rangle = \frac{1}{\sqrt{3}}\left(|100\rangle + |010\rangle + |001\rangle\right)$$

$$|\Psi_W\rangle = \frac{1}{\sqrt{3}}\left(|011\rangle + |101\rangle + |110\rangle\right)$$

Bell states in matrix representation

$$|\Psi^{(-)}\rangle = \tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \tfrac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\-1\\0\end{bmatrix}, \quad |\Psi^{(+)}\rangle = \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \tfrac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\1\\0\end{bmatrix},$$

$$|\Phi^{(-)}\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \tfrac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\-1\end{bmatrix}, \quad |\Phi^{(+)}\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \tfrac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix}$$

a GHZ state in matrix representation

$$|\Psi'\rangle = \tfrac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

$$= \tfrac{1}{\sqrt{2}}\left(\begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} + \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix}\right)$$

$$= \tfrac{1}{\sqrt{2}}([10000000]^T + [00000001]^T) = \tfrac{1}{\sqrt{2}}[10000001]^T$$

Applications of quantum entanglement (I)

in quantum information theory:

- dense coding [Bennett and Wiesner'92]
- quantum teleportation [Bennett et al.'93]
- entanglement swapping [Żukowski et al.'93]
- superfast [Shor'94] and fast [Grover'97] algorithms
- quantum error correction [Shor'95, Steane'96]

in quantum cryptography:

- quantum key distribution [Ekert'91, Bennett et al.'92]
- privacy amplification [Bennett et al.'96, Deutsch et al.'96]
- secret sharing [Żukowski et al.'98]
- quantum authentication [Ljunggren et al.'00]
- quantum watermarking [Imoto et al.'05]

Applications of quantum entanglement (II)

in quantum communication:

- to simplify communication complexity [Cleve & Buhrman'97]

in quantum state engineering:

- telecloning [Murao et al. 99]
- remote state preparation [Bennett et al.'01]

to increase precision of quantum measurements:

- quantum noise reduction in spectroscopy [Wineland et al.'92]
- to improve frequency standards [Huelga et al. '97]
- better clock synchronization [Jozsa et al.'00, Chuang'00]
- interferometric lithography beyond diffraction limit [Boto et al.'00]

  classical limit: $\lambda/2$

  quantum limit: $\lambda/(2N)$ for N-photon absorption

examples of separable states

example 1

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle)$$

proof:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|1\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B) = \frac{1}{\sqrt{2}}|1\rangle_A(|0\rangle_B+|1\rangle_B) = |1\rangle_A \underbrace{\frac{|0\rangle_B+|1\rangle_B}{\sqrt{2}}}_{|+\rangle_B} = |1\rangle_A|+\rangle_B$$

example 2

$$|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

proof:

$$|\psi\rangle = \frac{1}{2}[|0\rangle_A(|0\rangle_B + |1\rangle_B) + |1\rangle_A(|0\rangle_B + |1\rangle_B)] = \frac{1}{2}(|0\rangle_A + |1\rangle_A)(|0\rangle_B + |1\rangle_B)$$

$$= \frac{|0\rangle_A + |1\rangle_A}{\sqrt{2}} \cdot \frac{|0\rangle_B + |1\rangle_B}{\sqrt{2}} \equiv |+\rangle_A|+\rangle_B$$

example of inseparable state - singlet state

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

proof that it cannot be written as a product state

$$\frac{|01\rangle-|10\rangle}{\sqrt{2}} = (a|0\rangle + b|1\rangle) \otimes (a'|0\rangle + b'|1\rangle)$$

$$= aa'|00\rangle + ab'|01\rangle + ba'|10\rangle + bb'|11\rangle$$

where

$$|a|^2 + |b|^2 = |a'|^2 + |b'|^2 = 1$$

$$a, a', b, b' \in \mathcal{C}$$

So we get **set of equations**

$$aa' = 0, ab' = \frac{1}{\sqrt{2}}, ba' = -\frac{1}{\sqrt{2}}, bb' = 0$$

which admits no solution.

example of inseparable (Bell-like) state

$$|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$$

proof:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle_A \underbrace{\frac{|0\rangle_B + |1\rangle_B}{\sqrt{2}}}_{=|+\rangle_B} + |1\rangle_A \underbrace{\frac{|0\rangle_B - |1\rangle_B}{\sqrt{2}}}_{=|-\rangle_B}\Big) = \frac{|0+\rangle + |1-\rangle}{\sqrt{2}}$$

this state can be obtained from a Bell state
by applying Hadamard gate to 2nd qubit

$$|\psi\rangle = H_B \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$= \frac{1}{\sqrt{2}}(|0\rangle_A(\underbrace{H|0\rangle}_{=|+\rangle})_B + |1\rangle_A(\underbrace{H|1\rangle}_{=|-\rangle})_B)$$

$$= \frac{1}{\sqrt{2}}(|0\rangle_A|+\rangle_B + |1\rangle_A|-\rangle_B) \ \square$$

generation of all Bell states from one of them

e.g. from

$$|\Phi^{(+)}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

flip qubit B = apply NOT gate to qubit B:

$$X_B \frac{|0\underline{0}\rangle + |1\underline{1}\rangle}{\sqrt{2}} = \frac{|01\rangle + |10\rangle}{\sqrt{2}} = |\Psi^{(+)}\rangle$$

phase flip qubit B:

$$Z_B \frac{|0\underline{0}\rangle + |1\underline{1}\rangle}{\sqrt{2}} = \frac{|00\rangle - |11\rangle}{\sqrt{2}} = |\Phi^{(-)}\rangle$$

flip + phase flip qubit B:

$$Y_B \frac{|0\underline{0}\rangle + |1\underline{1}\rangle}{\sqrt{2}} = i\frac{|01\rangle - |10\rangle}{\sqrt{2}} = i|\Psi^{(-)}\rangle$$

How to generate Bell states from $|00\rangle$ # 1

Bell state $|\Phi^{(+)}\rangle$:

$$U_{\text{CNOT}} H_A |00\rangle = U_{\text{CNOT}}|+0\rangle$$

$$= U_{\text{CNOT}} \frac{|0\rangle + |1\rangle}{\sqrt{2}}|0\rangle = U_{\text{CNOT}} \frac{|00\rangle + |10\rangle}{\sqrt{2}}$$

$$= \frac{|\underline{0}, 0 \oplus \underline{0}\rangle + |\underline{1}, 0 \oplus \underline{1}\rangle}{\sqrt{2}}$$

$$= \frac{|00\rangle + |11\rangle}{\sqrt{2}} = |\Phi^{(+)}\rangle$$

Bell state $|\Phi^{(-)}\rangle$:

$$U_{\text{CNOT}} H_A X_A |00\rangle = U_{\text{CNOT}} H_A |10\rangle = U_{\text{CNOT}}|-0\rangle$$

$$= \frac{|0, 0 \oplus 0\rangle - |1, 0 \oplus 1\rangle}{\sqrt{2}} = \frac{|00\rangle - |11\rangle}{\sqrt{2}} = |\Phi^{(-)}\rangle \ \square$$

How to generate Bell states from $|00\rangle$ # 2

Bell state $|\Psi^{(+)}\rangle$:

$$U_{\text{CNOT}} H_A X_B |00\rangle = U_{\text{CNOT}} H_A |01\rangle$$

$$= U_{\text{CNOT}}|+0\rangle = \frac{|0, 1 \oplus 0\rangle + |1, 1 \oplus 1\rangle}{\sqrt{2}}$$

$$= \frac{|01\rangle + |10\rangle}{\sqrt{2}} = |\Psi^{(+)}\rangle \ \square$$

Bell state $|\Psi^{(-)}\rangle$:

$$U_{\text{CNOT}} H_A X_A X_B |00\rangle = U_{\text{CNOT}} H_A |11\rangle$$

$$= U_{\text{CNOT}}|-1\rangle = \frac{|0, 1 \oplus 0\rangle - |1, 1 \oplus 1\rangle}{\sqrt{2}}$$

$$= \frac{|01\rangle - |10\rangle}{\sqrt{2}} = |\Psi^{(-)}\rangle \ \square$$

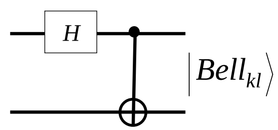
Generation of Bell states

general formula $(k, l = 0, 1)$

$$U_{\mathrm{CNOT}} H_A |kl\rangle = \frac{|0l\rangle + (-1)^k |1, 1 \oplus l\rangle}{\sqrt{2}} = |\mathrm{Bell}_{kl}\rangle$$

qubit A $|k\rangle$

qubit B $|l\rangle$



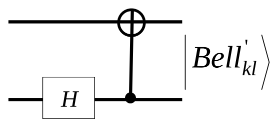
CNOT

obviously, we can obtain Bell states by:

$$U'_{\mathrm{CNOT}} H_B |lk\rangle = |\mathrm{Bell'}_{kl}\rangle$$

qubit A $|l\rangle$

qubit B $|k\rangle$

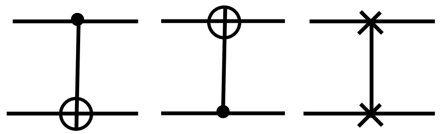


CNOT

CNOT and SWAP gates

```
CNOT         CNOT'        SWAP
in | out     in | out     in | out
--------     --------     --------
00 | 00      00 | 00      00 | 00
01 | 01      01 | 11      01 | 10
10 | 11      10 | 10      10 | 01
11 | 10      11 | 01      11 | 11
```

$$|\psi_{\mathrm{in}}\rangle = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle \equiv c_0|0\rangle + c_1|1\rangle + c_2|2\rangle + c_3|3\rangle$$
$$\hat{U}_{\mathrm{CNOT}}|\psi_{\mathrm{in}}\rangle = c_0|00\rangle + c_1|01\rangle + c_3|10\rangle + c_2|11\rangle \equiv c_0|0\rangle + c_1|1\rangle + c_3|2\rangle + c_2|3\rangle$$
$$\hat{U}'_{\mathrm{CNOT}}|\psi_{\mathrm{in}}\rangle = c_0|00\rangle + c_3|01\rangle + c_2|10\rangle + c_1|11\rangle \equiv c_0|0\rangle + c_3|1\rangle + c_2|2\rangle + c_1|3\rangle$$
$$\hat{U}_{\mathrm{SWAP}}|\psi_{\mathrm{in}}\rangle = c_0|00\rangle + c_2|01\rangle + c_1|10\rangle + c_3|11\rangle \equiv c_0|0\rangle + c_2|1\rangle + c_1|2\rangle + c_3|3\rangle$$



CNOT CNOT' SWAP

CNOT and SWAP gates in matrix representation

$$\hat{U}_{\mathrm{CNOT}} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} c_0 \\ c_1 \\ c_3 \\ c_2 \end{bmatrix}$$

$$\hat{U}'_{\mathrm{CNOT}} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 1&0&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \\ 0&1&0&0 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} c_0 \\ c_3 \\ c_2 \\ c_1 \end{bmatrix}$$

$$\hat{U}_{\mathrm{SWAP}} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 1&0&0&0 \\ 0&0&1&0 \\ 0&1&0&0 \\ 0&0&0&1 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} c_0 \\ c_2 \\ c_1 \\ c_3 \end{bmatrix}$$

Generation of Bell states

- decay of a particle with spin 0 into 2 particles with spin ½

$$|\Psi\rangle_{xy} = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle_x|\downarrow\rangle_y - |\downarrow\rangle_x|\uparrow\rangle_y\right)$$

- light generated by parametric down conventer (PDC II)

$$|\Psi\rangle_{xy} = \frac{1}{\sqrt{2}}\left(|H\rangle_x|V\rangle_y + e^{i\chi}|V\rangle_x|H\rangle_y\right)$$

$$|\Phi\rangle_{xy} = \frac{1}{\sqrt{2}}\left(|H\rangle_x|H\rangle_y + e^{i\chi}|V\rangle_x|V\rangle_y\right)$$

- output light of beam splitter 50:50 with a single input photon

$$|\Phi\rangle_{xy} = \frac{1}{\sqrt{2}}\left(|0\rangle_x|1\rangle_y + e^{i\chi}|1\rangle_x|0\rangle_y\right)$$

- projection of separable state onto entangled one

Entanglement
from a mystery to a physical resource

- An entangled wave-function does not describe the physical reality in a complete way. [Einstein,Podolsky,Rosen]
- For an entangled state is the best possible knowledge of the whole does not include the best possible knowledge of its parts. [E. Schrödinger]
- Entanglement is a "fundamental resource of Nature, of comparable importance to energy, information, entropy, or any other fundamental resource." [M. Nielsen, I. Chuang]

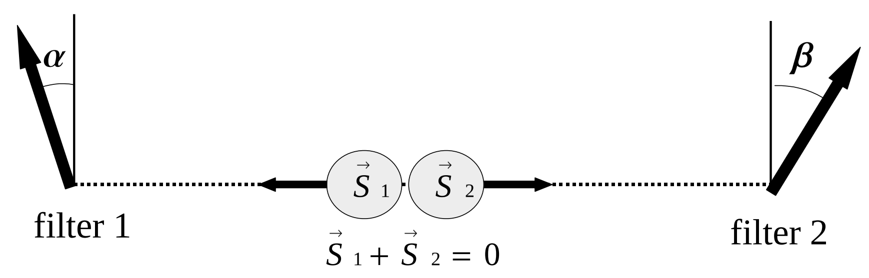
Entanglement is...

- a correlation that is stronger than any classical correlation. [J. Bell]
- a correlation that contradicts the theory of elements of reality. [D. Mermin]
- a trick that quantum magicians use to produce phenomena that cannot be imitated by classical magicians. [A. Peres]
- a resource that enables quantum teleportation. [C. Bennett]
- a global structure of the wavefunction that allows for faster algorithms. [P. Shor]
- a tool for secure communication. [A. Ekert]
- the need for first applications of positive maps in physics. [Horodecki family]

[collected by Dagmar Bruß, quant-ph/0110078]

Measurement of entangled spins and Bell inequalities

Stern-Gerlach filter



$N_{++}(\alpha,\beta)$ – number of outcomes when spin $+1$ was measured in filter 1 at angle α and in filter 2 at angle β

N – total number of outcomes

probability $P_{++}(\alpha,\beta) = N_{++}(\alpha,\beta)/N$

- **QM predictions**

for electrons in singlet state

$$|\psi^{(-)}\rangle = \frac{|\uparrow\rangle_1|\downarrow\rangle_2 - |\downarrow\rangle_1|\uparrow\rangle_2}{\sqrt{2}} \equiv \frac{|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle}{\sqrt{2}}$$

then

$$P_{++}(\alpha,\beta) = P_{--}(\alpha,\beta) = \frac{1}{2}\sin^2\left(\frac{\alpha-\beta}{2}\right)$$

$$P_{+-}(\alpha,\beta) = P_{-+}(\alpha,\beta) = \frac{1}{2}\cos^2\left(\frac{\alpha-\beta}{2}\right)$$

special cases:

1. $\alpha = \beta \quad \Rightarrow$ spins of opposite values

$$\Rightarrow \quad P_{++}(\alpha,\alpha) = P_{--}(\alpha,\alpha) = 0, \quad P_{+-}(\alpha,\alpha) = P_{-+}(\alpha,\alpha) = \frac{1}{2}$$

2. $\beta = \frac{\pi}{2} + \alpha \quad \Rightarrow$ measurement of 2 independent spins

$$\Rightarrow \quad P_{++}(\alpha,\beta) = P_{+-}(\alpha,\beta) = P_{-+}(\alpha,\beta) = P_{--}(\alpha,\beta) = \frac{1}{4}$$

- **Bell inequality** for 3 series of measurements

$$N_{++}(\alpha,\beta) + N_{++}(\beta,\gamma) \geq N_{++}(\alpha,\gamma)$$

$$P_{++}(\alpha,\beta) + P_{++}(\beta,\gamma) \geq P_{++}(\alpha,\gamma)$$

- **violation of Bell inequality**

occurs, e.g., for $\alpha = 0, \beta = \pi/4, \gamma = \pi/2$

$$\mathrm{LHS} = \sin^2(\pi/8) = 0.146\cdots \not\geq \mathrm{RHS} = 0.25$$

Mathematica:

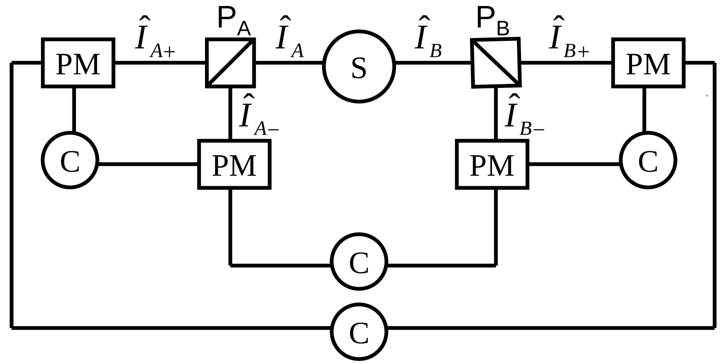
```
P[a_, b_] := 1/2*Sin[(a - b)/2]^2
LHS = P[0, Pi/4] + P[Pi/4, Pi/2]
RHS = P[0, Pi/2]
```


Bell assumptions

1. **reasoning by induction**
   – from large number of measurements probability can be determined
   – this is very natural assumption
2. **realism**
   – physical objects have properties independent of whether we measure them or not
3. **locality**
   – measurement by filter in position 1 does not influence the result of measurement by filter in a distant place 2

- violation of a Bell inequality implies that
the world is **nonrealistic or/and nonlocal**
- **"the deepest discovery in history of science"** [Stapp]
as enables to decide experimentally a dispute between Einstein and Bohr.

Aspect et al. tests of Bell-CHSH inequalities (1984)



Key:

C – correlation systems

S – source of photons

P_A, P_B – polarizing beam splitters = optical analogues of Stern-Gerlach filters

$\hat{I}_k \sim \hat{n}_k$ – intensity of kth beam

PM – photon multipliers

- **What is measured in the experiment?**

$$E(\phi_A,\phi_B) = \frac{\langle(\hat{I}_{A+}-\hat{I}_{A-})(\hat{I}_{B+}-\hat{I}_{B-})\rangle}{\langle(\hat{I}_{A+}+\hat{I}_{A-})(\hat{I}_{B+}+\hat{I}_{B-})\rangle} = \frac{\langle\hat{I}_{A+}\hat{I}_{B+}\rangle + \langle\hat{I}_{A-}\hat{I}_{B-}\rangle - \langle\hat{I}_{A+}\hat{I}_{B-}\rangle - \langle\hat{I}_{A-}\hat{I}_{B+}\rangle}{\langle\hat{I}_{A+}\hat{I}_{B+}\rangle + \langle\hat{I}_{A-}\hat{I}_{B-}\rangle + \langle\hat{I}_{A+}\hat{I}_{B-}\rangle + \langle\hat{I}_{A-}\hat{I}_{B+}\rangle}$$

at any angles ϕ_A, ϕ_B.

- **Bell inequality according to Clauser-Horne-Shimony-Holt**

$$|S| \leq 2$$

where

$$S = E(\phi'_A,\phi'_B) - E(\phi'_A,\phi''_B) + E(\phi''_A,\phi'_B) + E(\phi''_A,\phi''_B)$$

should be satisfied for realistic local theories.

- **polarization singlet state**

$$|\Psi^{(-)}\rangle = \frac{|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B}{\sqrt{2}}$$

- QM predicts that

$$E(\phi_A, \phi_B) = P_{++}(\phi_A, \phi_B) + P_{--}(\phi_A, \phi_B) - P_{+-}(\phi_A, \phi_B) - P_{-+}(\phi_A, \phi_B)$$

where $P_{jk}(\phi_A, \phi_B)$ in the former slides

- **maximal violation of Bell inequality**

$$\max|S| = 2\sqrt{2}$$

which can be obtained for the following angles of polarizers

$$\phi'_A = 0,\ \phi'_B = \frac{\pi}{4},\ \phi''_A = \frac{\pi}{2},\ \phi''_B = 3\frac{\pi}{4}$$

as

$$S = -3\cos^2\left(\frac{\pi}{8}\right) + \cos^2\left(\frac{3\pi}{8}\right) + 3\sin^2\left(\frac{\pi}{8}\right) - \sin^2\left(\frac{3\pi}{8}\right) = -2\sqrt{2} \approx -2.8$$

- **Note**: the same setup of Aspect was used for testing violation of **Schwarz inequality**

possible loopholes of Bell's inequalities (BI)

- in the present experimental BI tests
- in the proof or assumptions of BI
- in the BI interpretation

I. experimental loopholes

there has been no loophole-free experimental test of BI.

1. **detection efficiency and fair-sample assumption**:

   None experimental test does not detect 100% the particle pairs emitted.

   Thus it is not clear that the pairs registered are a fair sample of all pairs emitted.

2. **causality**:

   The choice of measurement settings of Alice and Bob should be **truly random** and placed at **sufficient physical distance**.

II. loopholes in BI assumptions

1. **independence assumption**:

   There are physical processes independent of the Bell experiment that can be used as an effective source of **randomness**.

III. interpretational loopholes

Accepting that Bell's theorem is true then either locality or realism might be false.

1. **universe is non-local but real**

   e.g. **Bohmian hidden variable theory** is explicitly non-local and contextual, but still fairly natural looking.

2. **operationalism of quantum mechanism (QM)**

   the standard **Copenhagen interpretation**:

   QM is just a set of recipes for calculating probabilities of measurement results.

   It says nothing about an underlying physical reality, which may not even exist, and therefore nothing about its locality.

loopholes in Aspect's et al. experiment (1982)

1. a fair-sample assumption

All experiments so far detect only a small subset of all pairs created thus it is necessary to assume that the pairs registered are a fair sample of all pairs emitted.

2. causality

(i) no true randomization

Analyzers were not randomly rotated during the flight of the particles.

Aspect et al. switched the directions of polarization analysers after the photons left the source, but they used periodic sinusoidal switching, which is predictable.

(ii) no true space-like separation

The necessary space-like separation of the observations was not achieved by sufficient physical distance between the measurement stations.

- **BI test more ideal than ever by Zeilinger** et al. (PRL 1998) on "Violation of Bell's inequality under strict Einstein locality conditions".

Two definitions of entanglement

Def. 1. A state ρ_{AB} is separable iff

$$\rho_{AB} = \sum_i p_i \rho_A^i \otimes \rho_B^i$$

where $\sum_i p_i = 1$ and $p_i \geq 0$ for all i.

Def. 2. A state ρ_{AB} is separable iff

$$\rho_{AB} = \sum_i p_i |\psi_A^i\rangle\langle\psi_A^i| \otimes |\psi_B^i\rangle\langle\psi_B^i|$$

where $\sum_i p_i = 1$ and $p_i \geq 0$ for all i.

These definitions are equivalent, as ρ_A^i (and ρ_B^i) can be expanded in terms eigenvectors

$$\rho_A^j = \sum q_j |\psi_A^j\rangle\langle\psi_A^j|$$

where $\sum_j q_j = 1$ and $q_j \geq 0$ for all i.

General definition of bipartite entanglement

A state $\hat\rho_{AB}$ is separable iff
it can be written or *approximated* (in, e.g., trace norm) by

$$\hat\rho_{AB} = \sum_i p_i \rho_A^i \otimes \rho_B^i$$

where $\sum_i p_i = 1$ and $p_i \geq 0$ for all i.

systems of finite dimensions

If $\hat\rho_{AB}$ acts in finite-dimensional Hilbert spaces then the *approximation* part is redundant.

trace norm

$$||\hat A|| = \mathrm{Tr}|\hat A| = \mathrm{Tr}(\sqrt{\hat A^\dagger \hat A})$$

Can we decompose Bell states into separable states?

e.g. the 'triplet' state

$$|\Psi^{(+)}\rangle\langle\Psi^{(+)}| = \sum_{i=1}^{5} p_i |a_i\rangle\langle a_i| \otimes |b_i\rangle\langle b_i|$$

$$p_1 = p_2 = p_3 = \frac{2}{3}, \quad p_4 = p_5 = -\frac{1}{2}$$

$$|a_1\rangle \;=\; |b_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|a_2\rangle \;=\; |b_2\rangle = \frac{|0\rangle + e^{i2\pi/3}|1\rangle}{\sqrt{2}}$$

$$|a_3\rangle \;=\; |b_3\rangle = \frac{|0\rangle + e^{-i2\pi/3}|1\rangle}{\sqrt{2}}$$

$$|a_4\rangle = |0\rangle, \quad |b_4\rangle = |1\rangle, \quad |a_5\rangle = |1\rangle, \quad |b_5\rangle = |0\rangle$$

note that $p_4 = p_5 < 0$

thus it is not a *convex* combination of product states and the state is entangled.

Werner state

$$\hat\rho_W^{(\pm)} = \frac{1-p}{4}\,\hat 1 \otimes \hat 1 + p|\Psi^{(\pm)}\rangle\langle\Psi^{(\pm)}|$$

is mixture of maximally entangled state

$$|\Psi^{(\pm)}\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}$$

and maximally mixed state

$$\hat 1 \otimes \hat 1 \equiv \hat 1_2 \otimes \hat 1_2 = \hat 1_4 = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11| = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

the Werner state is entangled

$E(\hat\rho_W) > 0$ for all $\frac{1}{3} < p \leq 1$

and violates Bell inequality

$B(\hat\rho_W) > 0$ for all $\frac{1}{\sqrt{2}} < p \leq 1$

decomposition of Werner state

$$\hat\rho_W^{(+)} = \sum_{i=1}^{7} p_i |a_i\rangle\langle a_i| \otimes |b_i\rangle\langle b_i|$$

$$p_1 = p_2 = p_3 = \frac{2}{3}, \quad p_4 = p_5 = \frac{1-3p}{4}, \quad p_6 = p_7 = \frac{1-p}{4}$$

$$\begin{aligned}
|a_1\rangle &= |b_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\\
|a_2\rangle &= |b_2\rangle = \frac{|0\rangle + e^{i2\pi/3}|1\rangle}{\sqrt{2}}\\
|a_3\rangle &= |b_3\rangle = \frac{|0\rangle + e^{-i2\pi/3}|1\rangle}{\sqrt{2}}\\
|a_4\rangle &= |0\rangle, \quad |b_4\rangle = |1\rangle\\
|a_5\rangle &= |1\rangle, \quad |b_5\rangle = |0\rangle\\
|a_6\rangle &= |0\rangle, \quad |b_6\rangle = |0\rangle\\
|a_7\rangle &= |1\rangle, \quad |b_7\rangle = |1\rangle
\end{aligned}$$

clearly, the state is separable only for $p \le \frac{1}{3}$ when all $p_i \ge 0$.

Werner and Werner-like states

$$\hat\rho_W(p) = \frac{1-p}{4}\hat{1} \otimes \hat{1} + p|\psi\rangle\langle\psi|$$

original Werner state

$$|\psi\rangle \to |\Psi^{(-)}\rangle = \tfrac{|01\rangle - |10\rangle}{\sqrt{2}}$$

isotropic state (Werner-like state)

$$|\psi\rangle \to |\Phi^{(+)}\rangle = \tfrac{|00\rangle + |11\rangle}{\sqrt{2}}$$

other Werner-like states

$$|\psi\rangle \to |\Psi^{(+)}\rangle = \tfrac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\psi\rangle \to |\Phi^{(-)}\rangle = \tfrac{|00\rangle - |11\rangle}{\sqrt{2}}$$

two qudit (d-dimensional) isotropic state

$$\hat\rho_W(p) = \tfrac{1-p}{d^2}\,\hat{1}^{\otimes d} + p|\Phi_d^{(+)}\rangle\langle\Phi_d^{(+)}|$$

where $-\frac{1}{d^2-1} \le p \le 1$

$$|\Phi_d^{(+)}\rangle = \tfrac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|ii\rangle$$

properties of Werner states

1. They are so-called **maximally entangled mixed states** (MEMS)
   - entanglement $E(\rho_W)$ cannot be increased by **any unitary operations**,
   - entanglement $E(\rho_W)$ is maximal for a given **linear entropy** (and vice versa)

   [Ishizaka, Hiroshima'00, Munro et al.'01]
2. Original Werner state exhibits $U \otimes U$ **invariance**:
   $\hat U \otimes \hat U \hat\rho_W^{(-)} = \hat\rho_W^{(-)}$
3. All entangled Werner states (even for $p \in (1/3, 1/\sqrt{2})$) can be used for quantum-information processing including **teleportation** [Popescu'94, Lee,Kim'00]

nonlocality

quantum states are called **nonlocal** if
there is no local unhidden variable model of their behavior.

Thus a **measurement of the whole** can reveal
more information about the system's state
than any sequence of classically coordinated measurements of the parts.

1. nonlocality without entanglement

[Bennett et al. 1999]

There are orthogonal sets of product states of **two qutrits**
that cannot be reliably distinguished by a pair of separated observers
ignorant of which of the states has been presented to them,
even if the observers are allowed to communicate by LOCC.

Note: **LOCC = LQCC**
local quantum operations and classical communication

2. entanglement without nonlocality

⇓

nonlocality and violation Bell-inequality

are often identified

(although there are some serious doubts about it)

2'. entanglement without violating Bell inequality

[Werner 1989]

two-qubit **mixed** states can be entangled without violating Bell inequality

e.g. **Werner states and isotropic states** for

$$\boxed{p \in (1/3, 1/\sqrt{2}\rangle}$$

are entangled and satisfy Bell inequality

thus they can be described in terms **realistic local theories**

Note: two-qubit **pure** states violate Bell inequality iff they are entangled.

Schrödinger cat paradox

- **questions**

– how to interpret superposition of states and entanglement?

– can we talk about of superposition, entanglement or smearing of classical objects?

- **gedanken experiment of Schrödinger cat**

image a chamber containing:

– a cat

– a bottle with poison gas

– radioactive atom

– automatic device to release the poison when the atom decays

- state of the isolated atom after a time equal to its half-time is

$$\frac{1}{\sqrt{2}}\Big(|u\rangle + |d\rangle\Big)$$

where $|d\rangle$ – decayed state, $|u\rangle$ – undecayed state.

- but the atom is **entangled** with the cat via the apparatus

so the state is

$$\frac{1}{\sqrt{2}}\Big(|u\rangle_{\rm atom}|{\rm alive}\rangle_{\rm cat} + |d\rangle_{\rm atom}|{\rm dead}\rangle_{\rm cat}\Big)$$

- **Copenhagen interpretation**

to understand it, one has to include the observer or measurement process:

the „quantum chamber" has to be opened to check the state of the „cat".

(modern) definition of Schrödinger cat (state)

it is a superposition of two macroscopically distinct states

Note: the definition can be applied to a single mode, thus not necessarily has to be related to entanglement

- e.g. superposition of two coherent states

$$|\psi\rangle = \mathcal{N}[|\alpha\rangle + e^{i\varphi}| - \alpha\rangle]$$

where $\mathcal{N}$ is a normalization constant assuming $\alpha \in \mathcal{R}$:

$$\mathcal{N} = [2 + 2\cos\varphi\exp(-2\alpha^2)]^{-1/2}$$

special cases of **single-mode Schrödinger cats**:

– **even coherent state** for $\varphi = 0$:

$$|\psi_+\rangle \;=\; \mathcal{N}_+\big(|\alpha\rangle + |-\alpha\rangle\big) = \frac{1}{\sqrt{\cosh(\alpha^2)}}\sum_{n=0}^{\infty}\frac{\alpha^{2n}}{\sqrt{(2n)!}}|2n\rangle \equiv |\mathbf{0}\rangle_{\rm L}$$

– **odd coherent state** for $\varphi = \pi$:

$$|\psi_-\rangle \;=\; \mathcal{N}_-\big(|\alpha\rangle - |-\alpha\rangle\big) = \frac{1}{\sqrt{\sinh(\alpha^2)}}\sum_{n=0}^{\infty}\frac{\alpha^{2n+1}}{\sqrt{(2n+1)!}}|2n+1\rangle \equiv |\mathbf{1}\rangle_{\rm L}$$

– **Yurke-Stoler states** for $\varphi = \pm\pi/2$:

$$|\psi_{\rm YS}\rangle = \frac{1}{\sqrt{2}}\big(|\alpha\rangle \pm i|-\alpha\rangle\big)$$

- **Note**: the above states are *not* mixtures of coherent states

$$\hat{\rho}_{\rm mix} = \frac{1}{2}\big(|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha|\big) \neq |\psi\rangle\langle\psi|$$

two-mode Schrödinger cats

continuous variable (CV) version of two-qubit Bell states

$$|\Phi^{(+)}\rangle = \frac{1}{\sqrt{2}}(|00\rangle_L + |11\rangle_L) = \mathcal{N}(|\alpha,\beta\rangle + |-\alpha,-\beta\rangle)$$

$$|\Phi^{(-)}\rangle = \frac{1}{\sqrt{2}}(|00\rangle_L - |11\rangle_L) = \mathcal{N}(|\alpha,-\beta\rangle + |-\alpha,\beta\rangle)$$

$$|\Psi^{(+)}\rangle = \frac{1}{\sqrt{2}}(|01\rangle_L + |10\rangle_L) = \mathcal{N}(|\alpha,\beta\rangle - |-\alpha,-\beta\rangle)$$

$$|\Psi^{(-)}\rangle = \frac{1}{\sqrt{2}}(|01\rangle_L + |10\rangle_L) = \mathcal{N}(|\alpha,-\beta\rangle - |-\alpha,\beta\rangle)$$

assumption $\alpha = \beta$

exemplary proof of a CV Bell state

definition of logical qubits ($\alpha = \beta$):

$$|0\rangle_L = \mathcal{N}_+\big(|\beta\rangle + |-\beta\rangle\big)$$

$$|1\rangle_L = \mathcal{N}_-\big(|\beta\rangle - |-\beta\rangle\big)$$

so

$$\frac{1}{\sqrt{2}}(|00\rangle_L + |11\rangle_L) = \frac{\mathcal{N}_+\mathcal{N}_-}{\sqrt{2}}\Big[(|\alpha\rangle+|-\alpha\rangle)(|\beta\rangle+|-\beta\rangle)+(|\alpha\rangle-|-\alpha\rangle)(|\beta\rangle-|-\beta\rangle)\Big]$$

$$= \frac{\mathcal{N}_+\mathcal{N}_-}{\sqrt{2}}\Big[\underline{|\alpha,\beta\rangle} + |\alpha,-\beta\rangle + |-\alpha,\beta\rangle + \underline{|-\alpha,-\beta\rangle}$$
$$+\underline{|\alpha,\beta\rangle} - |\alpha,-\beta\rangle - |-\alpha,\beta\rangle + \underline{|-\alpha,-\beta\rangle}\Big]$$

$$= \sqrt{2}\mathcal{N}_+\mathcal{N}_-\big(|\alpha,\beta\rangle + |-\alpha,-\beta\rangle\big)$$

Problems

– How to generate single photons?

– How to generate Bell polarization states?

spontaneous parametric down-conversion (SPDC)

a nonlinear optical phenomenon in which a nonlinear crystal splits incoming photons into pairs of photons of lower energy.

Hamiltonians

(for simplicity assume $g = |g|$)

1. hamiltonian for a degenerate process

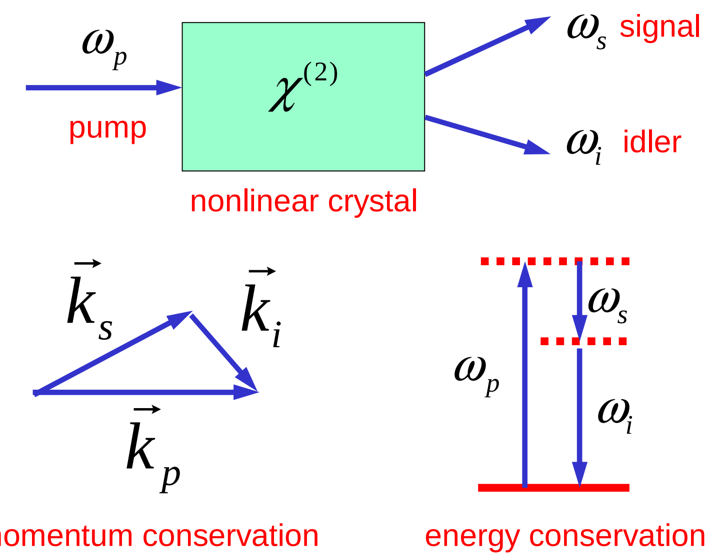
$$\hat{H}_{\text{deg}} = \hbar g[\hat{a}^2 + (\hat{a}^2)^\dagger]$$

2. hamiltonian for a nondegenerate process of **type I**

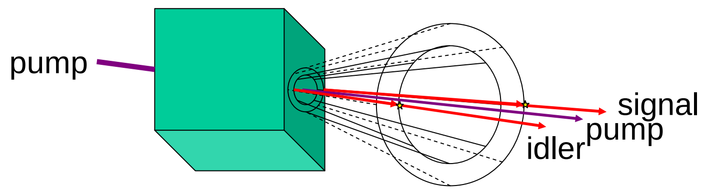
$$\hat{H}_1 = \hbar g \hat{a}_s^\dagger \hat{a}_i^\dagger + h.c.$$

Note: signal (s) and idler (i) have the same polarization

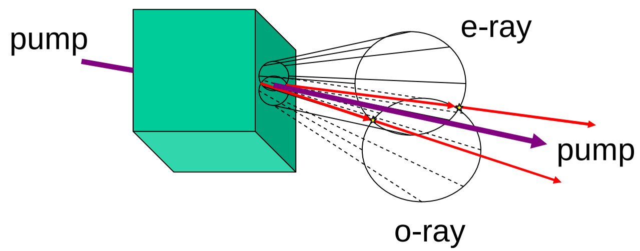
spontaneous parametric down-conversion (SPDC)



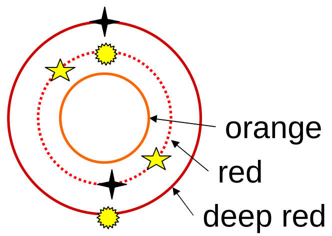
type I parametric down converter



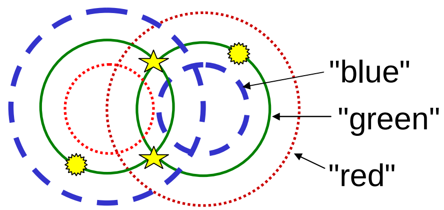
type II parametric down converter



type I parametric down converter



type II parametric down converter



3. hamiltonian for a nondegenerate process of **type II**

$$\hat{H}_2 = \hbar g(\hat{a}^\dagger_{Vs}\hat{a}^\dagger_{Hi} + \hat{a}^\dagger_{Hs}\hat{a}^\dagger_{Vi}) + h.c.$$

where

V (H) – linear vertical (horizontal) polarization

$\hat{a}^\dagger_{Vs}$ – creation operator for signal mode of vertical polarization etc.

Note: signal and idler modes have perpendicular polarizations

short-time evolution

$$|\psi(t)\rangle \;=\; \exp\left(\frac{1}{i\hbar}\hat{H}t\right)|\psi(0)\rangle \approx \left[1 + \frac{t}{i\hbar}\hat{H} + \frac{1}{2}\left(\frac{t}{i\hbar}\hat{H}\right)^2\right]|\psi(0)\rangle$$

– type I process:

$$|\psi(0)\rangle = |0\rangle_s|0\rangle_i$$

$$|\psi(t)\rangle = (1 - \tfrac{1}{2}\tau^2)|0\rangle_s|0\rangle_i - \frac{i\tau}{\sqrt{2}}|1\rangle_s|1\rangle_i$$

where $\tau = gt$

– type II process:

$$|\psi(0)\rangle = |0\rangle_{Vs}|0\rangle_{Hs}|0\rangle_{Vi}|0\rangle_{Hi}$$

$$\begin{aligned}|\psi(t)\rangle \;=\; & (1 - \tfrac{1}{2}\tau^2)|0\rangle_{Vs}|0\rangle_{Hs}|0\rangle_{Vi}|0\rangle_{Hi} \\ & -\frac{i\tau}{\sqrt{2}}(|1\rangle_{Vs}|0\rangle_{Hs}|0\rangle_{Vi}|1\rangle_{Hi} + |0\rangle_{Vs}|1\rangle_{Hs}|1\rangle_{Vi}|0\rangle_{Hi})\end{aligned}$$

- **notation**:

$$|0\rangle_{Vs}|0\rangle_{Hs} \equiv |0\rangle_s, \quad |1\rangle_{Vs}|0\rangle_{Hs} \equiv |V\rangle_s, \quad |0\rangle_{Vs}|1\rangle_{Hs} \equiv |H\rangle_s,$$

and analogously for mode i

thus we have

$$|\psi(t)\rangle = (1 - \tfrac{1}{2}\tau^2)|0\rangle_s|0\rangle_i - \frac{i\tau}{\sqrt{2}}(|V\rangle_s|H\rangle_i + |H\rangle_s|V\rangle_i)$$

the second term is a **polarization Bell state**

$$|\Psi^{(+)}\rangle = \frac{1}{\sqrt{2}}(|V\rangle_s|H\rangle_i + |H\rangle_s|V\rangle_i)$$

How to generate other polarization Bell states?

– place half-wave plate (HWP) on the path of one beams:

$$|\Psi^{(+)}\rangle = \frac{1}{\sqrt{2}}(|V\rangle_s|H\rangle_i + |H\rangle_s|V\rangle_i) \rightarrow \frac{1}{\sqrt{2}}(|H\rangle_s|H\rangle_i + |V\rangle_s|V\rangle_i) = |\Phi^{(+)}\rangle$$

– use phase shifter or simply rotate crystal to change α:

$$|\Psi^{(+)}\rangle \rightarrow |\psi^{(\alpha)}\rangle = \frac{1}{\sqrt{2}}(|V\rangle_s|H\rangle_i + e^{i\alpha}|H\rangle_s|V\rangle_i)$$

- this is how all four Bell states can be obtained including:

$$|\Psi^{(-)}\rangle = \frac{1}{\sqrt{2}}(|V\rangle_s|H\rangle_i - |H\rangle_s|V\rangle_i)$$
$$|\Phi^{(-)}\rangle = \frac{1}{\sqrt{2}}(|H\rangle_s|H\rangle_i - |V\rangle_s|V\rangle_i)$$

the experimental method was developed by **Kwiat, Zeilinger** et al. (1995) using crystals of BBO type II.

standard matrix representations of qubit states

so far we have been applying the orthonormal basis

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

satisfying the **identity** resolution

$$\hat{I} = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{bmatrix} 1 \\ 0 \end{bmatrix}[10] + \begin{bmatrix} 0 \\ 1 \end{bmatrix}[01] = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

then the **NOT gate** is

$$\hat{X} = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

and the **Hadamard gate** is

$$\hat{H} = |0\rangle\langle +| + |1\rangle\langle -| = |+\rangle\langle 0| + |-\rangle\langle 1| = \tfrac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

can we define other representations?

another matrix representation of qubit states

let's use the orthonormal basis

$$|0\rangle = \tfrac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad |1\rangle = \tfrac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

then

$$\langle 0|1\rangle = \tfrac{1}{2}[1,1]\begin{bmatrix} 1 \\ -1 \end{bmatrix} = 0$$

identity resolution

$$\hat{I} = \tfrac{1}{2}\begin{bmatrix} 1 \\ 1 \end{bmatrix}[11] + \tfrac{1}{2}\begin{bmatrix} 1 \\ -1 \end{bmatrix}[1,-1] = \tfrac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + \tfrac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

NOT gate

$$\hat{X} = |0\rangle\langle 1| + |1\rangle\langle 0| = \tfrac{1}{2}\begin{bmatrix} 1 \\ 1 \end{bmatrix}[1,-1] + \tfrac{1}{2}\begin{bmatrix} 1 \\ -1 \end{bmatrix}[1,1]$$
$$= \tfrac{1}{2}\begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix} + \tfrac{1}{2}\begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Hadamard gate

note that

$$|+\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$|-\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

so

$$\begin{aligned}\hat{H} &= |0\rangle\langle +| + |1\rangle\langle -| \\ &= \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}[10] + \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}[01] \\ &= \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} + \frac{1}{\sqrt{2}}\begin{bmatrix} 0 & 1 \\ 0 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\end{aligned}$$

phase-flip gate

$$\hat{Z} = |0\rangle\langle 0| - |1\rangle\langle 1| = \tfrac{1}{2}\begin{bmatrix} 1 \\ 1 \end{bmatrix}[1,1] - \tfrac{1}{2}\begin{bmatrix} 1 \\ -1 \end{bmatrix}[1,-1]$$
$$= \tfrac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} - \tfrac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

rotated matrix representation of qubit states

orthonormal basis

$$|0\rangle = \begin{bmatrix} \cos\theta \\ \sin\theta \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} -\sin\theta \\ \cos\theta \end{bmatrix}$$

or equivalently

$$\begin{bmatrix} |0\rangle' \\ |1\rangle' \end{bmatrix} = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} |0\rangle \\ |1\rangle \end{bmatrix}$$

in terms of standard qubit representations $|0\rangle = [1;0]$ and $|1\rangle = [0;1]$

identity resolution

$$\begin{aligned} \hat{I} &= \begin{bmatrix} \cos\theta \\ \sin\theta \end{bmatrix} [\cos\theta, \sin\theta] + \begin{bmatrix} -\sin\theta \\ \cos\theta \end{bmatrix} [-\sin\theta, \cos\theta] \\ &= \begin{bmatrix} \cos^2\theta & \sin\theta\cos\theta \\ \sin\theta\cos\theta & \sin^2\theta \end{bmatrix} + \begin{bmatrix} \sin^2\theta & -\sin\theta\cos\theta \\ -\sin\theta\cos\theta & \cos^2\theta \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

NOT gate: $\hat{X} = \begin{bmatrix} -\sin(2\theta) & \cos(2\theta) \\ \cos(2\theta) & \sin(2\theta) \end{bmatrix}$

Hadamard gate: $\hat{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} -\sin(2\theta) + \cos(2\theta), & \sin(2\theta) + \cos(2\theta) \\ \sin(2\theta) + \cos(2\theta), & \sin(2\theta) - \cos(2\theta) \end{bmatrix}$

singlet state and rotations of analyzer

Measurements of the polarization singlet state at different angles of the crystal

$$\frac{|0^0, 90^0\rangle - |90^0, 0^0\rangle}{\sqrt{2}} = \frac{|\theta, \theta + 90^0\rangle - |\theta + 90^0, \theta\rangle}{\sqrt{2}}$$

unitary transformation

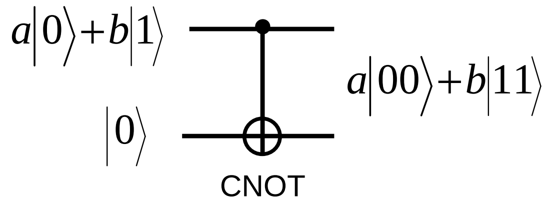
$$|0\rangle = a|x\rangle + b|y\rangle, \quad |1\rangle = c|x\rangle + d|y\rangle$$

proof

$$\begin{aligned} \frac{|01\rangle - |10\rangle}{\sqrt{2}} &= \frac{(a|x\rangle + b|y\rangle) \otimes (c|x\rangle + d|y\rangle) - (c|x\rangle + d|y\rangle) \otimes (a|x\rangle + b|y\rangle)}{\sqrt{2}} \\ &= \frac{\underline{ac|xx\rangle} + ad|xy\rangle + bc|yx\rangle + \underline{bd|yy\rangle} - \underline{ac|xx\rangle} - ad|yx\rangle - bc|xy\rangle - \underline{\underline{bd|yy\rangle}}}{\sqrt{2}} \\ &= \frac{ad(|xy\rangle - |yx\rangle) - bc(|xy\rangle - |yx\rangle)}{\sqrt{2}} \\ &= (ad - bc)\frac{|xy\rangle - |yx\rangle}{\sqrt{2}} = \det \begin{bmatrix} a & b \\ c & d \end{bmatrix} \frac{|xy\rangle - |yx\rangle}{\sqrt{2}} = e^{i\phi}\frac{|xy\rangle - |yx\rangle}{\sqrt{2}} \end{aligned}$$

CNOT as a cloning device?

$$\hat{U}_{\mathrm{CNOT}}\Big(a|0\rangle + b|1\rangle\Big) \otimes |0\rangle = a|0, 0 \oplus 0\rangle + b|1, 0 \oplus 1\rangle = a|00\rangle + b|11\rangle$$



now measure one of the qubits...

It is a cloning device iff $ab = 0$.

requirement for a cloning device

$$\begin{aligned} \hat{U}\Big(a|0\rangle + b|1\rangle\Big) \otimes |s\rangle \to \Big(a|0\rangle + b|1\rangle\Big) \otimes \Big(a|0\rangle + b|1\rangle\Big) \\ = a^2|00\rangle + ab(|01\rangle + |10\rangle) + b^2|11\rangle \end{aligned}$$

now measure one of the qubits...

Quantum no-cloning theorem:

It is impossible to copy (clone, reproduce) an unknown quantum pure state.

proof

let us clone two states

$$\hat{U}|\psi_1\rangle \otimes |s\rangle = |\psi_1\rangle \otimes |\psi_1\rangle$$
$$\hat{U}|\psi_2\rangle \otimes |s\rangle = |\psi_2\rangle \otimes |\psi_2\rangle$$

so

$$LHS = \Big(\langle s| \otimes \langle\psi_1|\hat{U}^\dagger\Big)\Big(\hat{U}|\psi_2\rangle \otimes |s\rangle\Big) = \langle\psi_1|\psi_2\rangle$$
$$RHS = \Big(\langle\psi_1| \otimes \langle\psi_1|\Big)\Big(|\psi_2\rangle \otimes |\psi_2\rangle\Big) = \langle\psi_1|\psi_2\rangle^2$$

equation $x = x^2$ has only trivial solutions: $x = 0$ and $x = 1$

so

either $|\psi_1\rangle = |\psi_2\rangle$ or $|\psi_1\rangle$ is orthogonal to $|\psi_2\rangle$

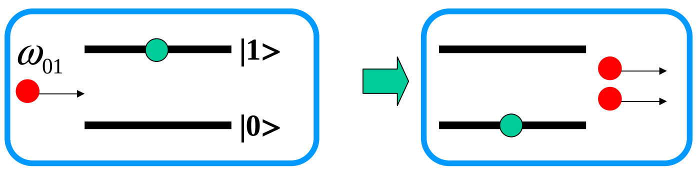
thus

it does not exist a general quantum cloning device as the device can clone only orthogonal states.

Further questions

1. Can we clone unknown mixed quantum states?
   Impossible!
2. What about cloning by non-unitary operations?
   Impossible!
3. What about optimal approximate cloning machines?
   For example, a cloning machine of Bužek and Hillery (1996)
4. Can we clone known quantum states?
   Yes.
5. Can we clone known quantum states by local operations?
   In general impossible!

Quantum cloning and stimulated emission



For each perfect clone there is also
one randomly polarized, spontaneously emitted, photon.

Another question

Suppose that we have several copies of a photon in an unknown state.

Is it possible to **delete the information** content of
one or more of these photons by a physical process?

Quantum no-deleting theorem:

It is impossible to delete an unknown quantum state against a copy.

note

It is not (time) reverse of quantum no-cloning theorem.

proof

we try to find a unitary operation $\hat{U}_{\rm del}$ such that

$$\hat{U}_{\rm del}|\psi\rangle|\psi\rangle|A\rangle = |\psi\rangle|S\rangle|A_\psi\rangle$$

where

$|\psi\rangle = a|0\rangle + b|1\rangle$ - arbitrary qubit state

$|A\rangle$ – initial state of ancilla

$|A_\psi\rangle$ – final state of ancilla (dependent on $|\psi\rangle$)

$|S\rangle$ – some standard final state of the qubit

Let us analyze polarization states

$|\psi\rangle = a|H\rangle + b|V\rangle$

We expect

$$\begin{aligned}\hat{U}_{\rm del}|H\rangle|H\rangle|A\rangle &= |H\rangle|S\rangle|A_H\rangle\\ \hat{U}_{\rm del}|V\rangle|V\rangle|A\rangle &= |V\rangle|S\rangle|A_V\rangle\end{aligned}$$

$$\hat{U}_{\rm del}\frac{|H\rangle|V\rangle + |V\rangle|H\rangle}{\sqrt{2}}|A\rangle = |B\rangle$$

where $|B\rangle$ is some combined input-ancilla state.

Thus, we have

$$\begin{aligned}LHS &= \hat{U}_{\rm del}|\psi\rangle|\psi\rangle|A\rangle\\ &= \hat{U}_{\rm del}(a|H\rangle + b|V\rangle)\otimes(a|H\rangle + b|V\rangle)|A\rangle\\ &= \hat{U}_{\rm del}[a^2|H\rangle|H\rangle + ab(|H\rangle|V\rangle + |V\rangle|H\rangle) + b^2|V\rangle|V\rangle]|A\rangle\\ &= a^2|H\rangle|S\rangle|A_H\rangle + \sqrt{2}ab|B\rangle + b^2|V\rangle|S\rangle|A_V\rangle\end{aligned}$$

$$RHS = a|H\rangle|S\rangle|A_\psi\rangle + b|V\rangle|S\rangle|A_\psi\rangle$$

having only solution for

$$\begin{aligned}|A_\psi\rangle &= a|A_H\rangle + b|A_V\rangle\\ \forall_\psi\langle A_\psi|A_\psi\rangle &= 1 \Rightarrow \langle A_H|A_V\rangle = 0\end{aligned}$$

and

$$|B\rangle = \frac{|H\rangle|S\rangle|A_V\rangle + |V\rangle|S\rangle|A_H\rangle}{\sqrt{2}}$$

so

$$\begin{aligned} LHS &= a^2|H\rangle|S\rangle|A_H\rangle + \sqrt{2}ab\frac{|H\rangle|S\rangle|A_V\rangle + |V\rangle|S\rangle|A_H\rangle}{\sqrt{2}} + b^2|V\rangle|S\rangle|A_V\rangle \\ &= \Big(a^2|H\rangle|S\rangle|A_H\rangle + ab|H\rangle|S\rangle|A_V\rangle\Big) + \Big(ab|V\rangle|S\rangle|A_H\rangle + b^2|V\rangle|S\rangle|A_V\rangle\Big) \\ &= a|H\rangle|S\rangle\Big(a|A_H\rangle + b|A_V\rangle\Big) + b|V\rangle|S\rangle\Big(a|A_H\rangle + b|A_V\rangle\Big) \\ &= \big(a|H\rangle + b|V\rangle\big)|S\rangle|A_\psi\rangle = RHS \,\square \end{aligned}$$

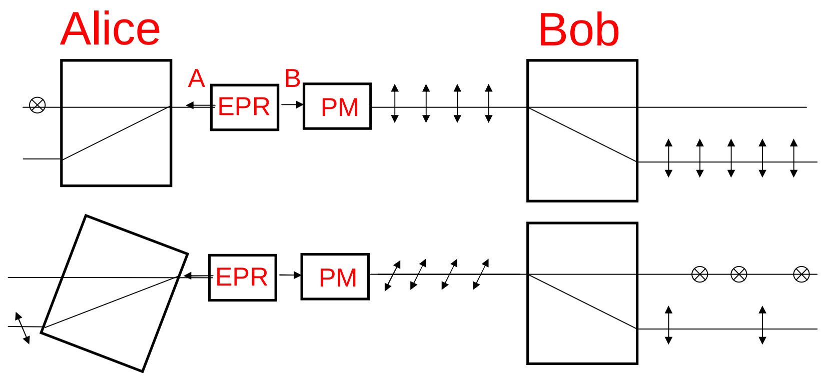
Thus it is seen that

"deleting" is just swapping onto 2D subspace of ancilla

as

$$|A_\psi\rangle = a|A_H\rangle + b|A_V\rangle.$$

superluminal communication?



PM = photon multiplier
EPR = source of the polarization singlet state (e.g. BBO)

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B\right) = \frac{1}{\sqrt{2}}\left(|+\rangle_A|-\rangle_B - |+\rangle_A|-\rangle_B\right)$$

no-go theorems

1. quantum no-cloning

[Wootters, Żurek, Dieks (1982)]

It is impossible to copy an unknown quantum pure state.

2. quantum no-deleting

[Pati, Braunstein (2000)]

It is impossible to delete an unknown quantum pure state.

3. quantum no-broadcasting

[Barnum, Caves, Fuchs, Jozsa, Schumacher (1996)]

It is impossible to copy an unknown quantum mixed state.

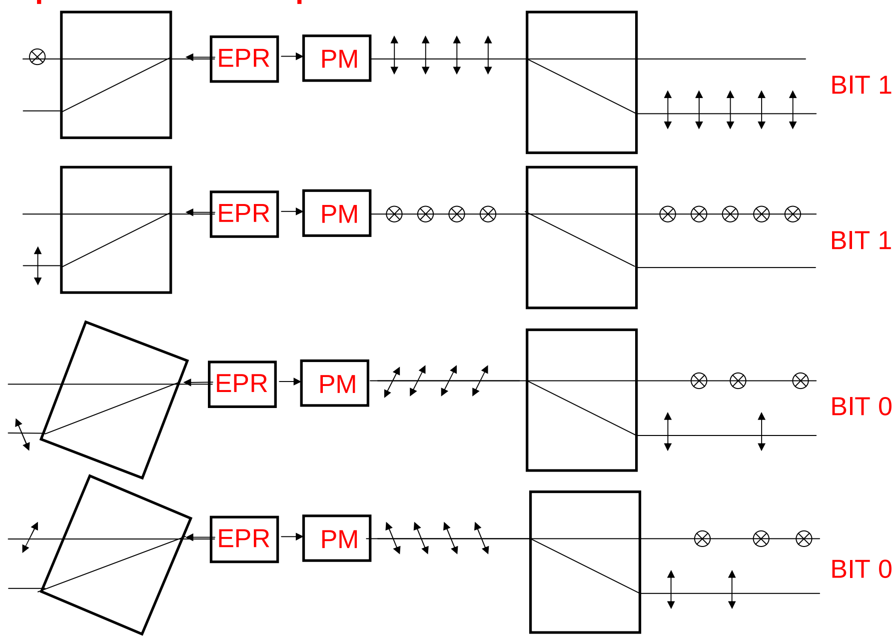
specifically

Given a general mixed state for a quantum system, there are no physical means for broadcasting that state onto two separate quantum systems, even when the states need only be reproduced marginally on the separate systems.

4. quantum no-deleting for mixed states ???

[it might be you...]

a patent for superluminal communication



(super)dense coding

[Bennett and Wiesner 1992]

How to send 2 bits of information by transmitting 1 qubit?

1. Alice and Bob share 2 qubits in an EPR state e.g.

$$|\Phi^{(+)}\rangle = \frac{|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B}{\sqrt{2}}$$

2. if Alice wants to send a message:

00 - then she does nothing $\Rightarrow$ $|\Phi^{(+)}\rangle$

01 - then flips phase of her qubit (Pauli Z gate) $\Rightarrow$ $\hat{Z}|\Phi^{(+)}\rangle = |\Phi^{(-)}\rangle$

10 - then flips her qubit (Pauli X gate) $\Rightarrow$ $\hat{X}|\Phi^{(+)}\rangle = |\Psi^{(+)}\rangle$

11 - then flips & phase-flips her qubit (Pauli iY gate) $\Rightarrow$ $i\hat{Y}|\Phi^{(+)}\rangle = |\Psi^{(-)}\rangle$

3. Alice sends her qubit to Bob
4. Bob measures both qubits using **Bell state analyzer**

superdense coding - a detailed analysis

1. Alice takes qubit A and Bob takes qubit B from an EPR pair:

$$|\Phi^{(+)}\rangle = \frac{|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B}{\sqrt{2}}$$

2. Alice encodes her message by applying proper gate to her qubit A:

$$|00\rangle \rightarrow \hat{I}_A|\Phi^{(+)}\rangle = |\Phi^{(+)}\rangle$$

$$|01\rangle \rightarrow \hat{X}_A|\Phi^{(+)}\rangle = \frac{|\underline{1}0\rangle + |\underline{0}1\rangle}{\sqrt{2}} = |\Psi^{(+)}\rangle$$

$$|10\rangle \rightarrow \hat{Z}_A|\Phi^{(+)}\rangle = \frac{|\underline{0}0\rangle - |\underline{1}1\rangle}{\sqrt{2}} = |\Phi^{(-)}\rangle$$

$$|11\rangle \rightarrow \hat{Z}_A\hat{X}_A|\Phi^{(+)}\rangle = \hat{Z}_A\frac{|\underline{1}0\rangle + |\underline{0}1\rangle}{\sqrt{2}} = \frac{-|\underline{1}0\rangle + |\underline{0}1\rangle}{\sqrt{2}} = |\Psi^{(-)}\rangle$$

2. Alice sends qubit A to Bob. So, he has now two entangled qubits A and B.

3. Bob applies CNOT to remove entanglement between qubits A and B:

$$\hat{U}_{\text{CNOT}}\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|0, 0\oplus 0\rangle + |1, 1\oplus 1\rangle}{\sqrt{2}} = \frac{|0\underline{0}\rangle + |1\underline{0}\rangle}{\sqrt{2}} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}|0\rangle = |+, 0\rangle$$

$$\hat{U}_{\text{CNOT}}\frac{|10\rangle + |01\rangle}{\sqrt{2}} = \frac{|1\underline{1}\rangle + |0\underline{1}\rangle}{\sqrt{2}} = \frac{|1\rangle + |0\rangle}{\sqrt{2}}|1\rangle = |+, 1\rangle$$

$$\hat{U}_{\text{CNOT}}\frac{|00\rangle - |11\rangle}{\sqrt{2}} = \frac{|0\underline{0}\rangle - |1\underline{0}\rangle}{\sqrt{2}} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}|0\rangle = |-, 0\rangle$$

$$\hat{U}_{\text{CNOT}}\frac{|01\rangle - |10\rangle}{\sqrt{2}} = \frac{|0\underline{1}\rangle - |1\underline{1}\rangle}{\sqrt{2}} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}|1\rangle = |-, 1\rangle$$

4. Bob applies Hadamard gate to qubit A:

$$\hat{H}_A|+, 0\rangle = |00\rangle$$

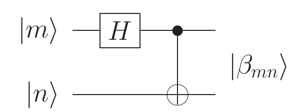
$$\hat{H}_A|+, 1\rangle = |01\rangle$$

$$\hat{H}_A|-, 0\rangle = |10\rangle$$

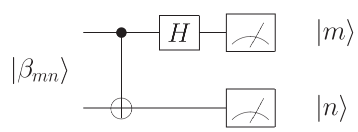
$$\hat{H}_A|-, 1\rangle = |11\rangle$$

4. Bob measures qubits A and B in the standard basis.

q-circuit for Bell-state generation



q-circuit for Bell-state analysis



where

$$|\beta_{00}\rangle = |\Phi^{(+)}\rangle, \quad |\beta_{01}\rangle = |\Psi^{(+)}\rangle, \quad |\beta_{10}\rangle = |\Phi^{(-)}\rangle, \quad |\beta_{11}\rangle = |\Psi^{(-)}\rangle$$

or compactly

$$|\beta_{mn}\rangle = \frac{|0, n\rangle + (-1)^m|1, 1-n\rangle}{\sqrt{2}} \quad \text{for } m, n = 0, 1$$

What is quantum teleportation?

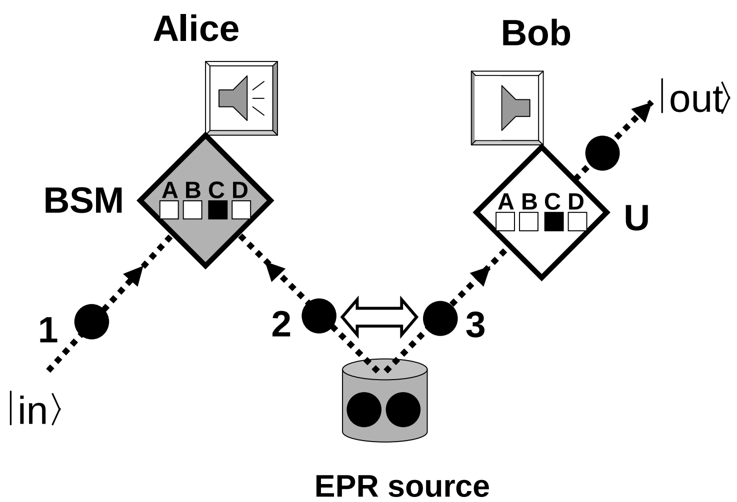
a method to transfer (information about) unknown quantum states
over large distances via entangled particles
and transmission of some classical information.

Remarks:

- Teleportation is a transfer of information about a quantum system without measuring it!
- Teleportation is not a transfer of an object itself, neither its energy etc.
- Teleportation does not violate the no-cloning theorem. (why?)
- Super-luminal communication via teleportation is impossible. (why?)
- Teleportation can provide the quantum channel for communication between quantum computers.
- *Universal quantum computation* via teleportation:
  any quantum circuit can be realized using only teleportation and single-qubit operations.

principles of teleportation

Bennett, Brassard, Crepeau, Jozsa, Peres, Wootters (1993)



explanation of teleportation

Problem: How to teleport state of qubit 1 to qubit 3 ?
Assumption: qubits 2 & 3 are in the singlet state

$$|in\rangle_1 \otimes |\Phi_A\rangle_{23} = \left(a|0\rangle_1 + b|1\rangle_1\right) \otimes \frac{|0\rangle_2|1\rangle_3 - |1\rangle_2|0\rangle_3}{\sqrt{2}}$$

$$= -\frac{1}{2}|\Phi_A\rangle_{12} \otimes \left(a|0\rangle_3 + b|1\rangle_3\right) - \frac{1}{2}|\Phi_B\rangle_{12} \otimes \left(a|0\rangle_3 - b|1\rangle_3\right)$$

$$+\frac{1}{2}|\Phi_C\rangle_{12} \otimes \left(a|1\rangle_3 + b|0\rangle_3\right) + \frac{1}{2}|\Phi_D\rangle_{12} \otimes \left(a|1\rangle_3 - b|0\rangle_3\right)$$

measurement in Bell basis

$\lvert\Phi_A\rangle_{12} \Rightarrow$	$a\lvert 0\rangle_3 + b\lvert 1\rangle_3$	OK
$\lvert\Phi_B\rangle_{12} \Rightarrow$	$\sigma_z\left(a\lvert 0\rangle_3 - b\lvert 1\rangle_3\right)$	phase flip $\lvert x\rangle \to (-1)^x \lvert x\rangle$
$\lvert\Phi_C\rangle_{12} \Rightarrow$	$-\sigma_x\left(-a\lvert 1\rangle_3 - b\lvert 0\rangle_3\right)$	bit flip $\lvert x\rangle \to -\lvert x\oplus 1\rangle$
$\lvert\Phi_D\rangle_{12} \Rightarrow$	$-i\sigma_y\left(a\lvert 1\rangle_3 - b\lvert 0\rangle_3\right)$	phase flip + bit flip $\lvert x\rangle \to (-1)^{x+1}\lvert x\oplus 1\rangle$

where $|\Phi_A\rangle = |\Psi^{(-)}\rangle, |\Phi_B\rangle = |\Psi^{(+)}\rangle, |\Phi_C\rangle = |\Phi^{(-)}\rangle, |\Phi_D\rangle = |\Phi^{(+)}\rangle$

Quantum teleportation - a detailed analysis

Let us analyze teleportation of a polarization state
as in Zeilinger's experiment

$$|\phi\rangle_1 = a|0\rangle_1 + b|1\rangle_1 = a|H\rangle_1 + b|V\rangle_1$$

via the singlet state

$$|\Psi^{(-)}\rangle_{23} = \frac{1}{\sqrt{2}}(|HV\rangle_{23} - |VH\rangle_{23})$$

main idea

Let's expand the total initial state $|\phi\rangle_1|\Psi^{(-)}\rangle_{23}$ in the Bell basis

$$\begin{aligned}|\Psi^{(\pm)}\rangle &= \frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle)\\ |\Phi^{(\pm)}\rangle &= \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle)\end{aligned}$$

note that

$$|\Psi^{(+)}\rangle\langle\Psi^{(+)}| + |\Psi^{(-)}\rangle\langle\Psi^{(-)}| + |\Phi^{(+)}\rangle\langle\Phi^{(+)}| + |\Phi^{(-)}\rangle\langle\Phi^{(-)}| = I_4 \equiv \mathrm{id}(4)$$

which leads to

$$\begin{aligned}|\phi\rangle_1|\Psi^{(-)}\rangle_{23} &= (|\Psi^{(-)}\rangle\langle\Psi^{(-)}| + |\Psi^{(+)}\rangle\langle\Psi^{(+)}| + |\Phi^{(-)}\rangle\langle\Phi^{(-)}| + |\Phi^{(+)}\rangle\langle\Phi^{(+)}|)_{12}|\phi\rangle_1|\Psi^{(-)}\rangle_{23}\\ &= |\Psi^{(-)}\rangle_{12}({}_{12}\langle\Psi^{(-)}|\phi\rangle_1|\Psi^{(-)}\rangle_{23}) + |\Psi^{(+)}\rangle_{12}({}_{12}\langle\Psi^{(+)}|\phi\rangle_1|\Psi^{(-)}\rangle_{23})\\ &+ |\Phi^{(-)}\rangle_{12}({}_{12}\langle\Phi^{(-)}|\phi\rangle_1|\Psi^{(-)}\rangle_{23}) + |\Phi^{(+)}\rangle_{12}({}_{12}\langle\Phi^{(+)}|\phi\rangle_1|\Psi^{(-)}\rangle_{23})\end{aligned}$$

Term 1:

$$\begin{aligned}{}_{12}\langle\Psi^{(-)}|\phi\rangle_1|\Psi^{(-)}\rangle_{23} &= \frac{1}{\sqrt{2}}({}_{12}\langle HV| - {}_{12}\langle VH|)(a|H\rangle_1 + b|V\rangle_1)\frac{1}{\sqrt{2}}(|HV\rangle_{23} - |VH\rangle_{23})\\ &= \frac{1}{2}\Big({}_{12}\langle\underline{HV}| - {}_{12}\langle\underline{VH}|\Big)\Big(a|HHV\rangle - a|\underline{HV}H\rangle + b|\underline{VH}V\rangle - b|VVH\rangle\Big)\\ &= \frac{1}{2}\Big(-a\,{}_{12}\langle HV|HVH\rangle - b\,{}_{12}\langle VH|VHV\rangle\Big)\\ &= -\frac{1}{2}\Big(a|H\rangle_3 + b|V\rangle_3\Big)\\ &= -\frac{1}{2}|\phi\rangle_3\end{aligned}$$

Term 2:

$$\begin{aligned}{}_{12}\langle\Psi^{(+)}|\phi\rangle_1|\Psi^{(-)}\rangle_{23} &= \frac{1}{2}\Big({}_{12}\langle\underline{HV}| +_{12}\langle\underline{VH}|\Big)\Big(a|HHV\rangle - a|\underline{HV}H\rangle + b|\underline{VH}V\rangle - b|VVH\rangle\Big)\\ &= \frac{1}{2}\Big(-a\,{}_{12}\langle HV|HVH\rangle + b\,{}_{12}\langle VH|VHV\rangle\Big)\\ &= -\frac{1}{2}(a|H\rangle_3 - b|V\rangle_3) = -\frac{1}{2}\hat{Z}|\phi\rangle_3\end{aligned}$$

since

$$\hat{Z}|\phi\rangle_3 = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}a\\ b\end{bmatrix} = \begin{bmatrix}a\\ -b\end{bmatrix} = a|H\rangle - b|V\rangle$$

Term 3:

$$\begin{aligned}{}_{12}\langle\Phi^{(-)}|\phi\rangle_1|\Psi^{(-)}\rangle_{23} &= \frac{1}{2}\Big({}_{12}\langle HH| -_{12}\langle VV|\Big)\Big(a|HHV\rangle - a|HVH\rangle + b|VHV\rangle - b|VVH\rangle\Big)\\ &= \frac{1}{2}\Big(a\,{}_{12}\langle HH|HHV\rangle + b\,{}_{12}\langle VV|VVH\rangle\Big)\\ &= \frac{1}{2}(a|V\rangle_3 + b|H\rangle_3) = \frac{1}{2}\hat{X}|\phi\rangle_3\end{aligned}$$

since

$$\hat{X}|\phi\rangle_3 = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}a\\ b\end{bmatrix} = \begin{bmatrix}b\\ a\end{bmatrix} = b|H\rangle + a|V\rangle$$

Term 4:

$$\begin{aligned}{}_{12}\langle\Phi^{(+)}|\phi\rangle_1|\Psi^{(-)}\rangle_{23} &= \frac{1}{2}\Big({}_{12}\langle HH| +_{12}\langle VV|\Big)\Big(a|HHV\rangle - a|HVH\rangle + b|VHV\rangle - b|VVH\rangle\Big)\\ &= \frac{1}{2}\Big(a\,{}_{12}\langle HH|HHV\rangle - b\,{}_{12}\langle VV|VVH\rangle\Big)\\ &= \frac{1}{2}(a|V\rangle_3 - b|H\rangle_3) = \frac{1}{2}(-i\hat{Y})|\phi\rangle_3\end{aligned}$$

since $(-i\hat{Y} = \hat{X}\hat{Z})$

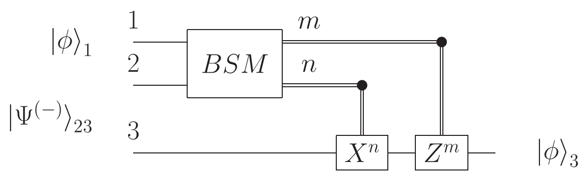
$$-i\hat{Y}|\phi\rangle_3 = -i\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}\begin{bmatrix}a\\ b\end{bmatrix} = \begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}\begin{bmatrix}a\\ b\end{bmatrix} = \begin{bmatrix}-b\\ a\end{bmatrix} = -b|H\rangle + a|V\rangle$$

thus we have

$$\begin{aligned}|\phi\rangle_1|\Psi^{(-)}\rangle_{23} &= \frac{1}{2}\Big(-|\Psi^{(-)}\rangle_{12}|\phi\rangle_3 - |\Psi^{(+)}\rangle_{12}\hat{Z}|\phi\rangle_3 + \hat{X}|\Phi^{(-)}\rangle_{12}|\phi\rangle_3 + |\Phi^{(+)}\rangle_{12}(-i\hat{Y})|\phi\rangle_3\Big)\\ &= -\frac{1}{2}\Big(|\Psi^{(-)}\rangle_{12}|\phi\rangle_3 + |\Psi^{(+)}\rangle_{12}\hat{Z}|\phi\rangle_3 - \hat{X}|\Phi^{(-)}\rangle_{12}|\phi\rangle_3 + |\Phi^{(+)}\rangle_{12}(i\hat{Y})|\phi\rangle_3\Big)\end{aligned}$$

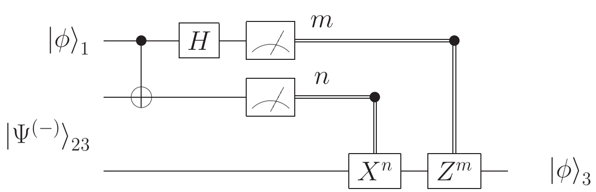
Now, Alice performs a **Bell-state measurement (BSM)**
- a projective measurement in the Bell-state basis (on particles 1 and 2).

q-circuit for quantum teleportation

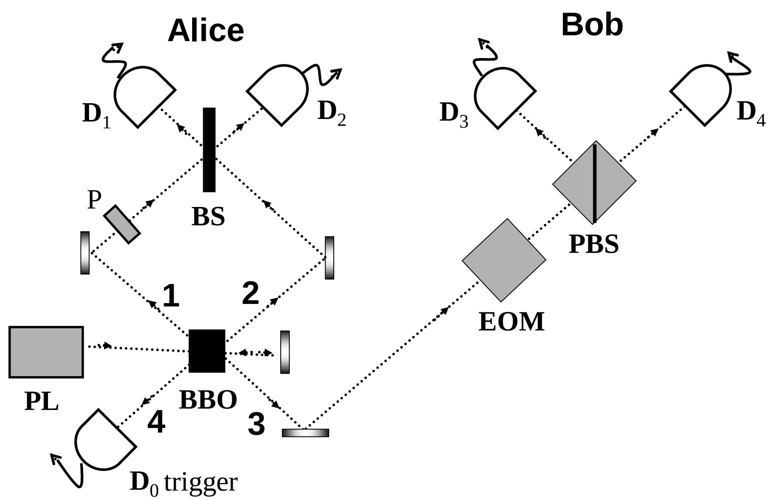


where $m, n \in \{0, 1\}$ and BSM stands for the Bell state measurement

or more explicitly



Zeilinger's experiment



teleportation across the River Danube

experiment of Zeilinger at al. (2004)

Key:

qubit – polarization states $|H\rangle$ and $|V\rangle$ of photon

F – optical fibre (length 800m) – quantum channel

RF - unit – classical channel

PL – pulsed laser (wavelength 394 nm, rate 76 MHz)

BBO – β-barium borate used to generate entangled photon pair (wavelength 788 nm) by spontaneous parametric down-conversion (**PDC**)

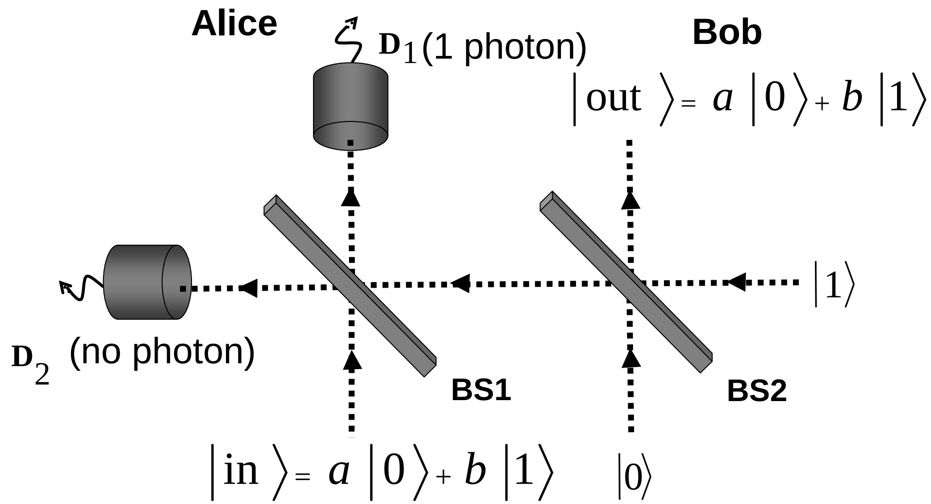
EOM – electro-optic modulator to perform Bob's unitary operation

PC – polarization controller to correct extra rotation of polarization in fibres

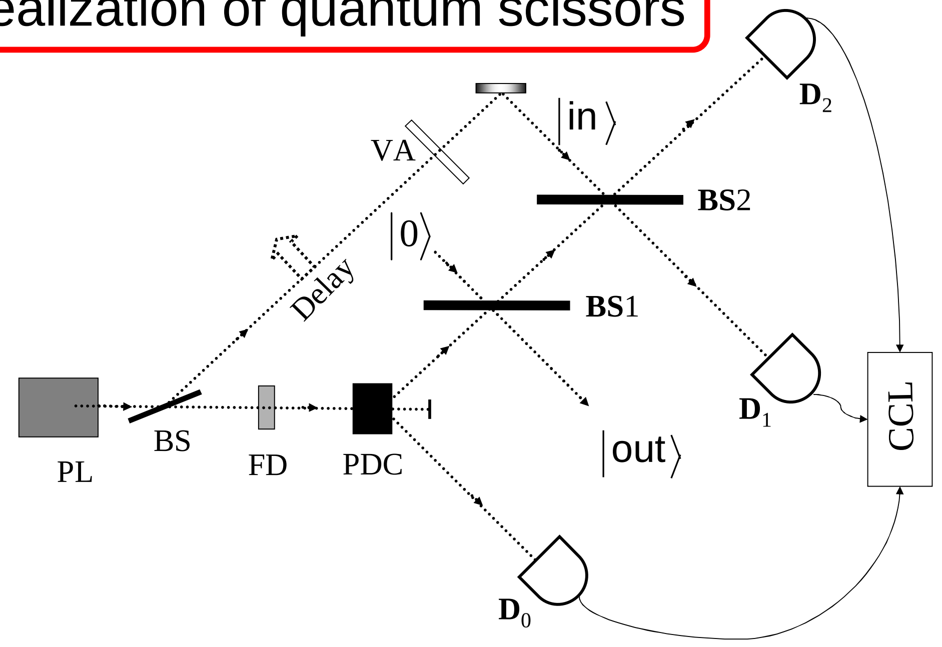
BS – beam splitter

PBS – polarizing beam splitter

teleportation of optical qubits using quantum scissors



realization of quantum scissors



experimental quantum scissors
for teleportation and generation of qubit states

Key:

PL – pulsed laser

FD – frequency doubler

PDC – parametric down conversion crystal

VA – variable attenuator with narrow-band filter

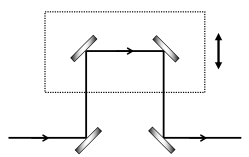
CCL – coincidence counter and logic

BS, BS1, BS2 – beam splitters

D_0, D_1, D_2 – photon-counting detectors

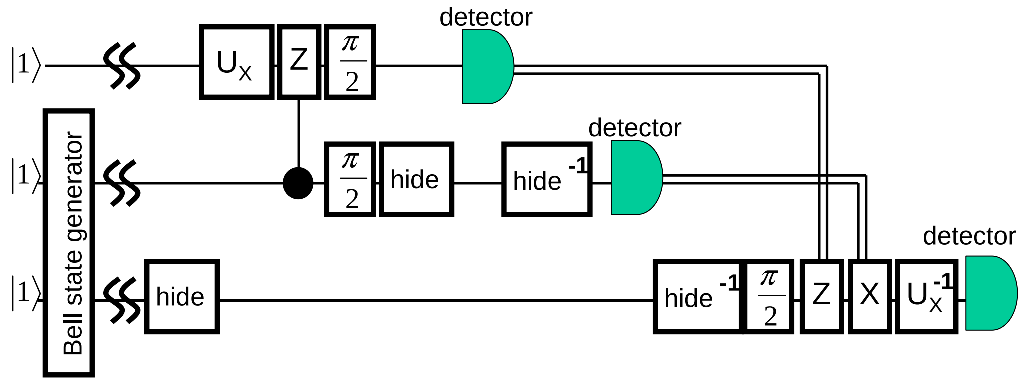
D_0 - acts as a trigger

delay - 'trombone' syste



deterministic teleportation of atomic states

experiment of Blatt et al. (2004)



Blatt et al. experiment (2004)

- 3 ions of $^{40}Ca^+$

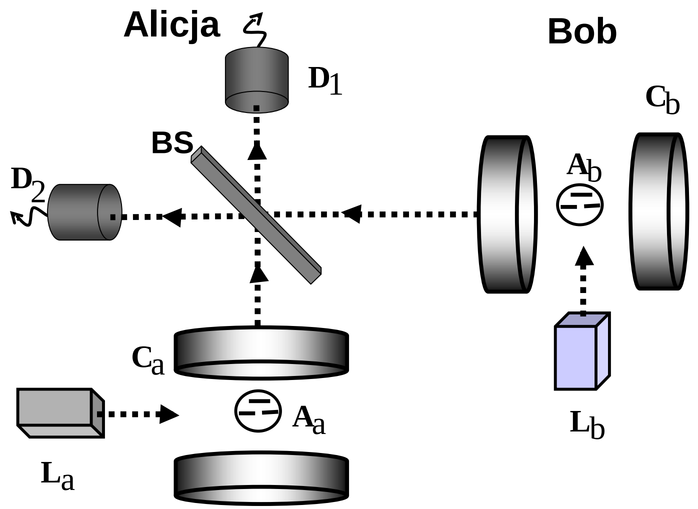
  states
  $$|1\rangle \equiv S_{1/2}(m_J = -1/2)$$
  $$|0\rangle \equiv D_{5/2}(m_J = -1/2)$$
  $$|H\rangle \equiv D_{5/2}(m_J = -5/2)$$

- $U_x|1\rangle \to |1\rangle, |0\rangle, \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{i|0\rangle + |1\rangle}{\sqrt{2}}$

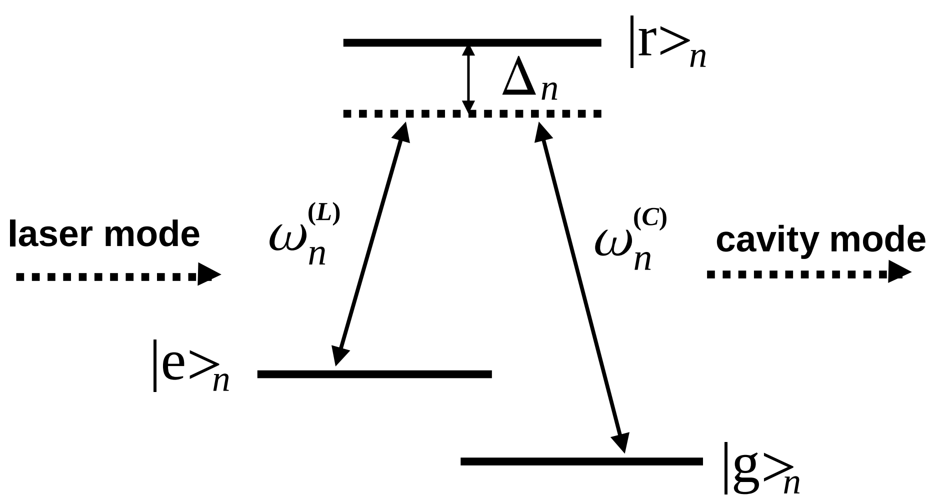
- $T_{\text{teleport}} = 2\,ms,\ T_{\text{Bell.state .lifetime}} = 100\ ms,\ T_{\text{delay}} = 10\ ms$

- fidelity: (66.7%<) 75% (<87%)

teleportation via cavity decay



3-level atom



What is the entanglement swapping?

a method to establish perfect entanglement between remote parties

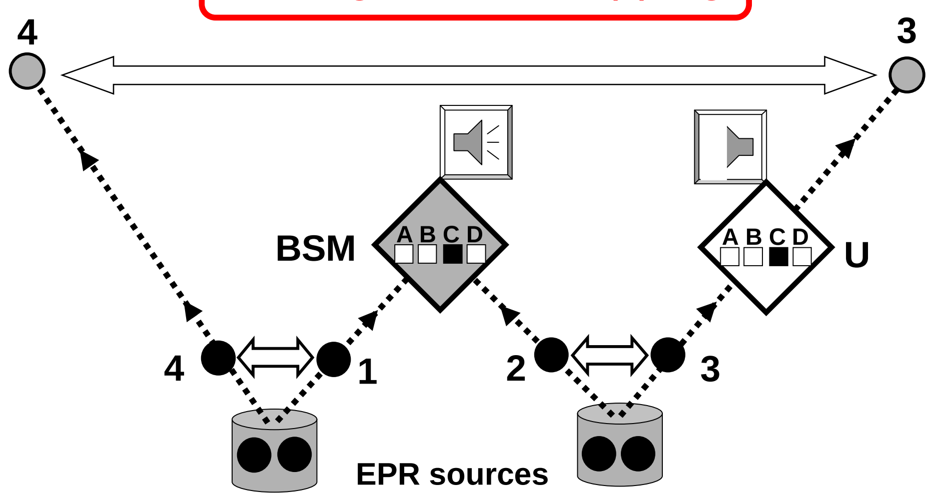
Remarks:

- it is quantum teleportation of unknown *entangled* quantum state
- *quantum repeaters* can be based on entanglement swapping

Simple description

1. Alice has particle A, Bob two particles B_1, B_2, and Claire particle C.
2. Initially particles A and B_1 are entangled, and so B_2 and C.
3. Bob performs BSM on his particles B_1 and B_2 and informs Claire about his measurement results.
4. Claire, as in the standard teleportation protocol, applies proper unitary operation to C. So, the state of B_1 is teleported to C.
5. Thus, although Alice and Claire never interacted with each other, their particles A and C are now entangled.

entanglement swapping



teleportation - theory and experiments

T 1935 quantum entanglement - Schrödinger, and Einstein, Podolsky, Rosen

T 1982 quantum no-cloning - Wootters, Żurek and Dieks

T 1993 quantum teleportation - Bennett,Brassard,Crepeau,Jozsa,Peres,Wootters

T 1993 entanglement swapping - Żukowski, Zeilinger, Horne, Ekert

E 1997 limited (conditional) optical teleportation - Zeilinger et al.

E 1998 unconditional optical teleportation - Furusawa, Kimble, Polzik et al.

E 1998 optical entanglement swapping - Zeilinger et al.

T 1999 universal quantum computation via teleportation - Gottesman and Chuang

E 2004 unconditional teleportation of atomic states
- (i) Barrett, Wineland at al. and (ii) Riebe, Blatt at al.

E 2006 unconditional teleportation between light and matter - Polzik et al.

E 2006 two-qubit teleportation - Zhang, Pan et al.

Key: **T - theory, E - experiment**

Introduction to linear-optical quantum computing

encoding optical qubits

linear-optical elements

scattering matrices

conditional measurements

optical single-qubit gates

optical two-qubit gates

a motto

efficient quantum computation with linear optics is possible!

What can be interesting about linear optics?

Can we construct a quantum computer composed only of:

- beam splitters
- phase shifters
- single-photon sources
- photodetectors

Yes!

[1] Knill, Laflamme and Milburn [Nature 2001]:

"A scheme for efficient quantum computation with linear optics"

[2] O'Brien et al. [Nature 2003]:

"[Experimental] demonstration of an all-optical quantum controlled-NOT gate"

[3] Briegel and Raussendorf [PRL 2001]:

"A one-way quantum computer"

[4] Zeilinger et al. [Nature 2005]:

"Experimental one-way quantum computing"

How to encode optical qubits

- **single-rail qubits**

logical values of qubits are encoded by number of photons

$|0\rangle_L = |0\rangle$ – vacuum

$|1\rangle_L = |1\rangle$ – single-photon state

- **two-rail qubits**

encoding in spatial modes

$|0\rangle_L = |1\rangle \otimes |0\rangle = |10\rangle$ – photon in the first mode

$|1\rangle_L = |0\rangle \otimes |1\rangle = |01\rangle$ – photon in the second mode

or vice versa

- **polarization qubits**

encoding in polarization modes of qubits

$|0\rangle_L = |H\rangle = |1_h, 0_v\rangle$ – photon with horizontal polarization

$|1\rangle_L = |V\rangle = |0_h, 1_v\rangle$ – photon with vertical polarization

or vice versa

Beam splitter (BS) = partially-transparent mirror

typical BS matrix

$$\mathrm{B}' = \begin{bmatrix} t & r \\ -r & t \end{bmatrix}, \quad \mathrm{B}'' = \begin{bmatrix} t & ir \\ ir & t \end{bmatrix}$$

the most general form of BS matrix

$$\mathrm{B} = e^{i\theta_0} \begin{bmatrix} t\exp(i\theta_t) & r\exp(i\theta_r) \\ -r\exp(-i\theta_r) & t\exp(-i\theta_t) \end{bmatrix}$$

where

t – [probability] amplitude of transmission

r – [probability] amplitude of reflection

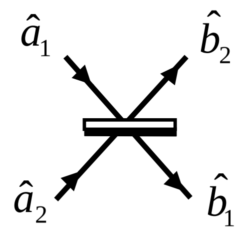
$T \equiv \tau = t^2$ – transmittance = transmittivity= transmission coefficient

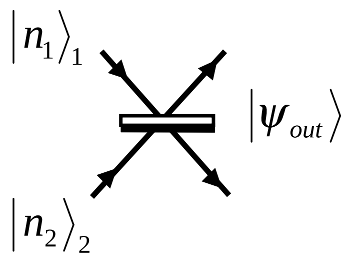
$R \equiv \rho = r^2$ – reflectance = reflectivity = reflection coefficient

$$1 = T + R = t^2 + r^2$$

$\theta_{t,r,0}$ – phase shifts

scheme of (asymmetrical) BS





$\hat{a}_{1,2}$ – annihilation operators for input modes

$\hat{b}_{1,2}$ – annihilation operators for output modes

$|\psi_{\rm out}\rangle$ - output state,

$|\psi_{\rm in}\rangle$ - input state, e.g. $|\psi_{\rm in}\rangle = |n_1\rangle_1 |n_2\rangle_2 \equiv |n_1, n_2\rangle$

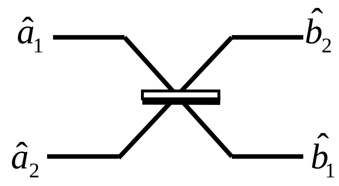
- **convention**

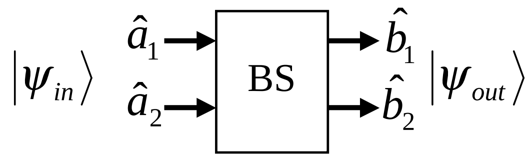
the phase of light reflected from the **'white'** surface is π-shifted

light reflected from the **'black'** surface does not change its phase

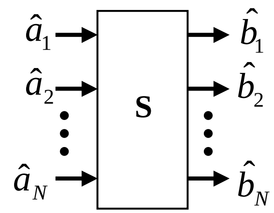
light **transmitted** from any side of BS does not change its phase

equivalent schemes of BS





linear optical multiport (MP)



S – scattering matrix

transformations of states and operators in MP

$$|\psi_{\rm out}\rangle = \hat{U}|\psi_{\rm in}\rangle$$

$$\hat{a}_i \to \hat{b}_i = \hat{U}^\dagger \hat{a}_i \hat{U} = \sum_{j=1}^{N} S_{ij}\hat{a}_j$$

where

S_{ij} – elements of unitary scattering matrix **S**

$\hat{U}$ – unitary operator describing evolution of N input modes

$\hat{a}_j$ – annihilation operator for the jth input mode

$\hat{b}_j$ – annihilation operator for the jth output mode

- in vector notation

$\hat{\mathbf{a}} \equiv [\hat{a}_1, \hat{a}_2, \ldots, \hat{a}_N]^T$

$\hat{\mathbf{b}} \equiv [\hat{b}_1, \hat{b}_2, \ldots, \hat{b}_N]^T$

for N-input Fock states

$|\psi_{\rm in}\rangle = |n_1, \ldots, n_N\rangle \equiv |\mathbf{n}\rangle$

the **MP transformations** can be written compactly:

$$\hat{\mathbf{b}} = \hat{U}^\dagger \hat{\mathbf{a}} \hat{U} = \mathbf{S}\,\hat{\mathbf{a}}$$

so

$$\hat{\mathbf{a}}^\dagger = \hat{U}\hat{\mathbf{b}}^\dagger \hat{U}^\dagger = \mathbf{S}^T \hat{\mathbf{b}}^\dagger$$

or explicitly

$$\hat{a}_i^\dagger = \sum_j S_{ji} \hat{b}_j^\dagger$$

• How to express output operators in terms of input operators without knowing explicitly $\hat{U}$?

$$\begin{aligned}\hat{U}\hat{a}_i^\dagger \hat{U}^\dagger &= \hat{U}\left(\sum_j S_{ji}\hat{b}_j^\dagger\right)\hat{U}^\dagger \\ &= \sum_j S_{ji}\hat{U}\hat{b}_j^\dagger \hat{U}^\dagger \\ &= \sum_j S_{ji}\hat{a}_j^\dagger\end{aligned}$$

general transformations in MP

input state $|\psi_{\rm in}\rangle = |n_1,\ldots,n_N\rangle \equiv |\mathbf{n}\rangle$

output state

$$\begin{aligned}|\psi_{\rm out}\rangle = \hat{U}|\psi_{\rm in}\rangle &= \hat{U}\prod_{i=1}^N \frac{(\hat{a}_i^\dagger)^{n_i}}{\sqrt{n_i!}}|\mathbf{0}\rangle = \hat{U}\frac{(\hat{a}_1^\dagger)^{n_1}}{\sqrt{n_1!}}\frac{(\hat{a}_2^\dagger)^{n_2}}{\sqrt{n_2!}}\cdots\frac{(\hat{a}_N^\dagger)^{n_N}}{\sqrt{n_N!}}|\mathbf{0}\rangle \\ &= \hat{U}\frac{(\hat{a}_1^\dagger)^{n_1}}{\sqrt{n_1!}}\hat{U}^\dagger\hat{U}\frac{(\hat{a}_2^\dagger)^{n_2}}{\sqrt{n_2!}}\hat{U}^\dagger\hat{U}\cdots\hat{U}^\dagger\hat{U}\frac{(\hat{a}_N^\dagger)^{n_N}}{\sqrt{n_N!}}\hat{U}^\dagger\hat{U}|\mathbf{0}\rangle \\ &= \prod_{i=1}^N \frac{1}{\sqrt{n_i!}}(\hat{U}\hat{a}_i^\dagger\hat{U}^\dagger)^{n_i}|\mathbf{0}\rangle \\ &= \prod_{i=1}^N \frac{1}{\sqrt{n_i!}}\left(\sum_{j=1}^N S_{ji}\hat{a}_j^\dagger\right)^{n_i}|\mathbf{0}\rangle = \frac{1}{\sqrt{n_1!\cdots n_N!}}\sum_{\mathbf{j}=1}^N\prod_{l=1}^M S_{j_l x_l}\hat{a}_{j_l}^\dagger|\mathbf{0}\rangle\end{aligned}$$

where $M=\sum_i n_i$ – is the total number of photons in system.

$\{x_l\} \equiv (\underbrace{1,...,1}_{n_1},\underbrace{2,...,2}_{n_2},...,\underbrace{N,...,N}_{n_N})$ for $l=1,...,M$

$\sum_{\mathbf{j}}$ – multiple sum $j_1, j_2, ..., j_M$

Exemplary transformations of states by beam-splitter

assuming that

$$\mathbf{S} = \mathbf{B}' = \begin{bmatrix} t & r \\ -r & t\end{bmatrix}$$

• **example 1:**

$$|\psi_{\rm in}\rangle = |10\rangle \quad\to\quad |\psi_{\rm out}\rangle = t|10\rangle - r|01\rangle$$

proof:

$$\begin{aligned}|\psi_{\rm out}\rangle &= \hat{U}|\psi_{\rm in}\rangle = \hat{U}|10\rangle = \hat{U}\hat{a}_1^\dagger|00\rangle \\ &= \hat{U}\hat{a}_1^\dagger\underbrace{\hat{U}^\dagger\hat{U}}_{=1}|00\rangle \\ &= \underbrace{\hat{U}\hat{a}_1^\dagger\hat{U}^\dagger}\underbrace{\hat{U}|00\rangle}_{=|00\rangle} \\ &= \left(\textstyle\sum_j S_{j1}\hat{a}_j^\dagger\right)|00\rangle \\ &= S_{11}\hat{a}_1^\dagger|00\rangle + S_{21}\hat{a}_2^\dagger|00\rangle = S_{11}|10\rangle + S_{21}|01\rangle \\ &= t|10\rangle - r|01\rangle\end{aligned}$$

so

$$|10\rangle \to t|10\rangle - r|01\rangle$$

in special case for **50:50 BS** (i.e., $t=r=1/\sqrt{2}$)

$$|10\rangle \to \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \equiv |\Psi^{(-)}\rangle \quad \text{(the singlet state)}$$

• **example 2:**

$$|01\rangle \to r|10\rangle + t|01\rangle$$

for 50:50 BS

$$|01\rangle \to \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \equiv |\Psi^{(+)}\rangle \quad \text{(the 'triplet' state)}$$

• **example 3:**

$$|11\rangle \to \sqrt{2}rt(|20\rangle - |02\rangle) + (t^2 - r^2)|11\rangle$$

for 50:50 BS

$$|11\rangle \to \frac{1}{\sqrt{2}}(|20\rangle - |02\rangle)$$

note: state $|11\rangle$ is not generated – it is so-called **photon coalescence** or **photon 'bunching'** (but not in Mandel's sense)

- **example 4:**

$$|20\rangle \rightarrow t^2|20\rangle - \sqrt{2}rt|11\rangle + r^2|02\rangle$$

for 50:50 BS

$$|20\rangle \rightarrow \frac{1}{2}\Big(|20\rangle - \sqrt{2}|11\rangle + |02\rangle\Big)$$

- **example 5:**

$$|21\rangle \rightarrow \sqrt{3}rt^2|30\rangle + t(t^2-2r^2)|21\rangle + (r^3-2rt^2)|12\rangle + \sqrt{3}r^2t|03\rangle$$

for 50:50 BS

$$|21\rangle \rightarrow \frac{1}{2\sqrt{2}}\Big(\sqrt{3}|30\rangle - |21\rangle - |12\rangle + \sqrt{3}|03\rangle\Big)$$

- **example 6:**

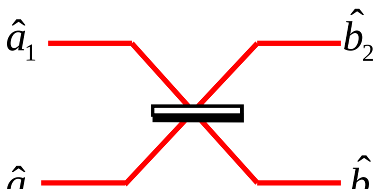
$$|22\rangle \rightarrow (r^4-4r^2t^2+t^4)|2,2\rangle + \sqrt{6}rt\Big[rt|0,4\rangle + (r^2-t^2)(|1,3\rangle - |3,1\rangle) + rt|4,0\rangle\Big]$$

for 50:50 BS

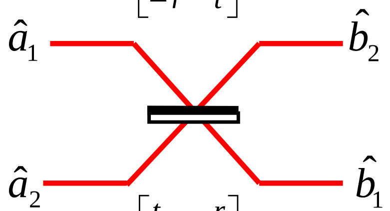
$$|22\rangle \rightarrow \frac{1}{2}\sqrt{\frac{3}{2}}\,|0,4\rangle - \frac{1}{2}\,|2,2\rangle + \frac{1}{2}\sqrt{\frac{3}{2}}\,|4,0\rangle$$

scattering matrices for BS

convention 1.

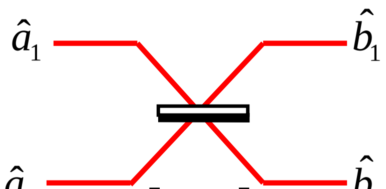


$$S = \begin{bmatrix} t & r \\ -r & t \end{bmatrix}$$

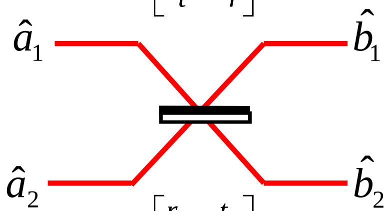


$$\begin{bmatrix} t & -r \\ r & t \end{bmatrix}$$

convention 2.

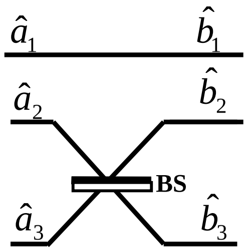


$$\begin{bmatrix} -r & t \\ t & r \end{bmatrix}$$

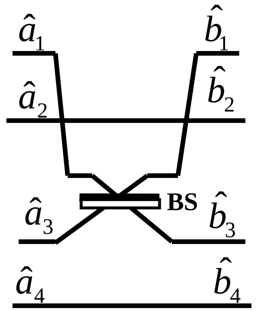


$$\begin{bmatrix} r & t \\ t & -r \end{bmatrix}$$

exemplary scattering matrices (I)

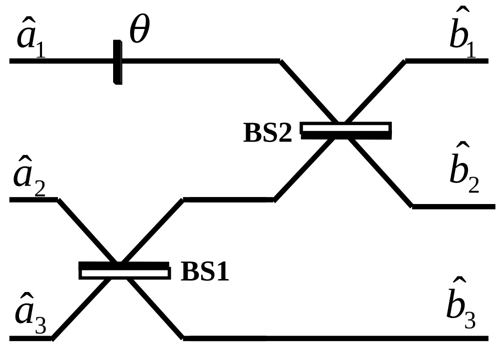


$$S = \begin{bmatrix} 1 & 0 & 0 \\ 0 & r & t \\ 0 & t & -r \end{bmatrix}$$



$$S = \begin{bmatrix} r & 0 & t & 0 \\ 0 & 1 & 0 & 0 \\ t & 0 & -r & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

exemplary scattering matrix (II)



$$S_\theta = \begin{bmatrix} e^{i\theta} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, S_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & r_1 & t_1 \\ 0 & t_1 & -r_1 \end{bmatrix}, S_2 = \begin{bmatrix} -r_2 & t_2 & 0 \\ t_2 & r_2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$S = S_2 S_\theta S_1 = S_2 S_1 S_\theta$$

von Neumann projective measurement

let us assume that the kth subsystem (e.g. mode, qubit) of a bipartite quantum system is represented by complete orthonormal set of states $|m\rangle$ then:

projector

= projection operator = projection valued (PV) measure
= orthogonal measurement operator is

$$\hat{P}_m^{(k)} = |m\rangle_{kk}\langle m|$$

for the kth subsystem corresponding to the measurement outcome m

probability of the measurement outcome m

$$\text{prob}_1(m) = \langle\psi|\hat{P}_m^{(1)} \otimes \hat{I}|\psi\rangle$$

$$\text{prob}_2(m) = \langle\psi|\hat{I} \otimes \hat{P}_m^{(2)}|\psi\rangle$$

state after projection/measurement

$$|\phi^{(1)}\rangle = \frac{\hat{P}_m^{(1)} \otimes \hat{I}|\psi\rangle}{\sqrt{\langle\psi|\hat{P}_m^{(1)} \otimes \hat{I})|\psi\rangle}}, \quad |\phi^{(2)}\rangle = \frac{\hat{I} \otimes \hat{P}_m^{(2)}|\psi\rangle}{\sqrt{\langle\psi|\hat{I} \otimes \hat{P}_m^{(2)}|\psi\rangle}}$$

where $\sqrt{\ldots}$ is the renormalization.

requirements for the projectors

non-negative, Hermitian, **orthogonal** and summing up to identity:

$$\sum_m \hat{P}_m^{(k)} \;=\; \hat{I}, \quad \hat{P}_m^{(k)} = (\hat{P}_m^{(k)})^\dagger,$$

$$_k\langle m|m'\rangle_k \;=\; \delta_{mm'}, \quad [\hat{P}_m^{(k)}, \hat{P}_{m'}^{(k')}] = 0$$

then

$$\sum_m \text{prob}(m) = 1$$

measurement outcomes corresponding to non-orthogonal states
do not commute and thus are not simultaneously observable

Note: number of projectors = dimension of Hilbert space

- **Can we apply a more general type of measurement?**

Yes!

positive operator valued measures (POVM, POM)

describe measurement outcomes associated with non-orthogonal states

... and we will discuss it later!

Example of von Neumann projective measurement

a projection synthesis via conditional measurements

general two-qubit pure state

$$|\psi\rangle = c_0|\underline{0}0\rangle + c_1|\underline{0}1\rangle + c_2|10\rangle + c_3|11\rangle$$

normalization

$$1 = |c_0|^2 + |c_1|^2 + |c_2|^2 + |c_3|^2$$

1) **probability of measuring 1st qubit in $|0\rangle$:**

$$\text{prob}_1(0) \equiv \text{prob}(|0\rangle_1) = |c_0|^2 + |c_1|^2$$

and **post measurement state** is

$$\frac{c_0|0\rangle + c_1|1\rangle}{\sqrt{|c_0|^2 + |c_1|^2}} \equiv |\phi_0\rangle$$

where $\sqrt{\ldots}$ is the renormalization.

2) probability of measuring **1st qubit in $|1\rangle$:**

$$\text{prob}(|1\rangle_1) = |c_2|^2 + |c_3|^2$$

if $|\psi\rangle = c_0|00\rangle + c_1|01\rangle + c_2|\underline{1}0\rangle + c_3|\underline{1}1\rangle$

the post measurement state is

$$\frac{c_2|0\rangle + c_3|1\rangle}{\sqrt{|c_2|^2 + |c_3|^2}} \equiv |\phi_1\rangle$$

3) probability of measuring **2nd qubit in $|0\rangle$:**

$$\text{prob}(|0\rangle_2) = |c_0|^2 + |c_2|^2$$

if $|\psi\rangle = c_0|0\underline{0}\rangle + c_1|01\rangle + c_2|1\underline{0}\rangle + c_3|11\rangle$

the post measurement state is

$$\frac{c_1|0\rangle + c_3|1\rangle}{\sqrt{|c_1|^2 + |c_3|^2}}$$

4) probability of measuring **2nd qubit in $|1\rangle$:**

- analogously

another description of projection synthesis

$$|\psi\rangle = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle$$

$$= |0\rangle \otimes (c_0|0\rangle + c_1|1\rangle) + |1\rangle \otimes (c_2|0\rangle + c_3|1\rangle)$$

$$= \underbrace{\sqrt{|c_0|^2+|c_1|^2}}\,|0\rangle \otimes \underbrace{\frac{c_0|0\rangle + c_1|1\rangle}{\sqrt{|c_0|^2+|c_1|^2}}} + \underbrace{\sqrt{|c_2|^2+|c_3|^2}}\,|1\rangle \otimes \underbrace{\frac{c_2|0\rangle + c_3|1\rangle}{\sqrt{|c_2|^2+|c_3|^2}}}$$

$$= \sqrt{\text{prob}(|0\rangle_1)}|0\rangle \otimes |\phi_0\rangle + \sqrt{\text{prob}(|1\rangle_1)}|1\rangle \otimes |\phi_1\rangle$$

projection synthesis

probabilistic quantum state engineering via conditional measurements

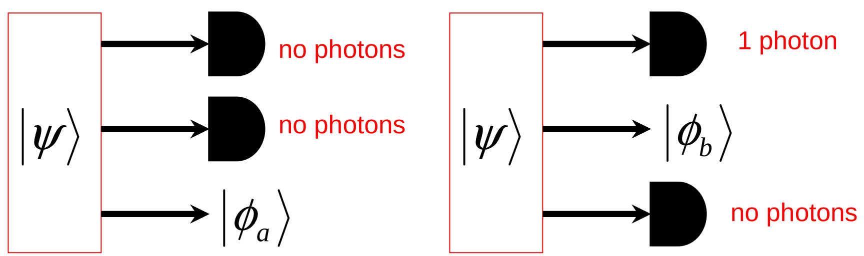
example: Let's analyze a three-mode state

$$|\psi\rangle = c_1|000\rangle + c_2|001\rangle + c_3|010\rangle + c_4|011\rangle + c_5|100\rangle + c_6|101\rangle + c_7|110\rangle + c_8|111\rangle$$

Problem: How to get single-mode states

$$|\phi_a\rangle \sim c_1|0\rangle + c_2|1\rangle \text{ and } |\phi_b\rangle \sim c_5|0\rangle + c_7|1\rangle?$$

Answer: Proper conditional measurements should be performed



- As we know, for **a two-mode system** (four-port system) holds:

$$\begin{bmatrix} \hat{a}_1^\dagger \\ \hat{a}_2^\dagger \end{bmatrix} \to \begin{bmatrix} \hat{b}_1^\dagger \\ \hat{b}_2^\dagger \end{bmatrix} = \mathbf{S}^T \begin{bmatrix} \hat{a}_1^\dagger \\ \hat{a}_2^\dagger \end{bmatrix}$$

where

$$\mathbf{S} = \begin{bmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{bmatrix} \quad \Rightarrow \quad \mathbf{S}^T = \begin{bmatrix} S_{11} & S_{21} \\ S_{12} & S_{22} \end{bmatrix}$$

e.g.

$$|10\rangle \to S_{11}\hat{a}_1^\dagger|00\rangle + S_{21}\hat{a}_2^\dagger|00\rangle = S_{11}|10\rangle + S_{21}|01\rangle$$
$$|01\rangle \to S_{12}\hat{a}_1^\dagger|00\rangle + S_{22}\hat{a}_2^\dagger|00\rangle = S_{12}|10\rangle + S_{22}|01\rangle$$

- Analogously for **a three-mode system** (six-port system) holds:

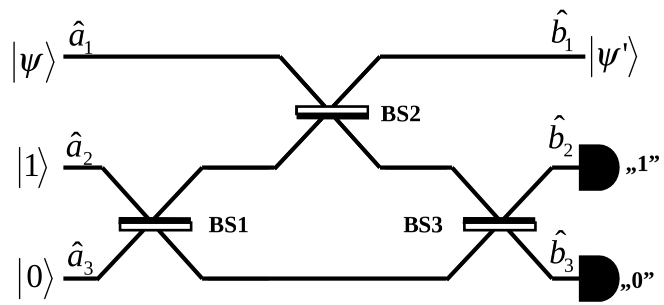
$$\begin{bmatrix} \hat{a}_1^\dagger \\ \hat{a}_2^\dagger \\ \hat{a}_3^\dagger \end{bmatrix} \to \begin{bmatrix} \hat{b}_1^\dagger \\ \hat{b}_2^\dagger \\ \hat{b}_3^\dagger \end{bmatrix} = \mathbf{S}^T \begin{bmatrix} \hat{a}_1^\dagger \\ \hat{a}_2^\dagger \\ \hat{a}_3^\dagger \end{bmatrix} = \begin{bmatrix} S_{11} & S_{21} & S_{31} \\ S_{12} & S_{22} & S_{32} \\ S_{13} & S_{23} & S_{33} \end{bmatrix} \begin{bmatrix} \hat{a}_1^\dagger \\ \hat{a}_2^\dagger \\ \hat{a}_3^\dagger \end{bmatrix}$$

e.g.

$$|100\rangle \to S_{11}\hat{a}_1^\dagger|000\rangle + S_{21}\hat{a}_2^\dagger|000\rangle + S_{31}\hat{a}_3^\dagger|000\rangle = S_{11}|100\rangle + S_{21}|010\rangle + S_{31}|001\rangle$$

nonlinear sign gate (NS)

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle + c_2|2\rangle \longrightarrow |\psi'\rangle = c_0|0\rangle + c_1|1\rangle - c_2|2\rangle$$



$$S_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & r_1 & t_1 \\ 0 & t_1 & -r_1 \end{bmatrix}, S_2 = \begin{bmatrix} -r_2 & t_2 & 0 \\ t_2 & r_2 & 0 \\ 0 & 0 & 1 \end{bmatrix}, S_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & r_3 & t_3 \\ 0 & t_3 & -r_3 \end{bmatrix}$$

$$S = S_3 S_2 S_1$$

- **scattering matrix**

Mathematica:
```
S1 := {{1, 0, 0}, {0, r1, t1}, {0, t1, -r1}}
S2 := {{-r2, t2, 0}, {t2, r2, 0}, {0, 0, 1}}
S3 := {{1, 0, 0}, {0, r3, t3}, {0, t3, -r3}}
S = S3.S2.S1
```
thus, after multiplication, one gets

$$\mathbf{S} = \begin{bmatrix} S_{11} & S_{12} & S_{13} \\ S_{21} & S_{22} & S_{23} \\ S_{31} & S_{32} & S_{33} \end{bmatrix} = \begin{bmatrix} -r_2, & t_2 r_1, & t_1 t_2 \\ t_2 r_3, & t_1 t_3 + r_1 r_2 r_3, & -t_3 r_1 + t_1 r_2 r_3 \\ t_2 t_3, & t_3 r_1 r_2 - t_1 r_3, & t_1 t_3 r_2 + r_1 r_3 \end{bmatrix} \leftrightarrow \hat{U}$$

- **probability amplitudes** $\langle n10|\hat{U}|n10\rangle$

Problem: find such reflection amplitudes r_1, r_2 and r_3 for BS that

$$\langle 010|\hat{U}|010\rangle = \langle 110|\hat{U}|110\rangle = -\langle 210|\hat{U}|210\rangle \equiv c$$

Note: transmission amplitudes for BS are calculated from $t_i = \sqrt{1 - r_i^2}$

- $|n10\rangle \longrightarrow c|n10\rangle$ **for** $n = 0$

$$\hat{U}|010\rangle = (S_{12}\hat{a}_1^\dagger + S_{22}\hat{a}_2^\dagger + S_{32}\hat{a}_3^\dagger)|000\rangle = S_{12}|100\rangle + S_{22}|010\rangle + S_{32}|001\rangle$$

so

$$\langle 010|\hat{U}|010\rangle = S_{12}\langle 010|100\rangle + S_{22}\langle 010|010\rangle + S_{32}\langle 010|001\rangle = S_{22} = t_1 t_3 + r_1 r_2 r_3 = c$$

- $|n10\rangle \longrightarrow c|n10\rangle$ **for** $n = 1$

$$\begin{aligned} \hat{U}|110\rangle &= \sum_{k,l=1}^{3} \frac{S_{k1}S_{l2}}{\sqrt{1!1!}} \hat{a}_k^\dagger \hat{a}_l^\dagger |000\rangle \\ &= (S_{11}S_{22}\hat{a}_1^\dagger \hat{a}_2^\dagger + S_{21}S_{12}\hat{a}_2^\dagger \hat{a}_1^\dagger + \cdots)|000\rangle \\ &= (S_{11}S_{22} + S_{21}S_{12})|110\rangle + \cdots \end{aligned}$$

so

$$\begin{aligned} \langle 110|\hat{U}|110\rangle &= (S_{11}S_{22} + S_{21}S_{12})\langle 110|110\rangle + \cdots \\ &= S_{11}S_{22} + S_{21}S_{12} \\ &= -r_2 c + (t_2 r_3)(t_2 r_1) \\ &= -r_2 c + r_1 r_3 t_2^2 \end{aligned}$$

- $|n10\rangle \longrightarrow -c|n10\rangle$ **for** $n = 2$

$$\begin{aligned} \hat{U}|210\rangle &= \sum_{k,l,m=1}^{3} \frac{S_{k1}S_{l1}S_{m2}}{\sqrt{2!1!}} \hat{a}_k^\dagger \hat{a}_l^\dagger \hat{a}_m^\dagger |000\rangle \\ &= \tfrac{1}{\sqrt{2}}(S_{11}^2 S_{22}\hat{a}_1^{2\dagger}\hat{a}_2^\dagger + S_{21}S_{11}S_{12}\hat{a}_2^\dagger \hat{a}_1^{2\dagger} + S_{11}S_{21}S_{12}\hat{a}_1^\dagger \hat{a}_2^\dagger \hat{a}_1^\dagger + \cdots)|000\rangle \\ &= \tfrac{1}{\sqrt{2}}(S_{11}^2 S_{22} + 2S_{11}S_{21}S_{12}) \underbrace{\hat{a}_1^{2\dagger}\hat{a}_2^\dagger|000\rangle}_{\sqrt{2}|210\rangle} + \cdots \\ &= (S_{11}^2 S_{22} + 2S_{11}S_{21}S_{12})|210\rangle + \cdots \end{aligned}$$

so

$$\begin{aligned} \langle 210|\hat{U}|210\rangle &= S_{11}^2 S_{22} + 2S_{11}S_{21}S_{12} \\ &= r_2^2 c - 2r_2(t_2 r_3)(t_2 r_1) \\ &= r_2^2 c - 2r_1 r_2 r_3 t_2^2 \end{aligned}$$

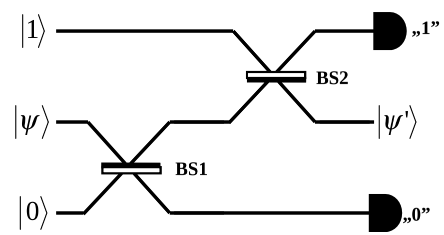
finally, we get **set of equations**

$$c = t_1 t_3 + r_1 r_2 r_3 = -r_2 c + (t_2 r_3)(t_2 r_1) = -(r_2^2 c - 2r_1 r_2 r_3 t_2^2)$$

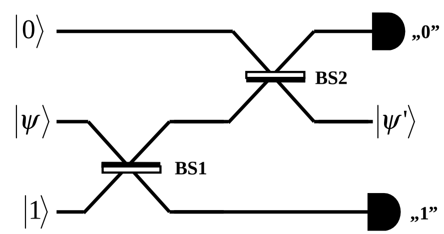
for which the solutions are $r_1 = r_3 = \frac{1}{\sqrt{4-2\sqrt{2}}}$, $r_2 = \sqrt{2} - 1$

simplified implementation of NS gate

(less number of optical elements but also lower probability of success!)

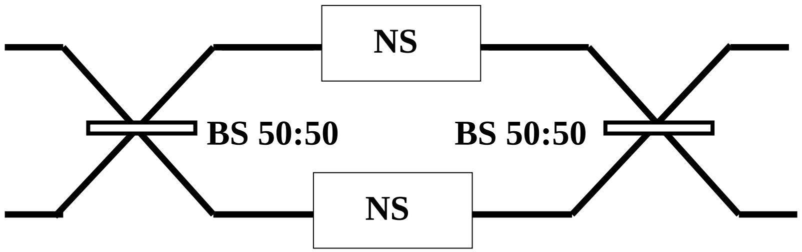


(a)

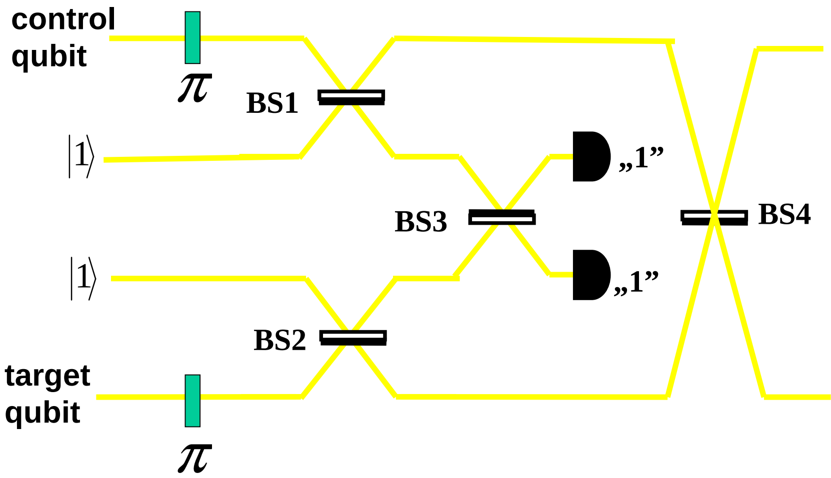


(b)

implementation of CZ gate



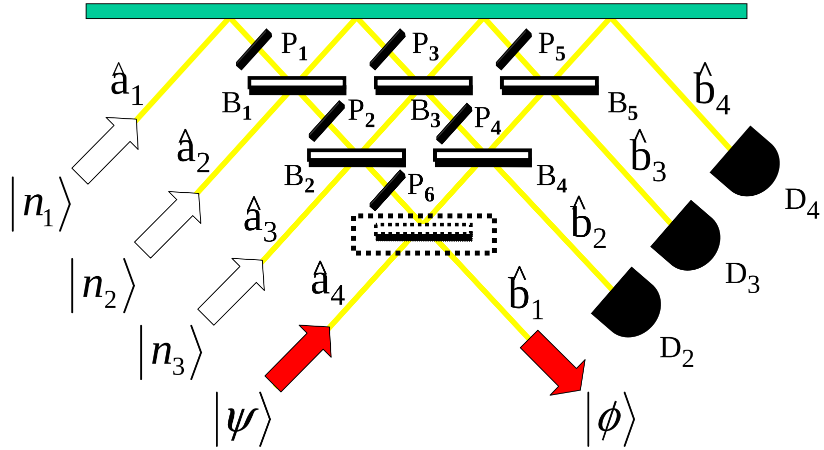
another implementation of CZ gate



transmission amplitudes for BSs:

$t_1 = t_2 = t_3 = \cos\theta$ where $\theta = 54.74$ and $t_4 = \cos\phi$ where $\phi = 17.63$

multiport Mach-Zehnder interferometer



unitary transformations

$$\mathbf{S} = \mathbf{P}_6\mathbf{B}_5\mathbf{P}_5\mathbf{B}_4\mathbf{P}_4\mathbf{B}_3\mathbf{P}_3\mathbf{B}_2\mathbf{P}_2\mathbf{B}_1\mathbf{P}_1$$

beam splitters

$$\mathrm{B}_1 = \begin{bmatrix} t_1 & r_1 & 0 & 0 \\ -r_1 & t_1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \mathrm{B}_2 = \begin{bmatrix} t_2 & 0 & r_2 & 0 \\ 0 & 1 & 0 & 0 \\ -r_2 & 0 & t_2 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \mathrm{B}_3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & t_3 & r_3 & 0 \\ 0 & -r_3 & t_3 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$\mathrm{B}_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & t_4 & 0 & r_4 \\ 0 & 0 & 1 & 0 \\ 0 & -r_4 & 0 & t_4 \end{bmatrix}, \quad \mathrm{B}_5 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & t_5 & r_5 \\ 0 & 0 & -r_5 & t_5 \end{bmatrix}$$

phase shifters

$$\begin{aligned} \mathbf{P}_k &= \mathrm{diag}[\exp(i\xi_k), 1, 1, 1] \quad \text{dla} \quad k = 1, 2, 6, \\ \mathbf{P}_k &= \mathrm{diag}[1, \exp(i\xi_k), 1, 1] \quad \text{dla} \quad k = 3, 4, \\ \mathbf{P}_5 &= \mathrm{diag}[1, 1, \exp(i\xi_5), 1]. \end{aligned}$$

mirror

$$\mathbf{M}_k = \mathrm{diag}[\exp(i\zeta\delta_{1k}), \exp(i\zeta\delta_{2k}), \exp(i\zeta\delta_{3k}), \exp(i\zeta\delta_{4k})]$$

projection synthesis

output state

$$|\phi_{\rm out}\rangle_{\mathbf 1} = \mathcal{N}\,{}_2\langle N_2|\,{}_3\langle N_3|\,{}_4\langle N_4|\hat U|n_1\rangle_1|n_2\rangle_2|n_3\rangle_3|\psi_{\rm in}\rangle_{\mathbf 4} = \mathcal{N}\sum_{n=0}^{d-1} c_n^{(d)}\gamma_{\mathbf n}|n\rangle$$

where amplitudes

$$c_n^{(d)}(\mathbf{T},\boldsymbol{\xi}) = \langle nN_2N_3N_4|\hat U|n_1n_2n_3n\rangle$$

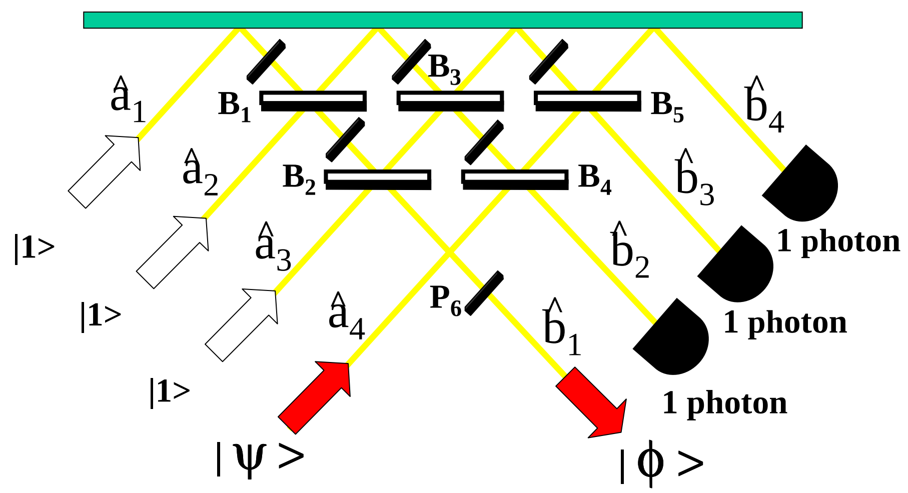
depend on:

transmittances T $\equiv [t_1^2, t_2^2, t_3^2, t_4^2, t_5^2]$

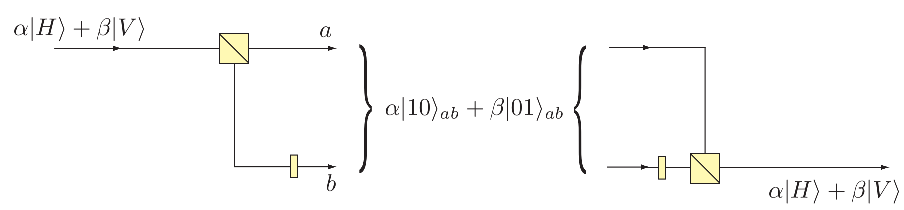
phase shifts $\boldsymbol{\xi} \equiv [\xi_1,\xi_2,\xi_3,\xi_4,\xi_5]$

input Fock states $|n_1\rangle$, $|n_2\rangle$ and $|n_3\rangle_3$

measurements results N_2, N_3, N_4



interchanging polarization qubits and two-rail qubits



PBS

– polarizing beam splitter (e.g. calcite crystal)

transmits $|H\rangle$ and reflects $|V\rangle$ (or vice versa)

HWP($\pi/4$)

– half-wave plate (polarization rotator)

changes photon polarization $|V\rangle \leftrightarrow |H\rangle$.

How to rotate polarization qubits?
wave plate = waveplate = retarder

a birefringent crystal (with a properly chosen thickness)

changes polarization of a light

by shifting its phase between two perpendicular polarization components.

half-wave plate (HWP)

$$\hat S_{\lambda/2}(\beta) = \begin{bmatrix} \cos(2\beta) & \sin(2\beta) \\ \sin(2\beta) & -\cos(2\beta) \end{bmatrix}$$

quarter-wave plate (QWP)

$$\hat S_{\lambda/4}(\beta) = \frac{\exp\left(i\frac{3}{4}\pi\right)}{\sqrt 2}\begin{bmatrix} \cos(2\beta)-i & \sin(2\beta) \\ \sin(2\beta) & -\cos(2\beta)-i \end{bmatrix}$$

special values β for HWP

$$\hat{S}_{\lambda/2}(\beta) = \begin{bmatrix} \cos(2\beta) & \sin(2\beta) \\ \sin(2\beta) & -\cos(2\beta) \end{bmatrix}$$

NOT gate = Pauli X gate = bit flip

$$\hat{S}_{\lambda/2}(\pi/4) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \equiv \hat{\sigma}_X$$

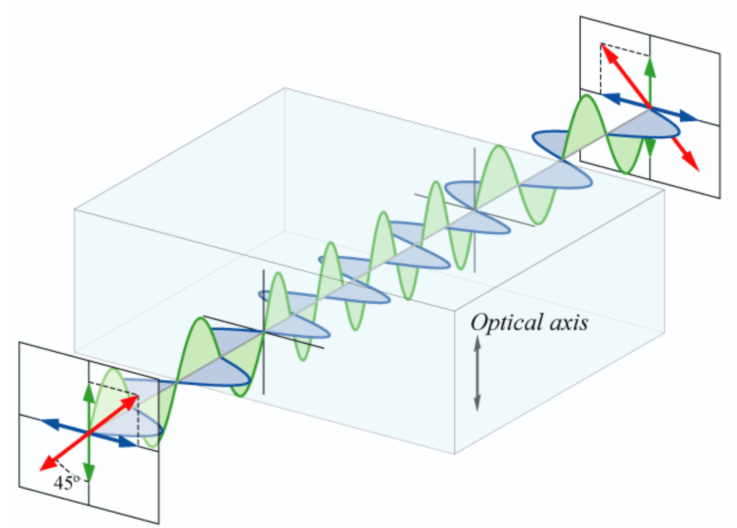
Pauli Z gate = phase flip

$$\hat{S}_{\lambda/2}(0) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \equiv \hat{\sigma}_Z$$

Hadamard gate

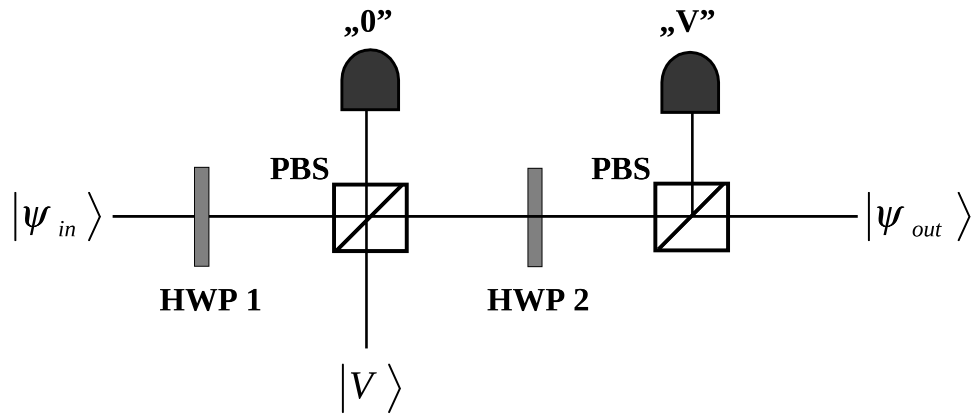
$$\hat{S}_{\lambda/2}(\pi/8) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \equiv \hat{H}$$

rotation of polarization in a waveplate



source: Wikipedia

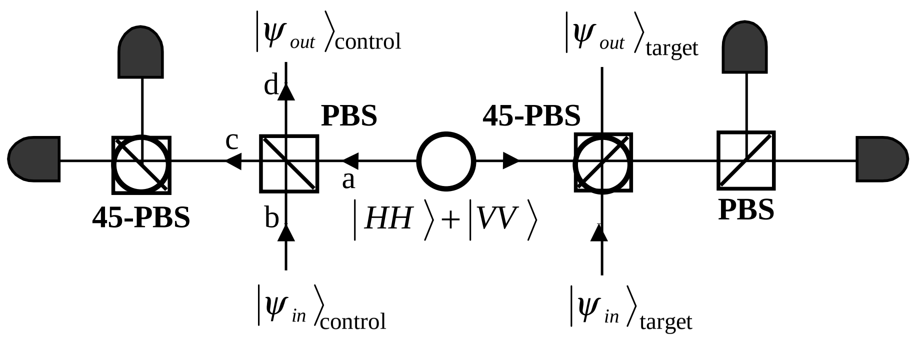
implementation of polarization NS gate



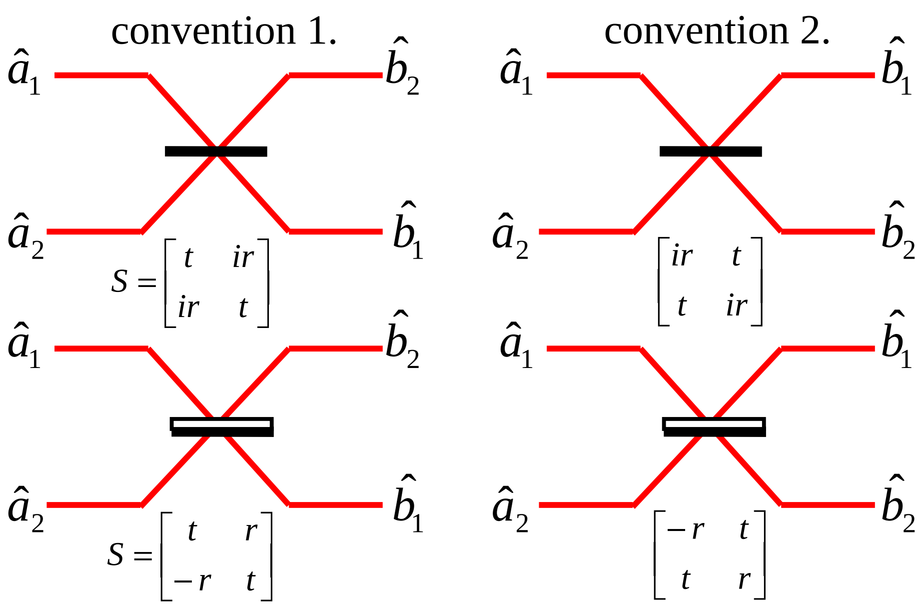
$\beta \approx 150.5^0$ for HWP1

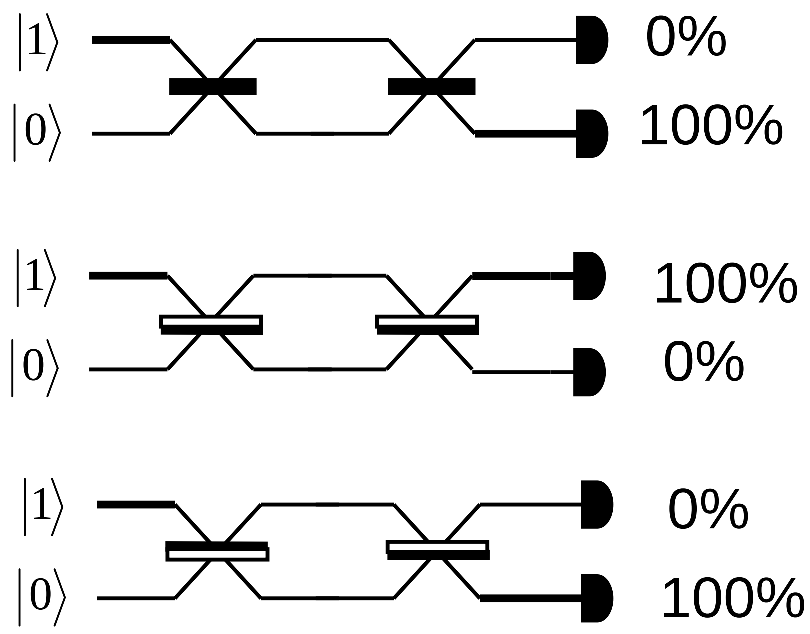
$\beta \approx 61.5^0$ for HWP2

implementation of polarization CNOT gate



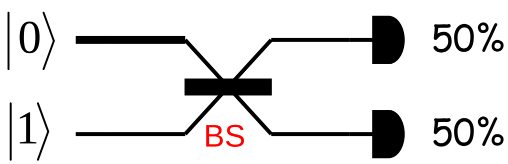
symmetric vs asymmetric BSs



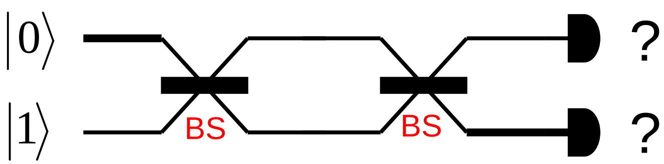


beam-splitter and interference

classical coin tossing

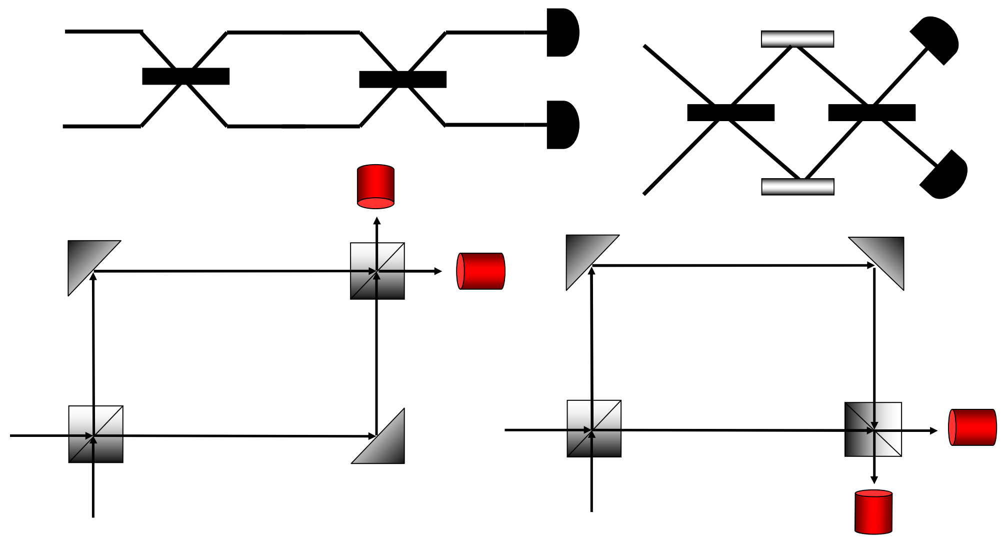


but here classical intuition fails



(all BSs are 50-50)

symmetric Mach-Zehnder interferometers



a single photon in Mach-Zehnder interferometer

We have already shown that 2x2 scattering matrix

$$S = \begin{bmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{bmatrix}$$

transforms

$$|10\rangle \longrightarrow S_{11}|10\rangle + S_{21}|01\rangle.$$

Equivalently, in terms of **two-rail qubit** notation

$$|10\rangle \equiv |0\rangle_L, \quad |01\rangle \equiv |1\rangle_L$$

one gets

$$|0\rangle_L \to S_{11}|0\rangle_L + S_{21}|1\rangle_L.$$

setup 1:

$$B_1 = B_2 = \frac{1}{\sqrt{2}}\begin{bmatrix} i & 1 \\ 1 & i \end{bmatrix}$$

this is the $\sqrt{NOT}$ **gate!**

as

$$S = B_2 B_1 = \frac{1}{2}\begin{bmatrix} i & 1 \\ 1 & i \end{bmatrix}\begin{bmatrix} i & 1 \\ 1 & i \end{bmatrix} = i\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = i\hat{X}$$

$$|0\rangle_L \to i|1\rangle_L \cong |1\rangle_L$$

setup 2:

$$B_1 = B_2 = \frac{1}{\sqrt{2}}\begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}$$

so

$$S = B_2 B_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \hat{I}$$

$$|0\rangle_L \to |0\rangle_L.$$

setup 3:

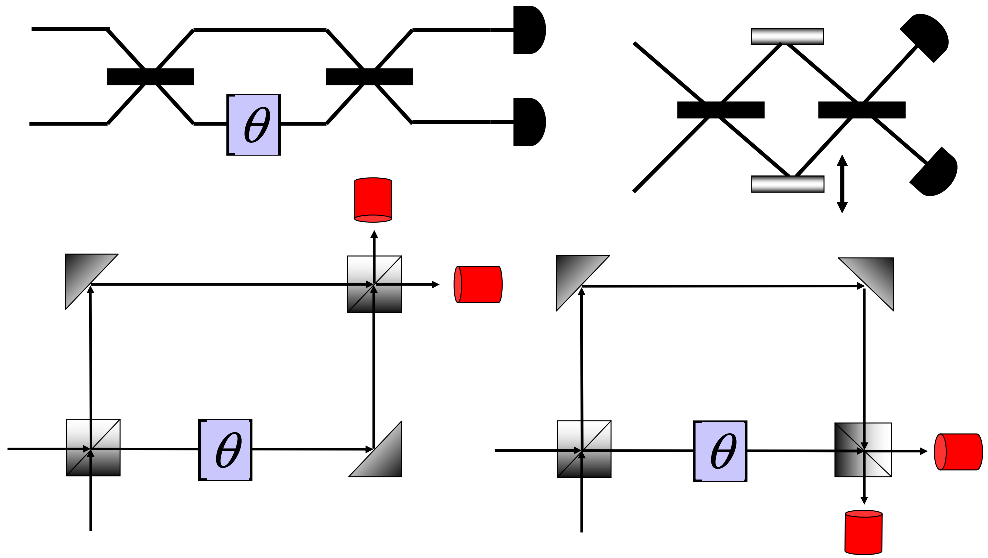
$$B_1 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad B_2 = \frac{1}{\sqrt{2}}\begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}$$

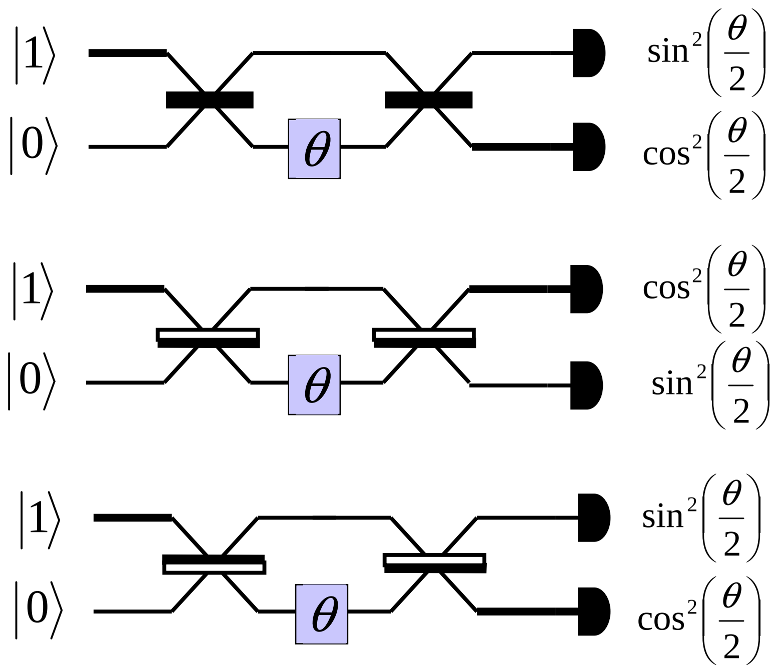
so

$$S = B_2 B_1 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = -i\hat{Y}$$

$$|0\rangle_L \to |1\rangle_L.$$

Mach-Zehnder interferometers with phase shifter





Mach-Zehnder interferometer with phase shifter

$$P_\theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$$

total scattering matrix

$$S = B_2 P_\theta B_1$$

setup 1:

$$S = \frac{1}{2}\begin{bmatrix} i & 1 \\ 1 & i \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}\begin{bmatrix} i & 1 \\ 1 & i \end{bmatrix} = \begin{bmatrix} f_- & if_+ \\ if_+ & -f_- \end{bmatrix}, \quad \text{where} \quad f_\pm = \frac{1}{2}(e^{i\theta} \pm 1)$$

so

$$|0\rangle_L \to |\psi\rangle = S_{11}|0\rangle_L + S_{21}|1\rangle_L = f_-|0\rangle_L + if_+|1\rangle_L$$

or explicitly

$$|0\rangle_L \to \boxed{B_1} \to \frac{i|0\rangle_L + |1\rangle_L}{\sqrt{2}} \to \boxed{P_\theta} \to \frac{i|0\rangle_L + e^{i\theta}|1\rangle_L}{\sqrt{2}} \to \boxed{B_2} \to f_-|0\rangle_L + if_+|1\rangle_L$$

thus

$$\text{prob}(0_L) = |_L\langle 0|\psi\rangle|^2 = |f_-|^2 = \sin^2\left(\frac{\theta}{2}\right)$$ – prob. of click in upper detector

$$\text{prob}(1_L) = |_L\langle 1|\psi\rangle|^2 = |f_+|^2 = \cos^2\left(\frac{\theta}{2}\right)$$ – prob. of click in lower detector

setup 2:

$$S = \frac{1}{2}\begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}\begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} f_+ & f_- \\ f_- & f_+ \end{bmatrix}$$

so

$$|0\rangle_L \to |\psi\rangle = S_{11}|0\rangle_L + S_{21}|1\rangle_L = f_+|0\rangle_L + f_-|1\rangle_L$$

and

$$\text{prob}(0_L) = |_L\langle 0|\psi\rangle|^2 = |f_+|^2 = \cos^2\left(\frac{\theta}{2}\right)$$

$$\text{prob}(1_L) = |_L\langle 1|\psi\rangle|^2 = |f_-|^2 = \sin^2\left(\frac{\theta}{2}\right)$$

setup 3:

$$S = \frac{1}{2}\begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} f_-, & -f_+ \\ f_+, & -f_- \end{bmatrix}$$

so

$$|0\rangle_L \to f_-|0\rangle_L + f_+|1\rangle_L$$

and

$$\text{prob}(0_L) = \sin^2\left(\frac{\theta}{2}\right)$$

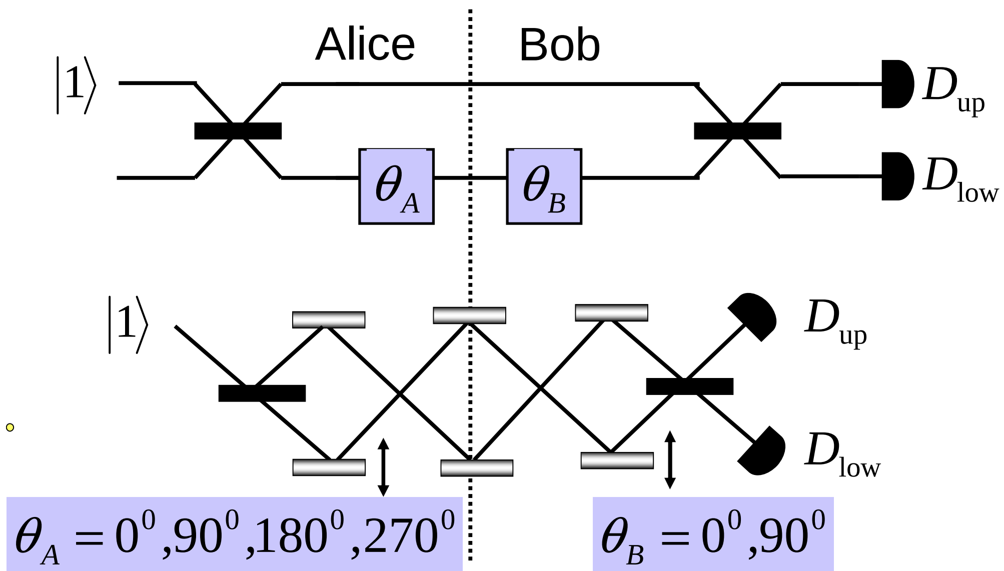
$$\text{prob}(1_L) = \cos^2\left(\frac{\theta}{2}\right)$$

QIP with simple linear-optical systems

1. quantum key distribution (QKD)
based on Mach-Zehnder interferometer
using Bennett's protocol B92

2. quantum-state engineering and teleportation
of qubit and qutrit states
using quantum scissors device

B92 protocol (Bennett 1992)



quantum key distribution (QKD) using B92 protocol

probabilities of click in upper and lower detectors

$$P_{\text{up}} = \sin^2\left(\frac{\theta_A+\theta_B}{2}\right), \quad P_{\text{low}} = \cos^2\left(\frac{\theta_A+\theta_B}{2}\right)$$

θ_A	θ_B	P_{up}	P_{low}	bit
0^o	0^o	0	1	1
0^o	90^o	$\frac{1}{2}$	$\frac{1}{2}$	–
90^o	0^o	$\frac{1}{2}$	$\frac{1}{2}$	–
90^o	90^o	1	0	0
180^o	0^o	1	0	0
180^o	90^o	$\frac{1}{2}$	$\frac{1}{2}$	–
270^o	0^o	$\frac{1}{2}$	$\frac{1}{2}$	–
270^o	90^o	0	1	1

QKD using B92 protocol

1. Alice sends photons each time randomly choosing one of 4 phase shifts (rotations): 0^o, 90^o 180^o, 270^o.
2. Bob, just before measuring each Alice's photon, randomly applies phase shift 90^o or 0^o.
3. Bob through a public channel informs Alice about his phase shifts without, of course, telling his measurement outcomes.
4. Alice publicly informs Bob, when their phase shifts fulfill the condition

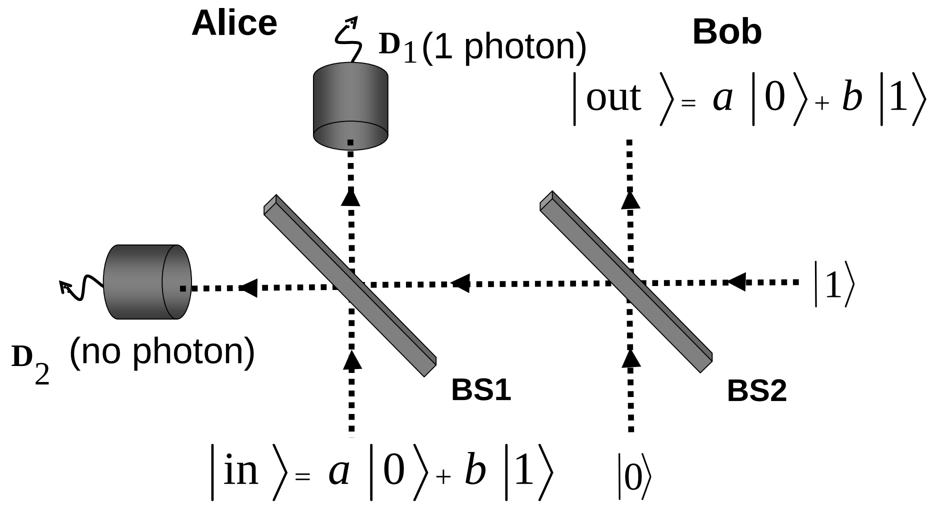
   $$\theta_A - \theta_B = n\,180^o \quad (n = 0, 1),$$

   which implies the deterministic detection of photons.

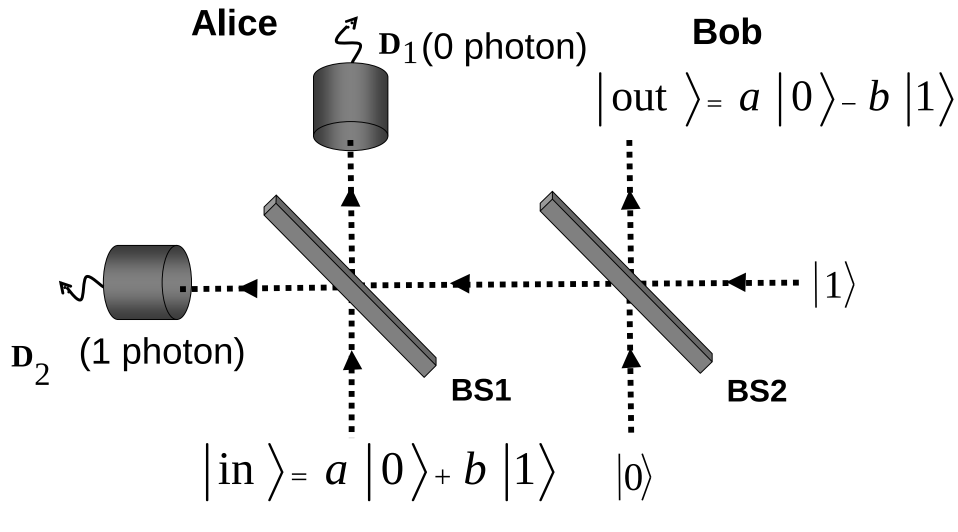
   Alice and Bob keep only those deterministic results.
5. Alice and Bob publicly check their results for some photons.

   Those photons are rejected from the key.
6. In case of full agreement of the tested photons, the secret key is formed by the remaining bits. Otherwise the protocol is repeated.

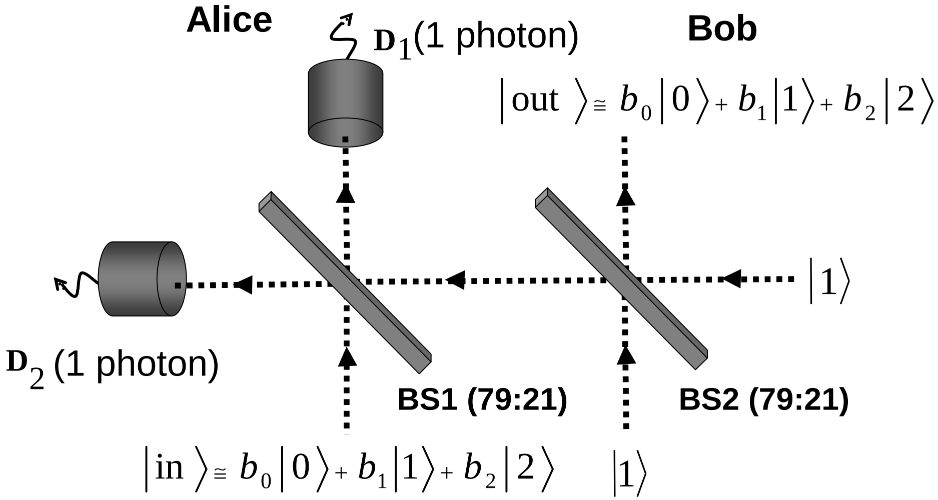
teleportation of optical qubits using quantum scissors



phase flip in teleportation



teleportation of optical qutrits



quantum scissors

Input: coherent state

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$$
$$= e^{-|\alpha|^2/2} \left\{ |0\rangle + \alpha|1\rangle + \frac{\alpha^2}{\sqrt{2}}|2\rangle + ... \right\}$$

Output: qubit state

$$|\Phi\rangle = \frac{|0\rangle + \alpha|1\rangle}{\sqrt{1+|\alpha|^2}}$$

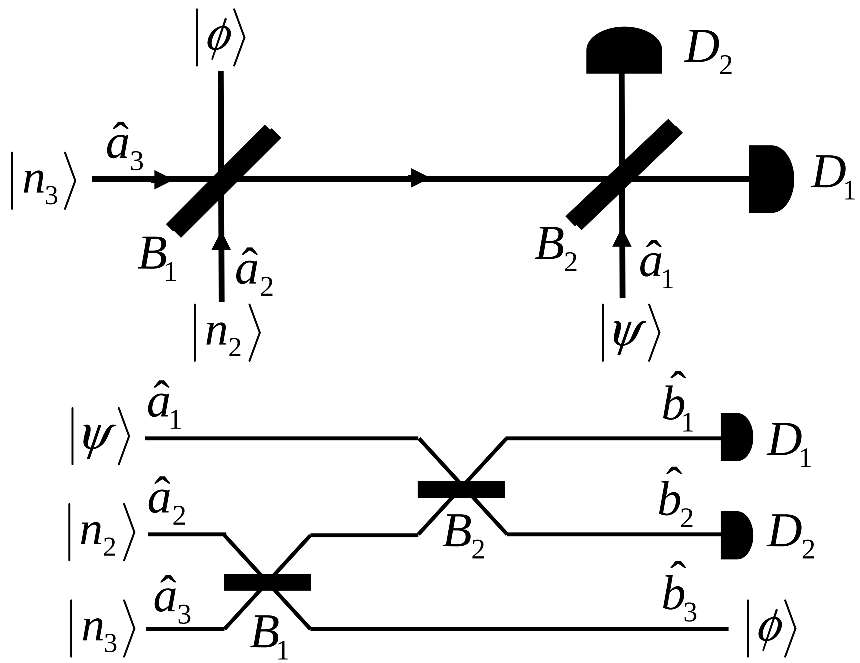
quantum scissors device

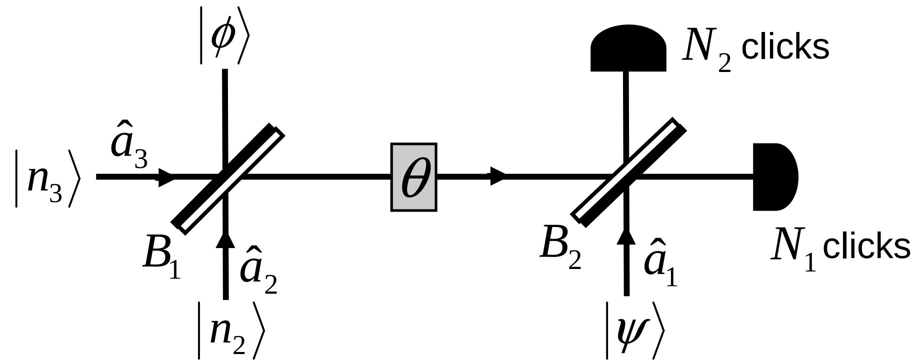
Fundamental Concepts

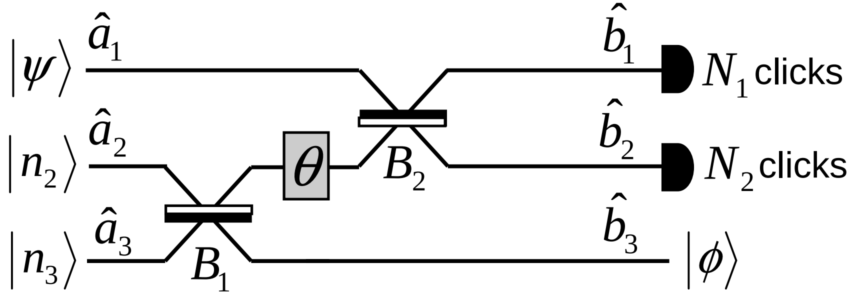
- Entanglement
- Non-locality
- Conditional measurement

Possible Applications

- Qubit generation
- Teleportation of superposition states
- Quantum state engineering
- Conversion of a classical state into a non-classical one
- Cryptography







output states of the quantum scissors

input state:

$$|\psi, n_2, n_3\rangle \text{ where } |\psi\rangle \sim \gamma_0|0\rangle + \gamma_1|1\rangle$$

three-mode output state (before projection):

$$|\Phi\rangle$$

single-mode output state:

$$|\phi\rangle \equiv |\phi^{N_1 N_2}_{n_2 n_3}\rangle =_1 \langle N_1|\,_2\langle N_2|\Phi\rangle$$

after projective measurements of N_1 and N_2 photons in the respective modes.

Example for $|\phi^{01}_{10}\rangle$:

- $|n10\rangle \to c|01n\rangle$ **for** $n = 0$

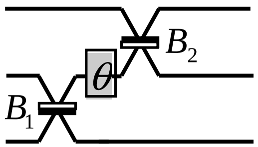
$$\begin{aligned} U|010\rangle &= (S_{12}\hat{a}_1^\dagger + S_{22}\hat{a}_2^\dagger + S_{32}\hat{a}_3^\dagger)|000\rangle \\ &= S_{12}|100\rangle + S_{22}|010\rangle + S_{32}|001\rangle \end{aligned}$$

so

$$\langle 010|\hat{U}|010\rangle = S_{22} = e^{i\theta} r_1 r_2$$

scattering matrix for quantum scissors

$$B_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -r_1 & t_1 \\ 0 & t_1 & r_1 \end{bmatrix}, P_\theta = \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{i\theta} & 0 \\ 0 & 0 & 1 \end{bmatrix}, B_2 = \begin{bmatrix} r_2 & t_2 & 0 \\ t_2 & -r_2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$



$$S = B_2 P_\theta B_1 = \begin{bmatrix} r_2 & -e^{i\theta} r_1 t_2 & e^{i\theta} t_1 t_2 \\ t_2 & e^{i\theta} r_1 r_2 & -e^{i\theta} r_2 t_1 \\ 0 & t_1 & r_1 \end{bmatrix}$$

Mathematica:

```
B1 := {{1, 0, 0}, {0, -r1, t1}, {0, t1, r1}}
B2 := {{r2, t2, 0}, {t2, -r2, 0}, {0, 0, 1}}
P := {{1, 0, 0}, {0, Exp[i*theta], 0}, {0, 0, 1}}
S = B2.P.B1 // MatrixForm
```


- $|n10\rangle \to c|01n\rangle$ **for** $n = 1$

$$\hat{U}|110\rangle = \sum_{k,l=1}^{3} \frac{S_{k1}S_{l2}}{\sqrt{1!1!}} \hat{a}_k^\dagger \hat{a}_l^\dagger |000\rangle = (S_{21}S_{32}\hat{a}_2^\dagger \hat{a}_3^\dagger + S_{31}S_{22}\hat{a}_3^\dagger \hat{a}_2^\dagger + \cdots)|000\rangle$$

$$= (S_{21}S_{32} + S_{31}S_{22})|011\rangle + \cdots$$

so

$$\langle 011|\hat{U}|110\rangle = S_{21}S_{32} + S_{31}S_{22} = t_2 t_1 + 0 \cdot S_{22} = t_1 t_2$$

thus we have

$$|\phi^{01}_{10}\rangle \sim e^{i\theta} r_1 r_2 \gamma_0|0\rangle + t_1 t_2 \gamma_1|1\rangle$$

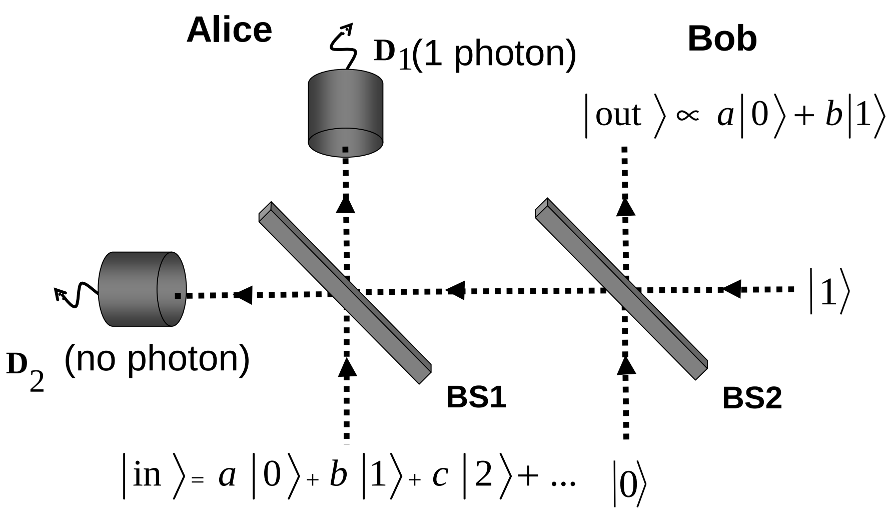
where $x \sim y$ means that x and y are equal up a renormalization constant.

Other examples

Analogously, we can show

$$\begin{aligned} |\phi^{10}_{01}\rangle &\sim e^{i\theta} t_1 t_2 \gamma_0|0\rangle + r_1 r_2 \gamma_1|1\rangle, \\ |\phi^{01}_{01}\rangle &\sim -e^{i\theta} t_1 r_2 \gamma_0|0\rangle + r_1 t_2 \gamma_1|1\rangle, \\ |\phi^{10}_{10}\rangle &\sim -e^{i\theta} r_1 t_2 \gamma_0|0\rangle + t_1 r_4 \gamma_1|1\rangle \end{aligned}$$

PPB quantum scissors
- truncation and teleportation of qubit states



quantum state truncation to qubit states

Note that the same solutions are for

$|\psi\rangle \sim \gamma_0|0\rangle + \gamma_1|1\rangle + \gamma_2|2\rangle + \cdots$

Why?

Since, in this case, the single-mode output state $|\phi\rangle$ is always a superposition of $|0\rangle$ and $|1\rangle$ for any $|\psi\rangle$.

conditions for perfect qubit-state truncation and teleportation

$t_1 = r_2$ and $\theta = 0$ for $|\phi_{10}^{01}\rangle$ and $|\phi_{01}^{10}\rangle$

$t_1 = t_2$ and $\theta = \pi$ for $|\phi_{01}^{01}\rangle$ and $|\phi_{10}^{10}\rangle$

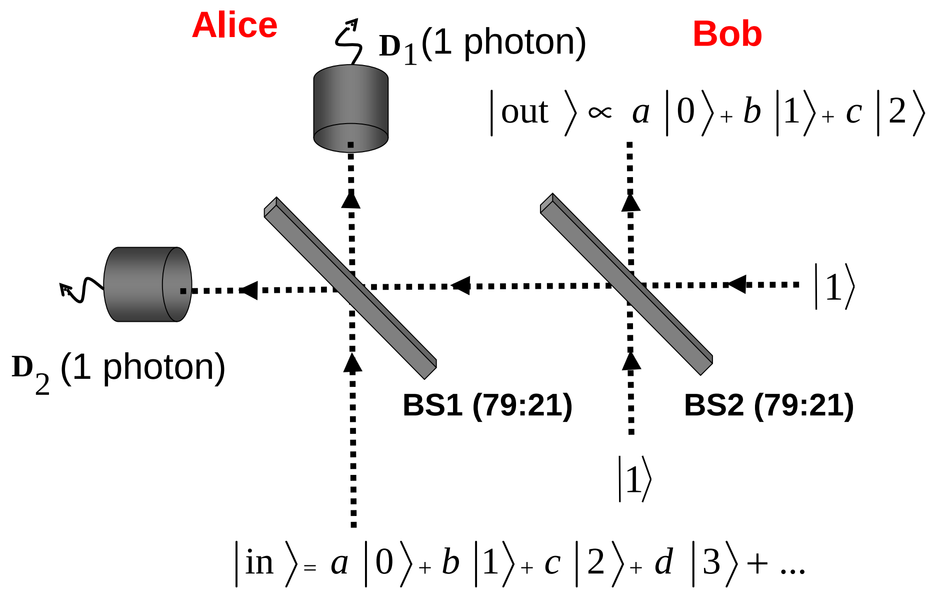
optimized solutions

correspond to the highest probability of successful truncation and teleportation.

In the all 4 cases, the optimized solutions are for the 50:50 BSs:

$$t_1 = t_2 = \frac{1}{\sqrt{2}}$$

truncation and teleportation of qutrit states



quantum scissors for qutrit states

$$|\phi\rangle \sim \gamma_0|0\rangle + \gamma_1|1\rangle + \gamma_2|2\rangle$$

general output state

assuming $n_1 = n_2 = N_1 = N_2 = 1$ is

$$|\phi_{11}^{11}\rangle \sim 2r_1t_1r_2t_2\left(e^{2i\theta_2}\gamma_0|0\rangle + \gamma_2|2\rangle\right) + e^{i\xi_2}(r_1^2 - t_1^2)(r_2^2 - t_2^2)\gamma_1|1\rangle$$

as can be shown analogously to $|\phi_{10}^{01}\rangle$.

truncation and teleportation to qutrit states

corresponds to $|\phi_{11}^{11}\rangle$ assuming

$$t_2^2 = \frac{1}{2}\left(1 \pm \frac{r_1t_1}{\sqrt{1-3(r_1t_1)^2}}\right)$$

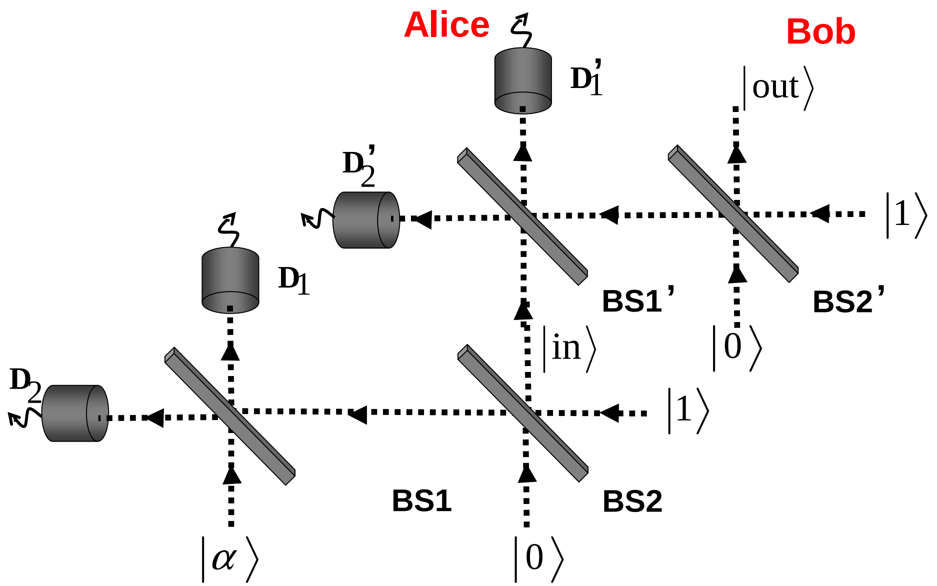
and $\theta_2 = 0$ or $= \pi$ (show this!).

optimized 4 solutions

for $t_1^2 = \frac{1}{6}(3-\sqrt{3}) \approx 0.21$ or $t_1^2 = \frac{1}{6}(3+\sqrt{3})/6 \approx 0.79$

and $t_2^2 = t_1^2$ if $\xi_4 = 0$ or $t_2^2 = 1 - t_1^2$ if $\xi_4 = \pi$.

generation and teleportation of qubit states



Introduction to quantum tomography

How to reconstruct density matrix of a quantum state?

Outline

1. optical-homodyne tomography of a single-mode field
2. tomography of a single qubit
3. tomography of two qubits
4. maximum-likelihood method
5. tomography of a single qu*d*it
6. tomography of nuclear spins I=1/2
7. tomography of a nuclear spin I=3/2

Plato's allegory

We are like slaves in a dark cave watching only shadows on a wall. The shadows are projections of the "real things". We think the shadows are real because we do not know better.

[$\Pi\lambda\alpha\tau\omega\nu o\varsigma$ $\Pi o\lambda\iota\tau\epsilon\iota\alpha$ - Plato's *Republic*]

question

Can we reconstruct a hidden object ("real thing") from its shadows?

tomography

a method to reconstruct the shape of a hidden object from shadows (projections) at different angles

quantum tomography

this is the tomography applied to quantum objects

optical homodyne tomography

this is the quantum tomography based on homodyne detection for reconstruction of Wigner function of optical fields

problem

We cannot measure simultaneously q and p, thus we cannot measure directly the Wigner function $W(q,p)$.

phase-space quasiprobability distributions in quantum mechanics

uncertainty principle

makes the concept of phase space in quantum mechanics problematic:

a particle cannot simultaneously have a well defined position and momentum, thus one cannot **define a probability** that a particle has a position q and a momentum p

quasiprobability distribution functions = quasiprobabilities = quasidistributions

functions which bear some resemblance to phase-space distribution functions

useful not only as calculational tools

but can also reveal the connections between classical and quantum mechanics.

examples:

- Wigner (Wigner-Ville) W function
- Husimi (Husimi-Kano) Q function
- Glauber-Sudarshan P function
- Cahill-Glauber s-parametrized $W^{(s)}$ function

What is the Wigner function?

$$W(q,p) = \frac{1}{2\pi\hbar}\int_{-\infty}^{\infty} dx \langle q+\tfrac{x}{2}|\hat{\rho}|q-\tfrac{x}{2}\rangle \exp\left(\frac{i}{\hbar}px\right)$$

where $|q \pm \frac{x}{2}\rangle$ – eigenstates of position operator $\hat{q}$

- Wigner function can be **negative**
- **density matrix** ρ can be calculated from Wigner function.

Why is the Wigner function so important?

marginal distributions of Wigner function correspond to classical distributions

- **position distribution**

$$\mathrm{pr}(q) \equiv \langle q|\hat{\rho}|q\rangle = \int_{-\infty}^{\infty} W(q,p)dp$$

- **momentum distribution**

$$\mathrm{pr}(p) \equiv \langle p|\hat{\rho}|p\rangle = \int_{-\infty}^{\infty} W(q,p)dq$$

10 formulations of quantum mechanics:

1. matrix formalism of Heisenberg (1925)
2. wave-function formalism of Schrödinger (1926)
3. density-matrix formalism of von Neumann (1927)
4. second-quantization formalism of Dirac, Jordan and Klein (1927)
5. variational formalism of Jordan and Klein (1927)
6. **phase-space formalism of Wigner** (1932)
7. path-integral formalism of Feynman (1948)
8. pilot-wave formalism of de Broglie and Bohm (1952)
9. many-worlds interpretation (MWI) of Everett (1957)
10. action-angle quantum formalism of Hamilton and Jacobi (1983)

simple examples of Wigner function

♣ **coherent state** $|\alpha_0\rangle$:

$$W(\alpha) = \frac{2}{\pi}\exp[-2|\alpha-\alpha_0|^2]$$

where $\alpha = q + ip$

♣ **Fock state** $|n\rangle$:

$$W(\alpha) = \frac{2}{\pi}(-1)^n L_n(4|\alpha|^2)\exp[-2|\alpha|^2]$$

where $L_n(x)$ is Laguerre polynomial

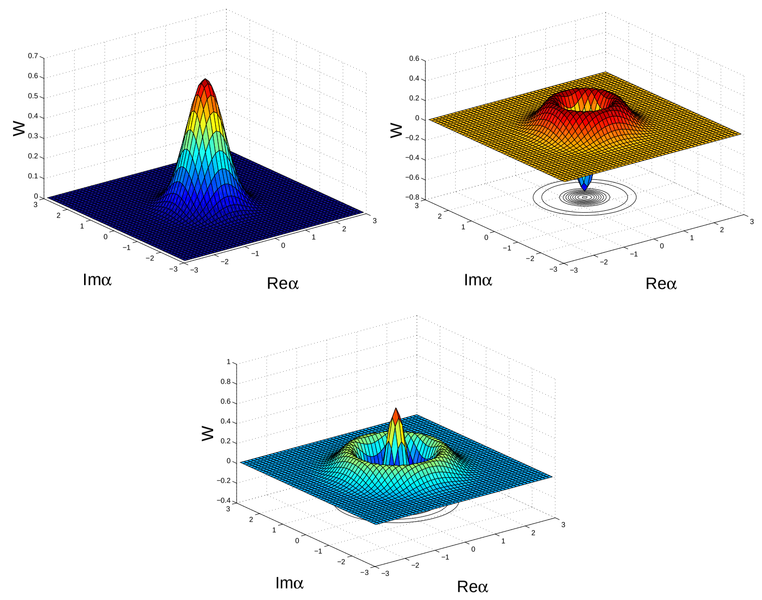
♣ **Schrödinger cat states** $|\psi_\pm\rangle \sim |\alpha_0\rangle \pm |-\alpha_0\rangle$:

$$W_\pm(\alpha = q+ip) = \frac{f_1 \pm f_0\cos(4p\alpha_0)}{\pi[1+\exp(-2\alpha_0^2)]}$$

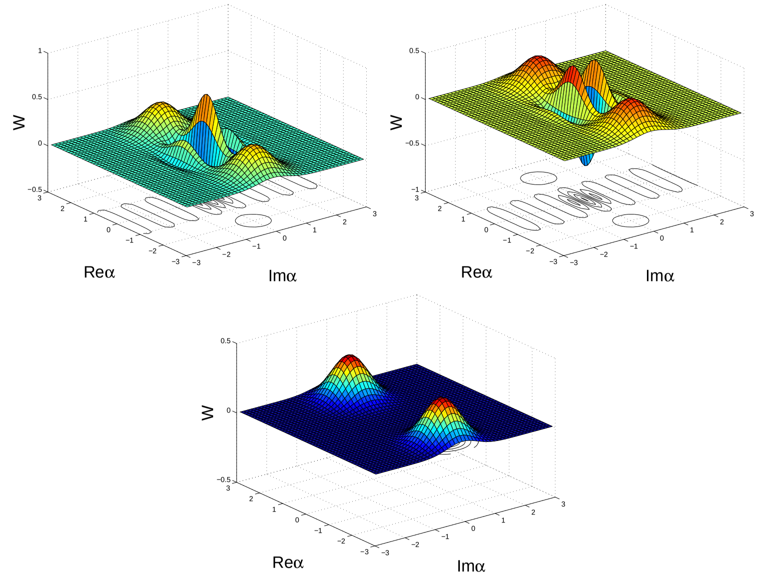
where $\alpha_0 \in \mathcal{R}$ and

$$f_1 = \exp[-2(q-\alpha_0)^2 - 2p^2] + \exp[-2(q+\alpha)^2 - 2p^2], \quad f_0 = 2\exp[-2q^2-2p^2]$$

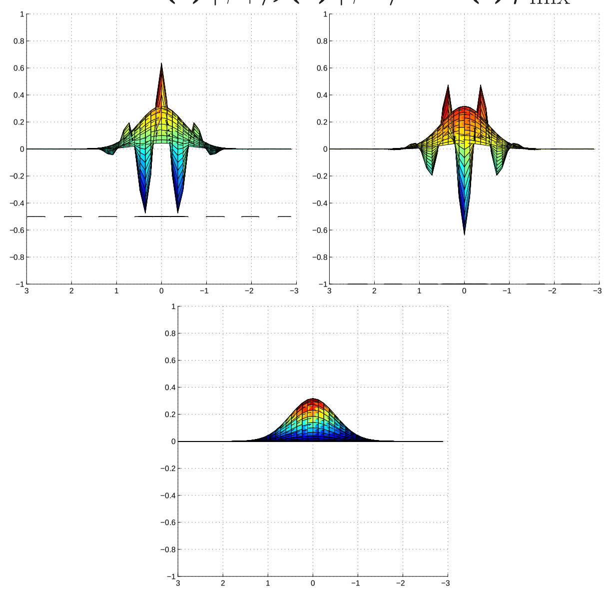
Wigner function for Fock states $|0\rangle, |1\rangle, |2\rangle$



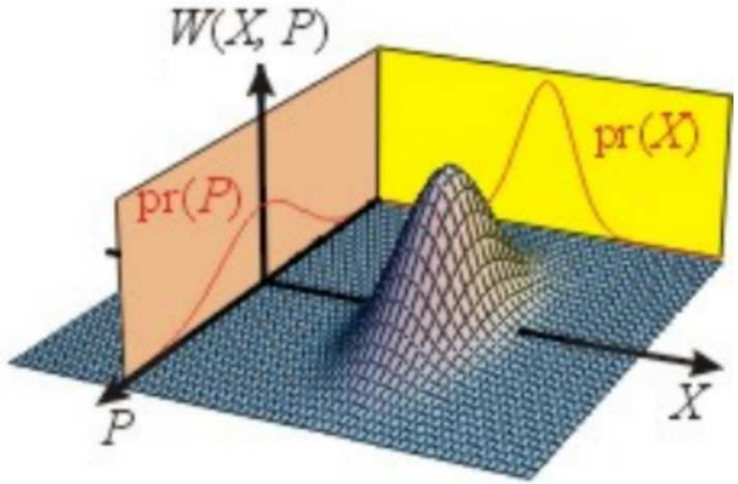
Wigner function for Schrödinger cat states (a) $|\psi_+\rangle$, (b) $|\psi_-\rangle$ and (c) mixture of coherent states $\hat{\rho}_{\rm mix} = |\alpha_0\rangle\langle\alpha_0| + |-\alpha_0\rangle\langle-\alpha_0|$



Wigner function for (a) $|\psi_+\rangle$, (b) $|\psi_-\rangle$ and (c) $\hat{\rho}_{\rm mix}$



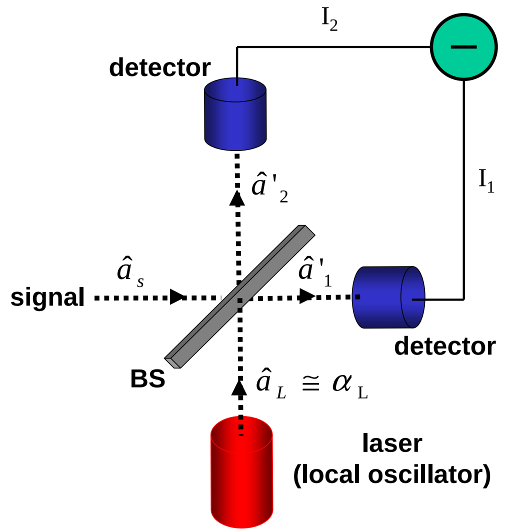
marginal distributions of Wigner function



$$\mathrm{pr}(x) \equiv \langle x|\hat{\rho}|x\rangle = \int_{-\infty}^{\infty} W(x,p)dp, \quad \mathrm{pr}(p) \equiv \langle p|\hat{\rho}|p\rangle = \int_{-\infty}^{\infty} W(x,p)dx$$

221

balanced homodyne detection



222

♣ What is measured in homodyne detection?

- **intensity** I_k ($k = 1, 2$) is proportional to the number of photons $\hat{n}_k$:

$$I_1 \sim \hat{n}_1 = \hat{a}_1'^{\dagger}\hat{a}_1'$$
$$I_2 \sim \hat{n}_2 = \hat{a}_2'^{\dagger}\hat{a}_2'$$

- **parametric approximation** for laser field:

$$\langle \hat{n}_L \rangle \gg 1 \quad \Rightarrow \quad \hat{a}_L \approx \alpha_L$$

- **beam splitter (BS)** is 50:50 ($T = R = 1/2$),

thus it is called 'balanced' detection.

- relations between input, $\hat{a}_k$, and output, $\hat{a}'_k$, annihilation operators:

$$\hat{a}'_1 = \frac{1}{\sqrt{2}}(\hat{a}_S - \hat{a}_L) \approx \frac{1}{\sqrt{2}}(\hat{a}_S - \alpha_L)$$
$$\hat{a}'_2 = \frac{1}{\sqrt{2}}(\hat{a}_S + \hat{a}_L) \approx \frac{1}{\sqrt{2}}(\hat{a}_S + \alpha_L)$$

223

- we measure **difference of intensities**, which is proportional to:

$$\begin{aligned}\hat{n}_2 - \hat{n}_1 &= \frac{1}{2}(\hat{a}_S^\dagger + \alpha_L^*)(\hat{a}_S + \alpha_L) - \frac{1}{2}(\hat{a}_S^\dagger - \alpha_L^*)(\hat{a}_S - \alpha_L)\\ &= \alpha_L^*\hat{a}_S + \alpha_L\hat{a}_S^\dagger\\ &= |\alpha_L|(e^{-i\theta}\hat{a}_S + e^{i\theta}\hat{a}_S^\dagger) = 2|\alpha_L|\hat{X}(\theta)\end{aligned}$$

where $\theta = \arg(\alpha_L)$ and

$$\hat{X}(\theta) = \frac{1}{2}(\hat{a}_S e^{-i\theta} + \hat{a}_S^\dagger e^{i\theta})$$

is the **generalized quadrature operator**

- special cases:

$\hat{X}(0) = \hat{q}$ – **position operator**

$\hat{X}(\frac{\pi}{2}) = \hat{p}$ – **momentum operator**

224

marginal distribution of Wigner function at angle θ

$$\mathrm{pr}(X,\theta) = \int_{-\infty}^{\infty} W(q\cos\theta - p\sin\theta, q\sin\theta + p\cos\theta)dp$$

describes probability of measurement result of the quadrature

$$\hat{X}(\theta) = \hat{q}\cos\theta - \hat{p}\sin\theta$$

Remarks:

- this is so-called **Radon transformation**
- $\mathrm{pr}(X,\theta)$ is directly measured in homodyne detection

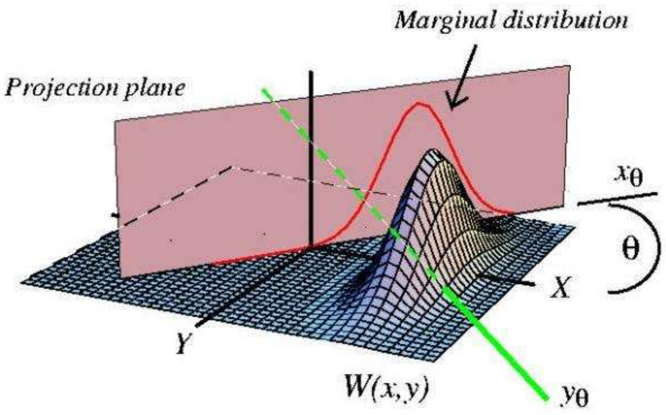
Can we reconstruct Wigner function from its marginal distributions?

$$W(q,p) = \frac{1}{(2\pi)^2}\int_{-\infty}^{\infty}\int_0^{\pi}\int_{-\infty}^{\infty} \mathrm{pr}(X,\theta)\exp[i\xi(q\cos\theta + p\sin\theta - X)]|\xi|dX\,d\theta\,d\xi$$

this is the **inverse Radon transformation**

[K. Vogel and H. Risken, 1989]

marginal distribution of Wigner function at angle θ



$$\mathrm{pr}(X,\theta) = \int_{-\infty}^{\infty} W(q\cos\theta - p\sin\theta, q\sin\theta + p\cos\theta)dp$$

Note: $x \equiv q, \quad y \equiv p, \quad \mathrm{pr}(X,0) = \langle q|\hat\rho|q\rangle, \quad \mathrm{pr}(X,\frac{\pi}{2}) = \langle p|\hat\rho|p\rangle$

one repeats measurements on many copies
i.e. identically prepared quantum objects

number of measurements

e.g., in the first experiment, Smithey et al. performed 4000 measurements at 27 angles θ, so in total **108 000 measurements**; in the second experiment they performed **160 000 measurements**.

history

1. theoretical proposal – K. Vogel and H. Risken (1989)
2. first experimental reconstruction of nonclassical state [i.e., squeezed vacuum] – D. Smithey, M. Raymer et al. (1993)
3. first experimental reconstruction of single-photon state and its superposition with vacuum (qubit state) – A. Lvovsky and J. Mlynek (2002)

Summary

1. We cannot measure simultaneously q and p, thus we cannot measure directly Wigner function.

2. But we can measure its marginal distributions $\mathrm{pr}(X,\theta)$ at various angles θ

3. By applying the inverse Radon transformation, we can reconstruct Wigner function and thus the density matrix.

hidden object $\longleftrightarrow$ Wigner function
quantum "shadows" $\longleftrightarrow$ marginal distributions of Wigner function

4. How to reconstruct finite-dimensional states?

   In principle, the same method can be applied,
   but there more effective methods, which will be described in the following.

Optical-qubit tomography (part II)

single-qubit tomography by measuring Stokes parameters

- **notation:**

$|H\rangle$ – horizontal polarization

$|V\rangle$ – vertical polarization

$|\overline{D}\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$ – linear-diagonal polarization at 45^0

$|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ – linear-diagonal polarization at 135^0

$|R\rangle = \frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle)$ – right-circular polarization

$|L\rangle = \frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle)$ – left-circular polarization

thus we readily have the inverse relations:

$$|H\rangle = \tfrac{|R\rangle+|L\rangle}{\sqrt{2}} = \tfrac{|D\rangle+|\overline{D}\rangle}{\sqrt{2}}, \qquad |V\rangle = i\tfrac{|R\rangle-|L\rangle}{\sqrt{2}} = \tfrac{|D\rangle-|\overline{D}\rangle}{\sqrt{2}}$$

$$|R\rangle = \tfrac{1+i}{2}(|\overline{D}\rangle - i|D\rangle) = e^{i\pi/4}\tfrac{|\overline{D}\rangle-i|D\rangle}{\sqrt{2}}, \qquad |L\rangle = e^{i\pi/4}\tfrac{|D\rangle-i|\overline{D}\rangle}{\sqrt{2}}$$

$$|D\rangle = e^{i\pi/4}\tfrac{|R\rangle-i|L\rangle}{\sqrt{2}}, \qquad |\overline{D}\rangle = e^{i\pi/4}\tfrac{|L\rangle-i|R\rangle}{\sqrt{2}}$$

moreover

$$|H\rangle\langle H| = \tfrac{|R\rangle+|L\rangle}{\sqrt{2}}\tfrac{\langle R|+\langle L|}{\sqrt{2}} = \tfrac{1}{2}\Big(|R\rangle\langle R| + |R\rangle\langle L| + |L\rangle\langle R| + |L\rangle\langle L|\Big)$$

$$|V\rangle\langle V| = \tfrac{|R\rangle-|L\rangle}{\sqrt{2}}\tfrac{\langle R|-\langle L|}{\sqrt{2}} = \tfrac{1}{2}\Big(|R\rangle\langle R| - |R\rangle\langle L| - |L\rangle\langle R| + |L\rangle\langle L|\Big)$$

$$|D\rangle\langle D| = \tfrac{|R\rangle-i|L\rangle}{\sqrt{2}}\tfrac{\langle R|+i\langle L|}{\sqrt{2}} = \tfrac{1}{2}\Big(|R\rangle\langle R| + i|R\rangle\langle L| - i|L\rangle\langle R| + |L\rangle\langle L|\Big)$$

$$|\overline{D}\rangle\langle\overline{D}| = \tfrac{|L\rangle-i|r\rangle}{\sqrt{2}}\tfrac{\langle L|+i\langle R|}{\sqrt{2}} = \tfrac{1}{2}\Big(|L\rangle\langle L| - i|R\rangle\langle L| + i|L\rangle\langle R| + |R\rangle\langle R|\Big)$$

Pauli operators

$$\hat{\sigma}_0 = |R\rangle\langle R| + |L\rangle\langle L|$$
$$\hat{\sigma}_1 = |R\rangle\langle L| + |L\rangle\langle R|$$
$$\hat{\sigma}_2 = i(|L\rangle\langle R| - |R\rangle\langle L|)$$
$$\hat{\sigma}_3 = |R\rangle\langle R| - |L\rangle\langle L|$$

four measurements of intensity, e.g.:

(1) with a filter that transmits 50% of the incident radiation, regardless of its polarization:

$$n_0 = \frac{\mathcal{N}}{2}\left(\langle H|\hat{\rho}|H\rangle + \langle V|\hat{\rho}|V\rangle\right) = \frac{\mathcal{N}}{2}\left(\langle R|\hat{\rho}|R\rangle + \langle L|\hat{\rho}|L\rangle\right)$$

(2) with a polarizer that transmits only photons in state $|H\rangle$:

$$n_1 = \mathcal{N}\langle H|\hat{\rho}|H\rangle$$

(3) with a polarizer that transmits only photons in state $|\overline{D}\rangle$:

$$n_2 = \mathcal{N}\langle\overline{D}|\hat{\rho}|\overline{D}\rangle$$

(4) with a polarizer that transmits only photons in state $|R\rangle$:

$$n_3 = \mathcal{N}\langle R|\hat{\rho}|R\rangle$$

Stokes parameters via photon counts

$$\begin{aligned}
\mathcal{S}_0 &\equiv 2n_0\\
\mathcal{S}_1 &\equiv 2\,(n_1 - n_0)\\
\mathcal{S}_2 &\equiv 2\,(n_2 - n_0)\\
\mathcal{S}_3 &\equiv 2\,(n_3 - n_0)
\end{aligned}$$

Single-qubit density matrix via Stokes parameters

$$\hat{\rho} = \frac{1}{2}\sum_{i=0}^{3}\frac{\mathcal{S}_i}{\mathcal{S}_0}\hat{\sigma}_i,$$

where

$$\mathcal{S}_i = \mathcal{N}\langle\hat{\sigma}_i\rangle = \mathcal{N}\mathrm{Tr}\{\hat{\sigma}_i\hat{\rho}\}$$

$$\hat{\rho} = \frac{1}{2}\begin{bmatrix} 1+\langle\hat{\sigma}_3\rangle & \langle\hat{\sigma}_1\rangle - i\langle\hat{\sigma}_2\rangle \\ \langle\hat{\sigma}_1\rangle + i\langle\hat{\sigma}_2\rangle & 1-\langle\hat{\sigma}_3\rangle \end{bmatrix}$$

Why do we need $\mathcal{S}_0$?

for renormalization of the count statistics

to compensate experimental inefficiencies (e.g. of detectors)

single polarization-qubit measurement operators

there are infinitely many sets of such projectors

the common ones are e.g.

$$\begin{aligned}
\hat{\mu}'_0 &= |H\rangle\langle H| + |V\rangle\langle V|\\
&= |L\rangle\langle L| + |R\rangle\langle R|\\
\hat{\mu}'_1 &= |H\rangle\langle H|\\
&\sim |R\rangle\langle R| + |R\rangle\langle L| + |L\rangle\langle R| + |L\rangle\langle L|\\
\hat{\mu}'_2 &= |\overline{D}\rangle\langle\overline{D}|\\
&\sim |L\rangle\langle L| - i|R\rangle\langle L| + i|L\rangle\langle R| + |R\rangle\langle R|\\
&= |H\rangle\langle H| - |H\rangle\langle V| - |V\rangle\langle H| + |V\rangle\langle V|\\
\hat{\mu}'_3 &= |R\rangle\langle R|\\
&\sim |H\rangle\langle H| - i|H\rangle\langle V| + i|V\rangle\langle H| + |V\rangle\langle V|
\end{aligned}$$

or $\quad \hat{\mu}''_0 = \hat{\mu}'_0, \qquad \hat{\mu}''_1 = \hat{\mu}'_1, \qquad \hat{\mu}''_2 = |D\rangle\langle D|, \qquad \hat{\mu}''_3 = \hat{\mu}'_3$

or

$$\begin{aligned}\hat{\mu}_0 &= \mathcal{N}\hat{\sigma}_0 = \hat{\mu}'_0\\ \hat{\mu}_1 &= \mathcal{N}\hat{\sigma}_1 = \hat{\mu}'_1 - \hat{\mu}'_0\\ \hat{\mu}_2 &= \mathcal{N}\hat{\sigma}_2 = \hat{\mu}'_2 - \hat{\mu}'_0\\ \hat{\mu}_3 &= \mathcal{N}\hat{\sigma}_3 = \hat{\mu}'_3 - \hat{\mu}'_0\end{aligned}$$

assuming loss-free detection (perfect detectors and wave plates)

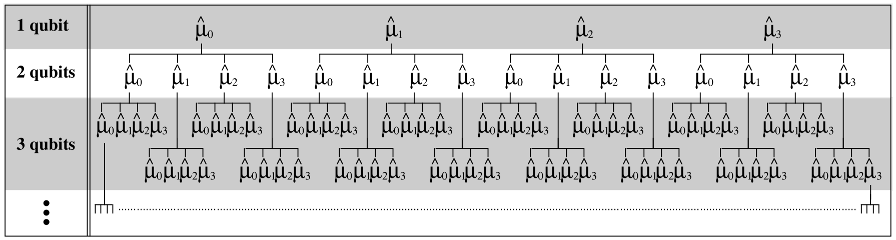
$$\mathcal{N} = 1 \Rightarrow \hat{\mu}_k = \hat{\sigma}_k \quad (k = 0, ..., 3)$$

two-qubit measurement operators

standard 16 projectors:

$$\begin{aligned}\hat{\mu}_{00} &= \mathcal{N}\hat{\sigma}_0 \otimes \hat{\sigma}_0,\\ \hat{\mu}_{01} &= \mathcal{N}\hat{\sigma}_0 \otimes \hat{\sigma}_1,\\ &\cdots\\ \hat{\mu}_{33} &= \mathcal{N}\hat{\sigma}_3 \otimes \hat{\sigma}_3\end{aligned}$$

measurement operators required for tomography



1 qubit – 4 measurement operators: $\hat{\mu}_i$

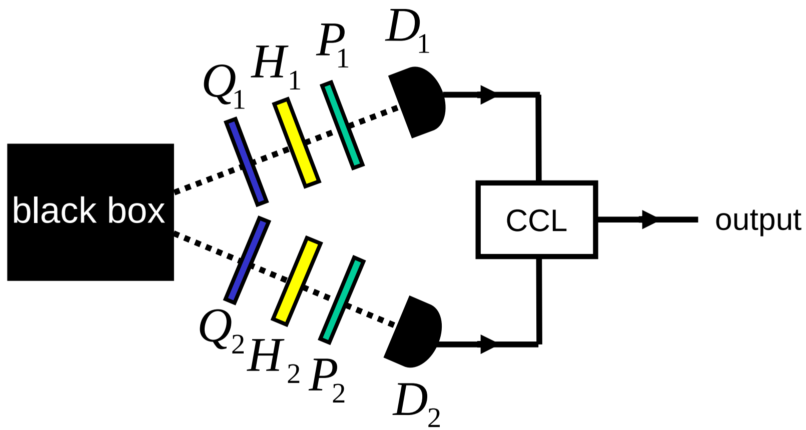
2 qubits – 16 measurement operators: $\hat{\mu}_i \otimes \hat{\mu}_j$

3 qubits – 64 measurement operators: $\hat{\mu}_i \otimes \hat{\mu}_j \otimes \hat{\mu}_k$

...

n qubits – 4^n measurement operators: $\hat{\mu}_{i_1} \otimes \hat{\mu}_{i_2} \otimes \cdots \otimes \hat{\mu}_{i_n}$

tomography of a polarization state of two photons



black box – a source of photon pairs in an unknown state

Q_1, Q_2 – QWPs, H_1, H_2 – HWPs

P_1, P_2 – polarizers transmits only photons of one polarization (say, vertical)

CCL – coincidence counter and logic

wave plates - a reminder

half-wave plate (HWP)

$$\hat{S}_{\lambda/2}(\beta) = \begin{bmatrix}\cos(2\beta) & \sin(2\beta)\\ \sin(2\beta) & -\cos(2\beta)\end{bmatrix}$$

special cases of HWPs

$$\begin{aligned}\hat{S}_{\lambda/2}(0) &= \hat{\sigma}_Z\\ \hat{S}_{\lambda/2}(22.5^0) &= \hat{H}\\ \hat{S}_{\lambda/2}(45^0) &= \hat{\sigma}_X\end{aligned}$$

quarter-wave plate (QWP)

$$\hat{S}_{\lambda/4}(\beta) \sim \frac{1}{\sqrt{2}}\begin{bmatrix}\cos(2\beta) - i & \sin(2\beta)\\ \sin(2\beta) & -\cos(2\beta) - i\end{bmatrix}$$

slightly modified defs.

$$\hat{S}'_{\lambda/2}(\beta) = \hat{S}_{\lambda/2}(-\beta), \quad \hat{S}'_{\lambda/4}(\beta) = -\hat{S}_{\lambda/4}(-\beta)$$

tomography of polarization state of two photons

No.	Mode 1	Mode 2	HWP 1	QWP 1	HWP 2	QWP 2
1	$\|\mathrm{H}\rangle$	$\|\mathrm{H}\rangle$	45^o	0	45^o	0
2	$\|\mathrm{H}\rangle$	$\|\mathrm{V}\rangle$	45^o	0	0	0
3	$\|\mathrm{V}\rangle$	$\|\mathrm{V}\rangle$	0	0	0	0
4	$\|\mathrm{V}\rangle$	$\|\mathrm{H}\rangle$	0	0	45^o	0
5	$\|\mathrm{R}\rangle$	$\|\mathrm{H}\rangle$	22.5^o	0	45^o	0
6	$\|\mathrm{R}\rangle$	$\|\mathrm{V}\rangle$	22.5^o	0	0	0
7	$\|\overline{\mathrm{D}}\rangle$	$\|\mathrm{V}\rangle$	22.5^o	45^o	0	0
8	$\|\overline{\mathrm{D}}\rangle$	$\|\mathrm{H}\rangle$	22.5^o	45^o	45^o	0
9	$\|\overline{\mathrm{D}}\rangle$	$\|\mathrm{R}\rangle$	22.5^o	45^o	22.5^o	0
10	$\|\overline{\mathrm{D}}\rangle$	$\|\overline{\mathrm{D}}\rangle$	22.5^o	45^o	22.5^o	45^o
11	$\|\mathrm{R}\rangle$	$\|\overline{\mathrm{D}}\rangle$	22.5^o	0	22.5^o	45^o
12	$\|\mathrm{H}\rangle$	$\|\overline{\mathrm{D}}\rangle$	45^o	0	22.5^o	45^o
13	$\|\mathrm{V}\rangle$	$\|\overline{\mathrm{D}}\rangle$	0	0	22.5^o	45^o
14	$\|\mathrm{V}\rangle$	$\|\mathrm{L}\rangle$	0	0	22.5^o	90^o
15	$\|\mathrm{H}\rangle$	$\|\mathrm{L}\rangle$	45^o	0	22.5^o	90^o
16	$\|\mathrm{R}\rangle$	$\|\mathrm{L}\rangle$	22.5^o	0	22.5^o	90^o

$$|\overline{\mathrm{D}}\rangle = \frac{|\mathrm{H}\rangle - |\mathrm{V}\rangle}{\sqrt{2}}, \quad |\mathrm{L}\rangle \equiv \frac{|\mathrm{H}\rangle + i|\mathrm{V}\rangle}{\sqrt{2}}, \quad |\mathrm{R}\rangle \equiv \frac{|\mathrm{H}\rangle - i|\mathrm{V}\rangle}{\sqrt{2}}.$$

Mathematica program for the tomography scheme

- def. of Kronecker tensor product (Kron) and Hermitian conjugate (hc)

```
<< LinearAlgebra'MatrixManipulation'
f[x_, y_] := x*y;
Kron[matrix1_, matrix2_]:= BlockMatrix[Outer[f, matrix1, matrix2]]
hc[x_] := Transpose[Conjugate[x]]
```

- def. of rotation by HWP and QWP and def. of $[\rho_{nm}]_{4\times4}$

$$\mathbf{HWP[t\_] :=} \begin{pmatrix} \mathrm{Cos[2\,t]} & \mathrm{Sin[2\,t]} \\ \mathrm{Sin[2\,t]} & -\mathrm{Cos[2\,t]} \end{pmatrix}$$

$$\mathbf{QWP[t\_] :=} \frac{1}{\sqrt{2}} \begin{pmatrix} i - \mathrm{Cos[2\,t]} & -\mathrm{Sin[2\,t]} \\ -\mathrm{Sin[2\,t]} & i + \mathrm{Cos[2\,t]} \end{pmatrix}$$

$$\mathbf{rho} = \begin{pmatrix} \rho_{0,0} & \rho_{0,1} & \rho_{0,2} & \rho_{0,3} \\ \rho_{1,0} & \rho_{1,1} & \rho_{1,2} & \rho_{1,3} \\ \rho_{2,0} & \rho_{2,1} & \rho_{2,2} & \rho_{2,3} \\ \rho_{3,0} & \rho_{3,1} & \rho_{3,2} & \rho_{3,3} \end{pmatrix};$$

- rotation matrix 4×4 of 2 beams by 2 HWPs and 2 QWPs

```
rotation[h1_, q1_, h2_, q2_] :=
  Kron[HWP[h1 Degree].QWP[q1 Degree], HWP[h2 Degree].QWP[q2 Degree]]
```

- our sequence of rotations

```
R[1]  := rotation[45, 0, 45, 0];
R[2]  := rotation[45, 0, 0, 0];
R[3]  := rotation[0, 0, 0, 0];
R[4]  := rotation[0, 0, 45, 0];
R[5]  := rotation[45/2, 0, 45, 0];
R[6]  := rotation[45/2, 0, 0, 0];
R[7]  := rotation[45/2, 45, 0, 0];
R[8]  := rotation[45/2, 45, 45, 0];
R[9]  := rotation[45/2, 45, 45/2, 0];
R[10] := rotation[45/2, 45, 45/2, 45];
R[11] := rotation[45/2, 0, 45/2, 45];
R[12] := rotation[45, 0, 45/2, 45];
R[13] := rotation[0, 0, 45/2, 45];
R[14] := rotation[0, 0, 45/2, 90];
R[15] := rotation[45, 0, 45/2, 90];
R[16] := rotation[45/2, 0, 45/2, 90]
```


- rotated $\hat{\rho}^{(n)} = \hat{R}^{(n)}\hat{\rho}(\hat{R}^{(n)})^{\dagger}$ for the nth measurement

```
RhoRotated[n_] := R[n].rho .hc[R[n]]
```

- examples

RhoRotated[1] // MF

$$\begin{pmatrix} \rho_{3,3} & -i\,\rho_{3,2} & -i\,\rho_{3,1} & -\rho_{3,0} \\ i\,\rho_{2,3} & \rho_{2,2} & \rho_{2,1} & -i\,\rho_{2,0} \\ i\,\rho_{1,3} & \rho_{1,2} & \rho_{1,1} & -i\,\rho_{1,0} \\ -\rho_{0,3} & i\,\rho_{0,2} & i\,\rho_{0,1} & \rho_{0,0} \end{pmatrix}$$

RhoRotated[2] // MF

$$\begin{pmatrix} \rho_{2,2} & -i\,\rho_{2,3} & -i\,\rho_{2,0} & -\rho_{2,1} \\ i\,\rho_{3,2} & \rho_{3,3} & \rho_{3,0} & -i\,\rho_{3,1} \\ i\,\rho_{0,2} & \rho_{0,3} & \rho_{0,0} & -i\,\rho_{0,1} \\ -\rho_{1,2} & i\,\rho_{1,3} & i\,\rho_{1,0} & \rho_{1,1} \end{pmatrix}$$

```
RhoRotated[5] // FS // MF
```

$$\begin{pmatrix} \frac{1}{2}(\rho_{1,1}+i(\rho_{1,3}-\rho_{3,1})+\rho_{3,3}) & -\frac{1}{2}i(\rho_{1,0}+i(\rho_{1,2}-\rho_{3,0})+\rho_{3,2}) & \frac{1}{2}(\rho_{1,1}-i(\rho_{1,3}+\rho_{3,1})-\rho_{3,3}) & -\frac{1}{2}i(\rho_{1,0}-i(\rho_{1,2}+\rho_{3,0})-\rho_{3,2}) \\ \frac{1}{2}i(\rho_{0,1}+i(\rho_{0,3}-\rho_{2,1})+\rho_{2,3}) & \frac{1}{2}(\rho_{0,0}+i(\rho_{0,2}-\rho_{2,0})+\rho_{2,2}) & \frac{1}{2}(i\rho_{0,1}+\rho_{0,3}+\rho_{2,1}-i\rho_{2,3}) & \frac{1}{2}(\rho_{0,0}-i(\rho_{0,2}+\rho_{2,0})-\rho_{2,2}) \\ \frac{1}{2}(\rho_{1,1}+i(\rho_{1,3}+\rho_{3,1}+i\rho_{3,3})) & \frac{1}{2}(-i\rho_{1,0}+\rho_{1,2}+\rho_{3,0}+i\rho_{3,2}) & \frac{1}{2}(\rho_{1,1}-i\rho_{1,3}+i\rho_{3,1}+\rho_{3,3}) & -\frac{1}{2}i(\rho_{1,0}-i\rho_{1,2}+i\rho_{3,0}+\rho_{3,2}) \\ \frac{1}{2}i(\rho_{0,1}+i(\rho_{0,3}+\rho_{2,1}+i\rho_{2,3})) & \frac{1}{2}(\rho_{0,0}+i(\rho_{0,2}+\rho_{2,0}+i\rho_{2,2})) & \frac{1}{2}i(\rho_{0,1}-i\rho_{0,3}+i\rho_{2,1}+\rho_{2,3}) & \frac{1}{2}(\rho_{0,0}-i\rho_{0,2}+i\rho_{2,0}+\rho_{2,2}) \end{pmatrix}$$

measured probabilities $P_n = \langle VV|\hat{\rho}^{(n)}|VV\rangle = \rho_{33}^{(n)}$ where $|V\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

so

```
ketV := (0
         1);
ketVV := Kron[ketV, ketV];
braVV := hc[ketVV]
P[n_] := braVV.RhoRotated[n].ketVV // FS
P[1]
```

$\{\{\rho_{0,0}\}\}$

```
P[2]
```

$\{\{\rho_{1,1}\}\}$

```
P[5]
```

$\{\{\frac{1}{2}(\rho_{0,0}-i\rho_{0,2}+i\rho_{2,0}+\rho_{2,2})\}\}$


```
all1 = Do[Print["P[", n, "]=", P[n]], {n, 1, 16}]
```

P[1] = $\{\{\rho_{0,0}\}\}$

P[2] = $\{\{\rho_{1,1}\}\}$

P[3] = $\{\{\rho_{3,3}\}\}$

P[4] = $\{\{\rho_{2,2}\}\}$

P[5] = $\{\{\frac{1}{2}(\rho_{0,0}-i\rho_{0,2}+i\rho_{2,0}+\rho_{2,2})\}\}$

P[6] = $\{\{\frac{1}{2}(\rho_{1,1}-i\rho_{1,3}+i\rho_{3,1}+\rho_{3,3})\}\}$

P[7] = $\{\{\frac{1}{2}(\rho_{1,1}-\rho_{1,3}-\rho_{3,1}+\rho_{3,3})\}\}$

P[8] = $\{\{\frac{1}{2}(\rho_{0,0}-\rho_{0,2}-\rho_{2,0}+\rho_{2,2})\}\}$

P[9] = $\{\{\frac{1}{4}(\rho_{0,0}-i\rho_{0,1}-\rho_{0,2}+i\rho_{0,3}+i\rho_{1,0}+\rho_{1,1}-i\rho_{1,2}-\rho_{1,3}-\rho_{2,0}+i\rho_{2,1}+\rho_{2,2}-i(\rho_{2,3}+\rho_{3,0}-i\rho_{3,1}-\rho_{3,2})+\rho_{3,3})\}\}$

P[10] = $\{\{\frac{1}{4}(\rho_{0,0}-\rho_{0,1}-\rho_{0,2}+\rho_{0,3}-\rho_{1,0}+\rho_{1,1}+\rho_{1,2}-\rho_{1,3}-\rho_{2,0}+\rho_{2,1}+\rho_{2,2}-\rho_{2,3}+\rho_{3,0}-\rho_{3,1}-\rho_{3,2}+\rho_{3,3})\}\}$

P[11] = $\{\{\frac{1}{4}(\rho_{0,0}-\rho_{0,1}-i(\rho_{0,2}-\rho_{0,3}-i\rho_{1,0}+i\rho_{1,1}-\rho_{1,2}+\rho_{1,3}-\rho_{2,0}+\rho_{2,1}+i(\rho_{2,2}-\rho_{2,3}-i\rho_{3,0}+i\rho_{3,1}-\rho_{3,2}+\rho_{3,3})))\}\}$

P[12] = $\{\{\frac{1}{2}(\rho_{0,0}-\rho_{0,1}-\rho_{1,0}+\rho_{1,1})\}\}$

P[13] = $\{\{\frac{1}{2}(\rho_{2,2}-\rho_{2,3}-\rho_{3,2}+\rho_{3,3})\}\}$

P[14] = $\{\{\frac{1}{2}(\rho_{2,2}+i(\rho_{2,3}-\rho_{3,2})+\rho_{3,3})\}\}$

P[15] = $\{\{\frac{1}{2}(\rho_{0,0}+i(\rho_{0,1}-\rho_{1,0})+\rho_{1,1})\}\}$

P[16] = $\{\{\frac{1}{4}(\rho_{0,0}+i\rho_{0,1}-i\rho_{0,2}+\rho_{0,3}-i\rho_{1,0}+\rho_{1,1}-\rho_{1,2}-i\rho_{1,3}+i\rho_{2,0}-\rho_{2,1}+\rho_{2,2}+i\rho_{2,3}+\rho_{3,0}+i(\rho_{3,1}-\rho_{3,2})+\rho_{3,3})\}\}$

equivalent approach using tomographic states

```
ketH := (1
         0); ketV := (0
                      1);
ketD := (ketH + ketV)/√2; ketDbar := (ketH − ketV)/√2;
ketL := (ketH + i ketV)/√2; ketR := (ketH − i ketV)/√2;
braH = hc[ketH]; braV = hc[ketV];
braD = hc[ketD]; braDbar = hc[ketDbar];
braR = hc[ketR]; braL = hc[ketL];
```

where $|H\rangle$=ketH, $\langle H|$=braH, etc.

our choice of tomographic states

= (projection) measurement states = projectors

$|\psi_1\rangle = |\mathrm{HH}\rangle, \quad |\psi_2\rangle = |\mathrm{HV}\rangle, \quad \ldots, \quad |\psi_{16}\rangle = |\mathrm{RL}\rangle$

```
psi[1]  := Kron[ketH, ketH];
psi[2]  := Kron[ketH, ketV];
psi[3]  := Kron[ketV, ketV];
psi[4]  := Kron[ketV, ketH];
psi[5]  := Kron[ketR, ketH];
psi[6]  := Kron[ketR, ketV];
psi[7]  := Kron[ketDbar, ketV];
psi[8]  := Kron[ketDbar, ketH];
psi[9]  := Kron[ketDbar, ketR];
psi[10] := Kron[ketDbar, ketDbar];
psi[11] := Kron[ketR, ketDbar];
psi[12] := Kron[ketH, ketDbar];
psi[13] := Kron[ketV, ketDbar];
psi[14] := Kron[ketV, ketL];
psi[15] := Kron[ketH, ketL];
psi[16] := Kron[ketR, ketL];
```

projection measurements

enable determination of the probabilities

$$p_1 = \langle HH|\hat{\rho}|HH\rangle, p_2 = \langle HV|\hat{\rho}|HV\rangle \text{ , etc.:}$$

```
p[1]  := Kron[braH, braH]      .rho.Kron[ketH, ketH];
p[2]  := Kron[braH, braV]      .rho.Kron[ketH, ketV];
p[3]  := Kron[braV, braV]      .rho.Kron[ketV, ketV];
p[4]  := Kron[braV, braH]      .rho.Kron[ketV, ketH];
p[5]  := Kron[braR, braH]      .rho.Kron[ketR, ketH];
p[6]  := Kron[braR, braV]      .rho.Kron[ketR, ketV];
p[7]  := Kron[braDbar, braV]   .rho.Kron[ketDbar, ketV];
p[8]  := Kron[braDbar, braH]   .rho.Kron[ketDbar, ketH];
p[9]  := Kron[braDbar, braR]   .rho.Kron[ketDbar, ketR];
p[10] := Kron[braDbar, braDbar].rho.Kron[ketDbar, ketDbar];
p[11] := Kron[braR, braDbar]   .rho.Kron[ketR, ketDbar];
p[12] := Kron[braH, braDbar]   .rho.Kron[ketH, ketDbar];
p[13] := Kron[braV, braDbar]   .rho.Kron[ketV, ketDbar];
p[14] := Kron[braV, braL]      .rho.Kron[ketV, ketL];
p[15] := Kron[braH, braL]      .rho.Kron[ketH, ketL];
p[16] := Kron[braR, braL]      .rho.Kron[ketR, ketL];

all2 := Do[Print[n, " -> ", p[n] // FS], {n, 1, 16}]
```


projection measurements

enable determination of the probabilities

$$p_1 = \langle\psi_1|\hat{\rho}|\psi_1\rangle = \langle HH|\hat{\rho}|HH\rangle, p_2 = \langle\psi_2|\hat{\rho}|\psi_2\rangle = \langle HV|\hat{\rho}|HV\rangle, \text{ etc.:}$$

```
p[1]  := hc[psi[1]] .rho.psi[1] ;
p[2]  := hc[psi[2]] .rho.psi[2] ;
p[3]  := hc[psi[3]] .rho.psi[3] ;
p[4]  := hc[psi[4]] .rho.psi[4] ;
p[5]  := hc[psi[5]] .rho.psi[5] ;
p[6]  := hc[psi[6]] .rho.psi[6] ;
p[7]  := hc[psi[7]] .rho.psi[7] ;
p[8]  := hc[psi[8]] .rho.psi[8] ;
p[9]  := hc[psi[9]] .rho.psi[9] ;
p[10] := hc[psi[10]].rho.psi[10];
p[11] := hc[psi[11]].rho.psi[11];
p[12] := hc[psi[12]].rho.psi[12];
p[13] := hc[psi[13]].rho.psi[13];
p[14] := hc[psi[14]].rho.psi[14];
p[15] := hc[psi[15]].rho.psi[15];
p[16] := hc[psi[16]].rho.psi[16];

all2 := Do[Print[n, " -> ", p[n] // FS], {n, 1, 16}]
```


both methods give the same probabilities

$$P(n) = p(n)$$

```
test = Do[Print["P[", n, "]-p[", n, "]=", P[n] - p[n] // FS], {n, 1, 16}]
P[1]-p[1]={{0}}
P[2]-p[2]={{0}}
P[3]-p[3]={{0}}
P[4]-p[4]={{0}}
P[5]-p[5]={{0}}
P[6]-p[6]={{0}}
P[7]-p[7]={{0}}
P[8]-p[8]={{0}}
P[9]-p[9]={{0}}
P[10]-p[10]={{0}}
P[11]-p[11]={{0}}
P[12]-p[12]={{0}}
P[13]-p[13]={{0}}
P[14]-p[14]={{0}}
P[15]-p[15]={{0}}
P[16]-p[16]={{0}}
```


reconstruction analysis

convert 4x4 matrix into 16-dim column vector

represent operators of Hilbert space as **superoperators in Liouville space**

possible methods:

- method 1:

$$\hat{\rho} = \begin{bmatrix} \rho_1 & \rho_2 & \rho_3 & \rho_4 \\ \rho_5 & \rho_6 & \rho_7 & \rho_8 \\ \rho_9 & \rho_{10} & \rho_{11} & \rho_{12} \\ \rho_{13} & \rho_{14} & \rho_{15} & \rho_{16} \end{bmatrix} \mapsto \begin{bmatrix} \rho_1 \\ \rho_2 \\ \vdots \\ \rho_{16} \end{bmatrix} \equiv \begin{bmatrix} \rho_{00} \\ \rho_{01} \\ \vdots \\ \rho_{33} \end{bmatrix}$$

- another labelling:

$$\hat{\rho} = \begin{bmatrix} x_1 & x_2 + ix_{11} & x_3 + ix_{12} & x_4 + ix_{13} \\ x_2 - ix_{11} & x_5 & x_6 + ix_{14} & x_7 + ix_{15} \\ x_3 - ix_{12} & x_6 - ix_{14} & x_8 & x_9 + ix_{16} \\ x_4 - ix_{13} & x_7 - ix_{15} & x_9 - ix_{16} & x_{10} \end{bmatrix} \mapsto \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{16} \end{bmatrix}$$

```
In[81]:=  all1 = Do[Print["P[", n, "]=", P[n][[1, 1]]], {n, 1, 16}]
```

$$P[1]-x[1]$$
$$P[2]-x[5]$$
$$P[3]-x[10]$$
$$P[4]-x[8]$$
$$P[5]-\frac{1}{2}(x[1]+x[8])+x[12]$$
$$P[6]-\frac{1}{2}(x[5]+x[10])+x[15]$$
$$P[7]-\frac{1}{2}(x[5]-2\,x[7]+x[10])$$
$$P[8]-\frac{1}{2}(x[1]-2\,x[3]+x[8])$$
$$P[9]-\frac{1}{4}(x[1]-2\,x[3]+x[5]-2\,x[7]+x[8]+x[10]+2\,(x[11]-x[13]+x[14]+x[16]))$$
$$P[10]-\frac{1}{4}(x[1]-2\,x[2]-2\,x[3]+2\,x[4]+x[5]+2\,x[6]-2\,x[7]+x[8]-2\,x[9]+x[10])$$
$$P[11]-\frac{1}{4}(x[1]-2\,x[2]+x[5]+x[8]-2\,x[9]+x[10]+2\,(x[12]-x[13]-x[14]+x[15]))$$
$$P[12]-\frac{1}{2}(x[1]-2\,x[2]+x[5])$$
$$P[13]-\frac{1}{2}(x[8]-2\,x[9]+x[10])$$
$$P[14]-\frac{1}{2}(x[8]+x[10]-2\,x[16])$$
$$P[15]-\frac{1}{2}(x[1]+x[5]-2\,x[11])$$
$$P[16]-\frac{1}{4}(x[1]+2\,x[4]+x[5]-2\,x[6]+x[8]+x[10]-2\,x[11]+2\,x[12]+2\,x[15]-2\,x[16])$$

set of equations $\mathrm{P} = \mathrm{A}\mathbf{x}$

where $\mathbf{P} = [P_1, P_2, \cdots, P_{16}]^T$, $\mathbf{x} = [x_1, x_2, \cdots, x_{16}]^T$, $\mathbf{A} = [a_{m,n}]_{16\times 16}$

$P_1 = x_1 = 1 \cdot x_1 + 0 \cdot x_2 + \cdots + 0 \cdot x_{16} = [1, 0, \cdots, 0] \cdot \mathbf{x} = \sum_n a_{1,n} x_n$, etc.

```
a[n_, m_] := Coefficient[P[n], x[m]]
A := Table[a[n, m][[1, 1]], {n, 1, 16}, {m, 1, 16}]
A // MF
```

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & \frac{1}{2} & 0 & -1 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{2} & 0 & -1 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{4} & 0 & -\frac{1}{2} & 0 & \frac{1}{4} & 0 & -\frac{1}{2} & \frac{1}{4} & 0 & \frac{1}{4} & \frac{1}{2} & 0 & -\frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} \\
\frac{1}{4} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{4} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{4} & -\frac{1}{2} & \frac{1}{4} & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{4} & -\frac{1}{2} & 0 & 0 & \frac{1}{4} & 0 & 0 & \frac{1}{4} & -\frac{1}{2} & \frac{1}{4} & 0 & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 \\
\frac{1}{2} & -1 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & -1 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & -1 \\
\frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{4} & 0 & 0 & \frac{1}{2} & \frac{1}{4} & -\frac{1}{2} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & -\frac{1}{2} & \frac{1}{2} & 0 & 0 & \frac{1}{2} & -\frac{1}{2}
\end{pmatrix}$$

solution of the set of equations

exists if A is **non-singular** and it is simply given by

$\mathbf{x} = \mathbf{A}^{-1}\mathbf{P}$ where $\mathbf{A}^{-1}$ is equal to

```
invA := Inverse[A]
invA // MF
```

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\
\frac{1}{2} & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & 0 & 1 & 0 & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & 0 & 1 & 0 & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -1 \\
0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
-\frac{1}{2} & 0 & 0 & -\frac{1}{2} & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -1 & 0 & -1 & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & 0 \\
-\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & 1 & 0 & -1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 \\
0 & -\frac{1}{2} & -\frac{1}{2} & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0
\end{pmatrix}$$

experimental data [James et al. 2002]

experimental coincidence counts $\mathrm{N}_{\mathrm{exp}} = \{n_1, ..., n_{16}\}$

experimental estimations of probabilities $\mathbf{P}_{\mathrm{exp}} = \{P_{\mathrm{exp}1}, ..., P_{\mathrm{exp}16}\} = \{\frac{n_1}{\mathcal{N}}, ..., \frac{n_{16}}{\mathcal{N}}\}$

where $n_\nu = \mathcal{N}\langle\psi_\nu|\hat{\rho}|\psi_\nu\rangle$ so

$$\sum_{\nu=1}^{4} n_\nu = \mathcal{N}\langle HH|\hat{\rho}|HH\rangle + \mathcal{N}\langle HV|\hat{\rho}|HV\rangle + \mathcal{N}\langle VH|\hat{\rho}|VH\rangle + \mathcal{N}\langle VV|\hat{\rho}|VV\rangle = \mathcal{N}$$

```
Nexp := Transpose[{{34749, 324, 35805, 444, 16324, 17521, 13441,
    16901, 17932, 32028, 15132, 17238, 13171, 17170, 16722, 33586}}]
Norm = Sum[Nexp[[i]], {i, 1, 4}][[1]]
Pexp = 1. Nexp / Norm;
Pexp // MF
```

$$\begin{pmatrix}
0.487213 \\ 0.00454278 \\ 0.502019 \\ 0.00622529 \\ 0.228877 \\ 0.245661 \\ 0.188455 \\ 0.236968 \\ 0.251423 \\ 0.449062 \\ 0.212165 \\ 0.241693 \\ 0.18467 \\ 0.240739 \\ 0.234458 \\ 0.470907
\end{pmatrix}$$

reconstructed $\hat{\rho}$ by linear tomography

final solution for **x** assuming the analyzed experimental data:

$$\mathbf{x} = \mathbf{A}^{-1}\mathbf{P}_{\text{exp}}$$

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{16} \end{bmatrix} \mapsto \hat{\rho} \equiv \hat{\rho}_{\text{exp}} = \begin{bmatrix} x_1 & x_2 + ix_{11} & x_3 + ix_{12} & x_4 + ix_{13} \\ x_2 - ix_{11} & x_5 & x_6 + ix_{14} & x_7 + ix_{15} \\ x_3 - ix_{12} & x_6 - ix_{14} & x_8 & x_9 + ix_{16} \\ x_4 - ix_{13} & x_7 - ix_{15} & x_9 - ix_{16} & x_{10} \end{bmatrix}$$

```
x = Flatten[invA.Pexp]

{0.487213, 0.00418524, 0.00975155, 0.519209, 0.00454278, 0.0271305, 0.0648257,
 0.00622529, 0.0694526, 0.502019, 0.01142, -0.0178416, -0.0380247, 0.0145958, -0.00762037, 0.013383}

rhoexp := ( x[[1]]                x[[2]] + i x[[11]]   x[[3]] + i x[[12]]   x[[4]] + i x[[13]]
            x[[2]] - i x[[11]]    x[[5]]               x[[6]] + i x[[14]]   x[[7]] + i x[[15]]
            x[[3]] - i x[[12]]    x[[6]] - i x[[14]]   x[[8]]               x[[9]] + i x[[16]]
            x[[4]] - i x[[13]]    x[[7]] - i x[[15]]   x[[9]] - i x[[16]]   x[[10]]            )

rhoexp // MF

( 0.487213                  0.00418524 + 0.01142 i    0.00975155 - 0.0178416 i   0.519209 - 0.0380247 i
  0.00418524 - 0.01142 i    0.00454278                0.0271305 + 0.0145958 i    0.0648257 - 0.00762037 i
  0.00975155 + 0.0178416 i  0.0271305 - 0.0145958 i   0.00622529                 0.0694526 + 0.013383 i
  0.519209 + 0.0380247 i    0.0648257 + 0.00762037 i  0.0694526 - 0.013383 i     0.502019                 )
```


- method 2: $\hat{\rho} \mapsto [r_\nu]_{16\times 1}$

find a set of 16 linearly independent 4×4 matrices $\{\hat{\gamma}_\nu\}$ satisfying:

$$\begin{aligned} \mathrm{Tr}\left\{\hat{\gamma}_\nu \cdot \hat{\gamma}_\mu\right\} &= \delta_{\nu,\mu} \\ \forall\hat{\rho} \quad \hat{\rho} &= \sum_{\nu=1}^{16} \hat{\gamma}_\nu \mathrm{Tr}\left\{\hat{\gamma}_\nu \cdot \hat{\rho}\right\} \equiv \sum_{\nu=1}^{16} \hat{\gamma}_\nu r_\nu, \end{aligned}$$

are **generalized Pauli operators** or their products chosen as, e.g., **generators of the Lie algebra $SU(4)$ or just $SU(2)\otimes SU(2)$**.

$$\hat{\gamma}_{4m+n} = \frac{1}{2}\hat{\sigma}_m \otimes \hat{\sigma}_n, \quad (m,n = 0,...,3)$$

where $\hat{\sigma}_n$ are the standard Pauli operators.

for convention we denote $\hat{\gamma}_{16} = \hat{\gamma}_0$

exemplary generators of the Lie algebra $SU(2)\otimes SU(2)$

```
σ0 = (1 0; 0 1); σ1 = (0 1; 1 0); σ2 = (0 -i; i 0); σ3 = (1 0; 0 -1);

GenerateGamma = Do[γ[4 m + n] = 1/2 Kron[σm, σn], {m, 0, 3}, {n, 0, 3}]

γ[16] := γ[0]

γ[1] // Simplify // MF

( 0    1/2  0    0
  1/2  0    0    0
  0    0    0    1/2
  0    0    1/2  0   )

γ[2] // Simplify // MF

( 0    -i/2  0    0
  i/2  0     0    0
  0    0     0    -i/2
  0    0     i/2  0    )
```


generators of the Lie algebra $SU(2)\otimes SU(2)$

$$\hat{\gamma}_1 = \tfrac{1}{2}\begin{bmatrix} 0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0 \end{bmatrix}, \quad \hat{\gamma}_2 = \tfrac{1}{2}\begin{bmatrix} 0&-i&0&0\\i&0&0&0\\0&0&0&-i\\0&0&i&0 \end{bmatrix}, \quad \hat{\gamma}_3 = \tfrac{1}{2}\begin{bmatrix} 1&0&0&0\\0&-1&0&0\\0&0&1&0\\0&0&0&-1 \end{bmatrix}, \quad \hat{\gamma}_4 = \tfrac{1}{2}\begin{bmatrix} 0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0 \end{bmatrix},$$

$$\hat{\gamma}_5 = \tfrac{1}{2}\begin{bmatrix} 0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0 \end{bmatrix}, \quad \hat{\gamma}_6 = \tfrac{1}{2}\begin{bmatrix} 0&0&0&-i\\0&0&i&0\\0&-i&0&0\\i&0&0&0 \end{bmatrix}, \quad \hat{\gamma}_7 = \tfrac{1}{2}\begin{bmatrix} 0&0&1&0\\0&0&0&-1\\1&0&0&0\\0&-1&0&0 \end{bmatrix}, \quad \hat{\gamma}_8 = \tfrac{1}{2}\begin{bmatrix} 0&0&-i&0\\0&0&0&-i\\i&0&0&0\\0&i&0&0 \end{bmatrix},$$

$$\hat{\gamma}_9 = \tfrac{1}{2}\begin{bmatrix} 0&0&0&-i\\0&0&-i&0\\0&i&0&0\\i&0&0&0 \end{bmatrix}, \quad \hat{\gamma}_{10} = \tfrac{1}{2}\begin{bmatrix} 0&0&0&-1\\0&0&1&0\\0&1&0&0\\-1&0&0&0 \end{bmatrix}, \quad \hat{\gamma}_{11} = \tfrac{1}{2}\begin{bmatrix} 0&0&-i&0\\0&0&0&i\\i&0&0&0\\0&-i&0&0 \end{bmatrix}, \quad \hat{\gamma}_{12} = \tfrac{1}{2}\begin{bmatrix} 1&0&0&0\\0&1&0&0\\0&0&-1&0\\0&0&0&-1 \end{bmatrix},$$

$$\hat{\gamma}_{13} = \tfrac{1}{2}\begin{bmatrix} 0&1&0&0\\1&0&0&0\\0&0&0&-1\\0&0&-1&0 \end{bmatrix}, \quad \hat{\gamma}_{14} = \tfrac{1}{2}\begin{bmatrix} 0&-i&0&0\\i&0&0&0\\0&0&0&i\\0&0&-i&0 \end{bmatrix}, \quad \hat{\gamma}_{15} = \tfrac{1}{2}\begin{bmatrix} 1&0&0&0\\0&-1&0&0\\0&0&-1&0\\0&0&0&1 \end{bmatrix}, \quad \hat{\gamma}_{16} = \tfrac{1}{2}\begin{bmatrix} 1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1 \end{bmatrix}.$$

reconstruction analysis

projection measurement

$$\hat{\mu}_\nu = |\psi_\nu\rangle\langle\psi_\nu|$$

average number of coincidence counts

$$n_\nu = \mathcal{N}\langle\psi_\nu|\hat{\rho}|\psi_\nu\rangle$$

reconstructed ρ

$$\hat{\rho} = (\mathcal{N})^{-1}\sum_{\nu=1}^{16}\hat{M}_\nu n_\nu$$

where

$$\hat{M}_\nu = \sum_{\nu=1}^{16}\left(B^{-1}\right)_{\nu,\mu}\hat{\gamma}_\mu.$$

$$B = [B_{\nu,\mu}]_{16\times16} \quad \text{with} \quad B_{\nu,\mu} = \langle\psi_\nu|\hat{\gamma}_\mu|\psi_\nu\rangle$$

non-singularity of B $\leftrightarrow$ sensitivity of method

$$\mathbf{B} = [B_{m,n}]_{16\times16} \quad \text{where} \quad B_{m,n} = \langle\psi_m|\hat{\gamma}_n|\psi_m\rangle$$

```
b[m_, n_] := hc[psi[m]].γ[n].psi[m]
B := Table[b[m, n][[1, 1]], {m, 1, 16}, {n, 1, 16}]

B // MF
```

$$\begin{pmatrix}
0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & \frac{1}{2} & \frac{1}{2} \\
0 & 0 & -\frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & -\frac{1}{2} & \frac{1}{2} \\
0 & 0 & -\frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{2} & 0 & 0 & \frac{1}{2} & \frac{1}{2} \\
0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{2} & 0 & 0 & -\frac{1}{2} & \frac{1}{2} \\
0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & -\frac{1}{2} & 0 & 0 & -\frac{1}{2} & 0 & 0 & 0 & 0 & \frac{1}{2} \\
0 & 0 & -\frac{1}{2} & 0 & 0 & 0 & 0 & -\frac{1}{2} & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & \frac{1}{2} \\
0 & 0 & -\frac{1}{2} & -\frac{1}{2} & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \\
0 & 0 & \frac{1}{2} & -\frac{1}{2} & 0 & 0 & -\frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \\
0 & -\frac{1}{2} & 0 & -\frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \\
-\frac{1}{2} & 0 & 0 & -\frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \\
-\frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \\
-\frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & -\frac{1}{2} & 0 & 0 & \frac{1}{2} \\
-\frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{2} & \frac{1}{2} & 0 & 0 & \frac{1}{2} \\
0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{2} & 0 & -\frac{1}{2} & 0 & \frac{1}{2} \\
0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & \frac{1}{2} \\
0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & -\frac{1}{2} & 0 & -\frac{1}{2} & 0 & 0 & 0 & 0 & 0 & \frac{1}{2}
\end{pmatrix}$$

inverse matrix B^{-1}

```
invB := Inverse[B]
invB // MF
```

$$\begin{pmatrix}
\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & 0 & 0 & 0 \\
-\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & 0 & -1 & -1 & 0 & 2 & 0 & -1 & -1 & 0 & 0 & 0 \\
-\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & 0 & 0 & -1 & -1 & 2 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -1 & -1 & 0 & 0 & 0 & 0 & 2 & -1 & -1 & 0 & 0 & 0 \\
-\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & -2 \\
\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\
-\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\
\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

$\hat{M}_\nu = \sum_{\nu=1}^{16} B^{-1}_{\nu,\mu}\,\hat{\gamma}_\mu$ for our set of tomographic states

```
M[n_] := Sum[invB[[m, n]] γ[m], {m, 1, 16}]
M[1] // MF
```

$$\begin{pmatrix}
1 & \frac{1}{2}+\frac{i}{2} & \frac{1}{2}-\frac{i}{2} & \frac{1}{2} \\
\frac{1}{2}-\frac{i}{2} & 0 & -\frac{i}{2} & 0 \\
\frac{1}{2}+\frac{i}{2} & \frac{i}{2} & 0 & 0 \\
\frac{1}{2} & 0 & 0 & 0
\end{pmatrix}$$

```
M[2] // MF
```

$$\begin{pmatrix}
0 & \frac{1}{2}+\frac{i}{2} & 0 & \frac{1}{2} \\
\frac{1}{2}-\frac{i}{2} & 1 & -\frac{i}{2} & \frac{1}{2}-\frac{i}{2} \\
0 & \frac{i}{2} & 0 & 0 \\
\frac{1}{2} & \frac{1}{2}+\frac{i}{2} & 0 & 0
\end{pmatrix}$$

```
M[16] // MF
```

$$\begin{pmatrix}
0 & 0 & 0 & 1 \\
0 & 0 & -1 & 0 \\
0 & -1 & 0 & 0 \\
1 & 0 & 0 & 0
\end{pmatrix}$$

another common set of tomographic states

No.	Mode 1	Mode 2
1	$\|H\rangle$	$\|H\rangle$
2	$\|H\rangle$	$\|V\rangle$
3	$\|V\rangle$	$\|V\rangle$
4	$\|V\rangle$	$\|H\rangle$
5	$\|R\rangle$	$\|H\rangle$
6	$\|R\rangle$	$\|V\rangle$
7	$\|D\rangle$	$\|V\rangle$
8	$\|D\rangle$	$\|H\rangle$
9	$\|D\rangle$	$\|R\rangle$
10	$\|D\rangle$	$\|D\rangle$
11	$\|R\rangle$	$\|D\rangle$
12	$\|H\rangle$	$\|D\rangle$
13	$\|V\rangle$	$\|D\rangle$
14	$\|V\rangle$	$\|L\rangle$
15	$\|H\rangle$	$\|L\rangle$
16	$\|R\rangle$	$\|L\rangle$

Note: we have just replaced $\overline{D}$ by D.

$\hat{M}_\nu = \sum_{\nu=1}^{16} B^{-1}_{\nu,\mu}\,\hat{\gamma}_\mu$ for the new set of tomographic states

```
b[m_, n_] := hc[psi[m]].γ[n].psi[m]
B := Table[b[n, m][[1, 1]], {n, 1, 16}, {m, 1, 16}]
invB := Inverse[B]
M[n_] := Sum[invB[[m, n]] γ[m], {m, 1, 16}]
M[1] // MF
```

$$\begin{pmatrix} 1 & -\frac{1}{2}+\frac{i}{2} & -\frac{1}{2}-\frac{i}{2} & \frac{1}{2} \\ -\frac{1}{2}-\frac{i}{2} & 0 & \frac{i}{2} & 0 \\ -\frac{1}{2}+\frac{i}{2} & -\frac{i}{2} & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 0 \end{pmatrix}$$

```
M[2] // MF
```

$$\begin{pmatrix} 0 & -\frac{1}{2}+\frac{i}{2} & 0 & \frac{1}{2} \\ -\frac{1}{2}-\frac{i}{2} & 1 & \frac{i}{2} & -\frac{1}{2}-\frac{i}{2} \\ 0 & -\frac{i}{2} & 0 & 0 \\ \frac{1}{2} & -\frac{1}{2}+\frac{i}{2} & 0 & 0 \end{pmatrix}$$

16 matrices $\hat{M}_n$ for the latter tomographic states

$$\hat{M}_1 = \frac{1}{2}\begin{pmatrix} 2 & -\beta & -\alpha & 1 \\ -\alpha & 0 & i & 0 \\ -\beta & -i & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad \hat{M}_2 = \frac{1}{2}\begin{pmatrix} 0 & -\beta & 0 & 1 \\ -\alpha & 2 & i & -\alpha \\ 0 & -i & 0 & 0 \\ 1 & -\alpha & 0 & 0 \end{pmatrix},$$

$$\hat{M}_3 = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & i & -\alpha \\ 0 & -i & 0 & -\beta \\ 1 & -\beta & -\alpha & 2 \end{pmatrix}, \quad \hat{M}_4 = \frac{1}{2}\begin{pmatrix} 0 & 0 & -\alpha & 1 \\ 0 & 0 & i & 0 \\ -\beta & -i & 2 & -\beta \\ 1 & 0 & -\alpha & 0 \end{pmatrix},$$

$$\hat{M}_5 = \frac{1}{2}\begin{pmatrix} 0 & 0 & 2i & -\alpha \\ 0 & 0 & \beta & 0 \\ -2i & \alpha & 0 & 0 \\ -\beta & 0 & 0 & 0 \end{pmatrix}, \quad \hat{M}_6 = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & -\alpha \\ 0 & 0 & \beta & 2i \\ 0 & \alpha & 0 & 0 \\ -\beta & -2i & 0 & 0 \end{pmatrix},$$

$$\hat{M}_7 = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & -\alpha \\ 0 & 0 & -\beta & 2 \\ 0 & -\alpha & 0 & 0 \\ -\beta & 2 & 0 & 0 \end{pmatrix}, \quad \hat{M}_8 = \frac{1}{2}\begin{pmatrix} 0 & 0 & 2 & -\alpha \\ 0 & 0 & -\beta & 0 \\ 2 & -\alpha & 0 & 0 \\ -\beta & 0 & 0 & 0 \end{pmatrix},$$

$$\hat{M}_9 = \begin{pmatrix} 0 & 0 & 0 & i \\ 0 & 0 & -i & 0 \\ 0 & i & 0 & 0 \\ -i & 0 & 0 & 0 \end{pmatrix}, \quad \hat{M}_{10} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

$$\hat{M}_{11} = \begin{pmatrix} 0 & 0 & 0 & i \\ 0 & 0 & i & 0 \\ 0 & -i & 0 & 0 \\ -i & 0 & 0 & 0 \end{pmatrix}, \quad \hat{M}_{12} = \frac{1}{2}\begin{pmatrix} 0 & 2 & 0 & -\alpha \\ 2 & 0 & -\alpha & 0 \\ 0 & -\beta & 0 & 0 \\ -\beta & 0 & 0 & 0 \end{pmatrix},$$

$$\hat{M}_{13} = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & -\alpha \\ 0 & 0 & -\alpha & 0 \\ 0 & -\beta & 0 & 2 \\ -\beta & 0 & 2 & 0 \end{pmatrix}, \quad \hat{M}_{14} = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & -\beta \\ 0 & 0 & -\beta & 0 \\ 0 & -\alpha & 0 & -2i \\ -\alpha & 0 & 2i & 0 \end{pmatrix},$$

$$\hat{M}_{15} = \frac{1}{2}\begin{pmatrix} 0 & -2i & 0 & -\beta \\ 2i & 0 & \beta & 0 \\ 0 & \alpha & 0 & 0 \\ -\alpha & 0 & 0 & 0 \end{pmatrix}, \quad \hat{M}_{16} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

where $\alpha \equiv 1 + i; \beta \equiv 1 - i$.

Note: other $\hat{M}_n$'s are obtained for other sets of rotations.

experimental example of James et al.

counts for 16 projection measurements

$$n_1 = 34749, n_2 = 324, n_3 = 35805, n_4 = 444,$$
$$n_5 = 16324, n_6 = 17521, n_7 = 13441, n_8 = 16901,$$
$$n_9 = 17932, n_{10} = 32028, n_{11} = 15132, n_{12} = 17238,$$
$$n_{13} = 13171, n_{14} = 17170, n_{15} = 16722, n_{16} = 33586$$

reconstructed $\hat{\rho}$ by linear tomography

$$\hat{\rho} = \begin{pmatrix} 0.4872 & 0.0042 + i0.0114 & 0.0098 - i0.0178 & 0.5192 - i0.0380 \\ 0.0042 - i0.0114 & 0.0045 & 0.0271 + i0.0146 & 0.0648 - i0.0076 \\ 0.0098 + i0.0178 & 0.0271 - i0.0146 & 0.0062 & 0.0695 + i0.0134 \\ 0.5192 + i0.0380 & 0.0648 + i0.0076 & 0.0695 - i0.0134 & 0.5020 \end{pmatrix}$$

problems with semi-definiteness and normalization

$$\mathrm{eig}\,\hat{\rho} = \{1.02155, 0.0681238, -0.065274, -0.024396\}$$
$$\mathrm{Tr}\,\hat{\rho}^2 = 1.053$$

this is not a physical density matrix!

maximum-likelihood (MaxLik) method

1. construct explicitly a "physical" density matrix $\hat{\rho}_{\text{phys}}$

- normalized
- Hermitian
- positive

e.g.

$$\hat{\rho}_{\text{phys}} \equiv \hat{\rho}_{\text{phys}}(t_1, t_2, \ldots t_{16}) = \frac{\hat{T}^\dagger \hat{T}}{\mathrm{Tr}\{\hat{T}^\dagger \hat{T}\}}$$

with e.g.

$$\hat{T} = \begin{pmatrix} t_1 & 0 & 0 & 0 \\ t_5 + it_6 & t_2 & 0 & 0 \\ t_{11} + it_{12} & t_7 + it_8 & t_3 & 0 \\ t_{15} + it_{16} & t_{13} + it_{14} & t_9 + it_{10} & t_4 \end{pmatrix},$$

of lower-triangular (or upper-triangular) form, which is easily invertible

By the **Schur decomposition**, any normal matrix $\hat{A}$ (i.e., $\hat{A}^\dagger \hat{A} = \hat{A}\hat{A}^\dagger$) can be represented as $\hat{A} = \hat{U}\hat{T}\hat{U}^\dagger$ in terms of a triangular $\hat{T}$ and a unitary $\hat{U}$. For simplicity, we neglect $\hat{U}$.

maximum-likelihood method

2. construct a likelihood function

assuming e.g. **Gaussian noise** of the measurements, the probability of obtaining a set of counts

$$\mathbf{n} = (n_1, n_2, \ldots n_{16})$$

for given $\hat{\rho}_{\text{phys}}(\mathbf{t})$ with $\mathbf{t} = (t_1, t_2, \ldots t_{16})$

is

$$P(\mathbf{n}, \mathbf{t}) = \frac{1}{N_{\text{norm}}(\mathbf{t})} \prod_{\nu=1}^{16} \exp\left[-\frac{(n_\nu - \bar{n}_\nu(\mathbf{t}))^2}{2\sigma_\nu^2(\mathbf{t})}\right]$$

where

$\bar{n}_\nu(\mathbf{t}) = \mathcal{N}\langle\psi_\nu|\hat{\rho}_{\text{phys}}(\mathbf{t})|\psi_\nu\rangle$ – number of counts expected for νth measurement

$\sigma_\nu(\mathbf{t}) \approx \sqrt{\bar{n}_\nu(\mathbf{t})}$ – standard deviation

$\mathcal{N} = \sum_{\nu=1}^{4} n_\nu \gg 1$ – normalization, so $\frac{\bar{n}_\nu}{\mathcal{N}}$ corresponds to a probability

$N_{\text{norm}}(\mathbf{t}) = \text{const}$ – normalization assumed to be independent of $\mathbf{t}$

maximum-likelihood method

3. optimize $\hat{\rho}_{\text{phys}}(\mathbf{t})$:

find numerically a maximum of $P(\mathbf{n}, \mathbf{t})$

for a given measured data $\mathbf{n}$:

$$\max_{\mathbf{t}} \prod_{\nu=1}^{16} \exp\left[-\frac{\left(\mathcal{N}\langle\psi_\nu|\hat{\rho}_p(\mathbf{t})|\psi_\nu\rangle - n_\nu\right)^2}{2\mathcal{N}\langle\psi_\nu|\hat{\rho}_p(\mathbf{t})|\psi_\nu\rangle}\right].$$

or, equivalently, analyze logarithm of $P(\mathbf{n}, \mathbf{t})$:

$$\max_{\mathbf{t}} \sum_{\nu=1}^{16} -\frac{\left(\mathcal{N}\langle\psi_\nu|\hat{\rho}_p(\mathbf{t})|\psi_\nu\rangle - n_\nu\right)^2}{2\mathcal{N}\langle\psi_\nu|\hat{\rho}_p(\mathbf{t})|\psi_\nu\rangle} = \frac{\mathcal{N}}{2} \min_{\mathbf{t}} \mathcal{L}(\mathbf{t})$$

where

$$\mathcal{L}(\mathbf{t}) = \sum_{\nu=1}^{16} \frac{\left(\langle\psi_\nu|\hat{\rho}_p(\mathbf{t})|\psi_\nu\rangle - \frac{n_\nu}{\mathcal{N}}\right)^2}{\langle\psi_\nu|\hat{\rho}_p(\mathbf{t})|\psi_\nu\rangle}$$

is a useful **'likelihood' function**.

‘likelihood’ function

```
L[t1_, t2_, t3_, t4_, t5_, t6_, t7_, t8_, t9_, t10_, t11_,
  t12_, t13_, t14_, t15_, t16_] := Module[{T, RhoPhys, sum, Nmean},
  T := ( t1          0          0       0
         t5 + i t6   t2         0       0
         t11 + i t12 t7 + i t8  t3      0
         t15 + i t16 t13 + i t14 t9 + i t10 t4 );
  RhoPhys := hc[T].T / Tr[hc[T].T];
  sum = 0;
  Do[
   {Nmean = Re[Norm * hc[psi[m]].ρphys.psi[m]];
    sum = sum + (Nmean - Nexp[[m]])^2 / 2 / Nmean}, {m, 1, 16}];
  Return[Re[sum]]
 ];
```

numerical optimalization

```
FindMinimum[
L[t1,t2,t3,t4,t5,t6,t7,t8,t9,t10,t11,t12,t13,t14,t15,t16],
{t1,tini1},{t2,tini2},{t3,tini3},{t4,tini4},{t5,tini5},{t6,tini6},
{t7,tini7},{t8,tini8},{t9,tini9},{t10,tini10},{t11,tini11},
{t12,tini12},{t13,tini13},{t14,tini14},{t15,tini15},{t16,tini16}]
```

thus, we need initial values $\mathbf{t}_{\rm ini}$.

How to estimate initial ‘physical’ matrix $\hat{T}(\mathbf{t}_{\rm ini})$?

By calculating $\hat{T}$ from our “unphysical” $\hat{\rho}$:

$$\hat{T}(\mathbf{t}_{\rm ini}) = \begin{pmatrix} \sqrt{\frac{\mathcal{M}^{(0)}}{\mathcal{M}^{(1)}_{00}}} & 0 & 0 & 0 \\ \frac{\mathcal{M}^{(1)}_{01}}{\sqrt{\mathcal{M}^{(1)}_{00}\mathcal{M}^{(2)}_{00,11}}} & \sqrt{\frac{\mathcal{M}^{(1)}_{00}}{\mathcal{M}^{(2)}_{00,11}}} & 0 & 0 \\ \frac{\mathcal{M}^{(2)}_{01,12}}{\sqrt{\rho_{33}}\sqrt{\mathcal{M}^{(2)}_{00,11}}} & \frac{\mathcal{M}^{(2)}_{00,12}}{\sqrt{\rho_{33}}\sqrt{\mathcal{M}^{(2)}_{00,11}}} & \sqrt{\frac{\mathcal{M}^{(2)}_{00,11}}{\rho_{33}}} & 0 \\ \frac{\rho_{30}}{\sqrt{\rho_{33}}} & \frac{\rho_{31}}{\sqrt{\rho_{33}}} & \frac{\rho_{32}}{\sqrt{\rho_{33}}} & \sqrt{\rho_{33}} \end{pmatrix}$$

where

$\mathcal{M}^{(0)} = {\rm Det}(\hat{\rho})$,

$\mathcal{M}^{(1)}_{ij} = {\rm Det}(\hat{\rho}_{\text{without row i \& col j}})$,

$\mathcal{M}^{(2)}_{ij,kl} = {\rm Det}(\hat{\rho}_{\text{without rows i,k \& cols j,l}})$

$i, j, k, l = 0, ..., 3$

for our experimental data

$$\hat{T}(\mathbf{t}_{\rm ini}) = \begin{bmatrix} 0.5948i & 0 & 0 & 0 \\ 0.8706 + 0.7282i & 0.4060 & 0 & 0 \\ -0.0215 + 0.9933i & -0.2827 - 0.2982i & 0.0615i & 0 \\ 0.7328 + 0.0536i & 0.0915 + 0.0107i & 0.0981 - 0.0189i & 0.7085 \end{bmatrix}$$

$$\hat{\rho}_{\rm phys}(\mathbf{t}_{\rm ini}) = \begin{bmatrix} 0.7870 & 0.0325 - 0.0014i & 0.0328 - 0.0051i & 0.1289 - 0.0094i \\ 0.0325 + 0.0014i & 0.0850 & -0.0024 - 0.0050i & 0.0161 - 0.0019i \\ 0.0328 + 0.0051i & -0.0024 + 0.0050i & 0.0034 & 0.0173 + 0.0033i \\ 0.1289 + 0.0094i & 0.0161 + 0.0019i & 0.0173 - 0.0033i & 0.1247 \end{bmatrix}$$

$$\mathcal{L}(\mathbf{t}_{\rm ini}) = 3.0695$$

by applying the optimalization procedure we can diminish this value to

$$\mathcal{L}(\mathbf{t}_{\rm opt}) = 0.0104$$

for the following matrix ...

our matrix reconstructed by MaxLik method

$$\hat{\rho}_{\rm phys}(\mathbf{t}_{\rm opt}) = \begin{bmatrix} 0.5028 & 0.0230 + 0.0117i & 0.0279 - 0.0130i & 0.4686 - 0.0346i \\ 0.0230 - 0.0117i & 0.0051 & 0.0050 + 0.0001i & 0.0333 - 0.0082i \\ 0.0279 + 0.0130i & 0.0050 - 0.0001i & 0.0066 & 0.0416 + 0.0102i \\ 0.4686 + 0.0346i & 0.0333 + 0.0082i & 0.0416 - 0.0102i & 0.4854 \end{bmatrix}$$

is a physical density matrix as it is

- positive (semidefinite)

$${\rm eig}\,\hat{\rho}_{\rm phys} = \{0.9687, 0.0313, 0, 0\}$$

- Hermitian

$$\hat{\rho}_{\rm phys} = \hat{\rho}^{\dagger}_{\rm phys}$$

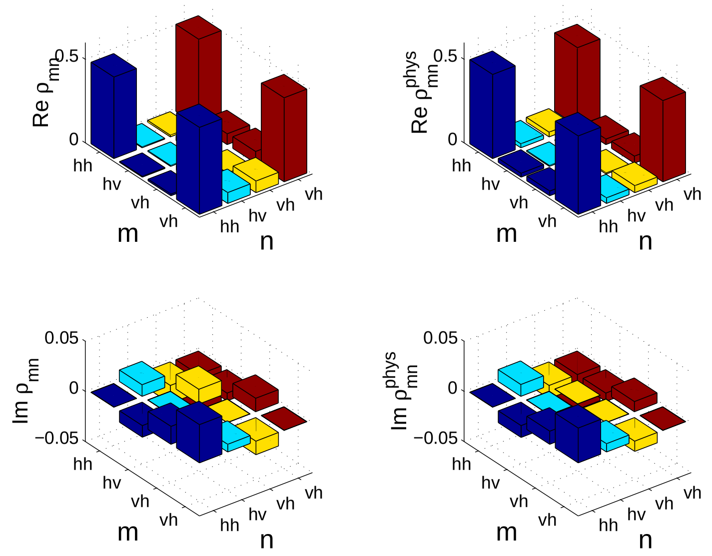
- normalized

$${\rm Tr}\{\hat{\rho}_{\rm phys}\} = 1$$

$${\rm Tr}\{\hat{\rho}^2_{\rm phys}\} = 0.9394 \leq 1$$

comparison of reconstructed matrices

$\hat{\rho}$ by linear tomography (left) and $\hat{\rho}_{\rm phys}$ by MaxLik tomography (right figures)



reconstruction of a qutrit density matrix

$$\hat{\rho}=\frac{1}{3}\begin{bmatrix} 1+\frac{\sqrt{3}}{2}(\langle\hat{\sigma}_8\rangle+\sqrt{3}\langle\hat{\sigma}_3\rangle) & \frac{3}{2}(\langle\hat{\sigma}_1\rangle-i\langle\hat{\sigma}_2\rangle) & \frac{3}{2}(\langle\hat{\sigma}_4\rangle-i\langle\hat{\sigma}_5\rangle)\\ \frac{3}{2}(\langle\hat{\sigma}_1\rangle+i\langle\hat{\sigma}_2\rangle) & 1+\frac{\sqrt{3}}{2}(\langle\hat{\sigma}_8\rangle-\sqrt{3}\langle\hat{\sigma}_3\rangle) & \frac{3}{2}(\langle\hat{\sigma}_6\rangle-i\langle\hat{\sigma}_7\rangle)\\ \frac{3}{2}(\langle\hat{\sigma}_4\rangle+i\langle\hat{\sigma}_5\rangle) & \frac{3}{2}(\langle\hat{\sigma}_6\rangle+i\langle\hat{\sigma}_7\rangle) & 1-\sqrt{3}\langle\hat{\sigma}_8\rangle \end{bmatrix}$$

via measurement of the generalized Pauli operators

which can be chosen as generators of the Lie algebra $SU(3)$

$$\hat{\sigma}_1=\begin{bmatrix}0&1&0\\1&0&0\\0&0&0\end{bmatrix},\quad \hat{\sigma}_2=\begin{bmatrix}0&-i&0\\i&0&0\\0&0&0\end{bmatrix},\hat{\sigma}_3=\begin{bmatrix}1&0&0\\0&-1&0\\0&0&0\end{bmatrix},\hat{\sigma}_4=\begin{bmatrix}0&0&1\\0&0&0\\1&0&0\end{bmatrix},$$

$$\hat{\sigma}_5=\begin{bmatrix}0&0&-i\\0&0&0\\i&0&0\end{bmatrix},\ \hat{\sigma}_6=\begin{bmatrix}0&0&0\\0&0&1\\0&1&0\end{bmatrix},\hat{\sigma}_7=\begin{bmatrix}0&0&0\\0&0&-i\\0&i&0\end{bmatrix},\hat{\sigma}_8=\frac{1}{\sqrt{3}}\begin{bmatrix}1&0&0\\0&1&0\\0&0&-2\end{bmatrix}.$$

Analogously, **a qudit density matrix** can be reconstructed via measurement of generators of the Lie algebra $SU(d)$

Question

Quantum tomography and no-cloning theorem:

For complete reconstruction of $\hat{\rho}$ we need to repeat measurements on many copies of $\hat{\rho}$.

But unknown $\hat{\rho}$ cannot be copied.

Thus, do we violate the no-cloning theorem?

Answer

No! The term “copies” refers to identically prepared quantum objects.

Copies of $\hat{\rho}$ are generated from the same (known) initial state(s) by applying the same transformations in the same experimental setup.

Quantum gates
(part II)

reversible gates

Toffoli and CCU gates

simulation of gates by various circuits

reversible computing

- a computational process that is (or almost is) time-invertible (time-reversible).

Landauer's principle

- a computational process to be **physically reversible**, it must also be **logically reversible**.

logically-reversible process

- a discrete, deterministic computational process for which the transition function that maps input states to output states is a one-to-one function.

examples of reversible quantum gates

all unitary quantum gates are reversible, e.g.:

$$\hat{H}(c_0|0\rangle + c_1|1\rangle) = c_0|+\rangle + c_1|-\rangle \quad \rightarrow \quad \hat{H}(c_0|+\rangle + c_1|-\rangle) = c_0|0\rangle + c_1|1\rangle$$

$$|\psi_{\mathrm{in}}\rangle = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle$$

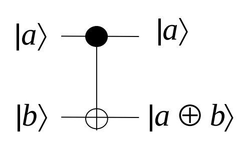
$$\hat{U}_{\mathrm{CNOT}}|\psi_{\mathrm{in}}\rangle = c_0|00\rangle + c_1|01\rangle + c_2|11\rangle + c_3|10\rangle \equiv |\psi_{\mathrm{out}}\rangle$$

$$\hat{U}_{\mathrm{CNOT}}|\psi_{\mathrm{out}}\rangle = c_0|00\rangle + c_1|01\rangle + c_2|1, 1 \oplus 1\rangle + c_3|1, 0 \oplus 1\rangle = |\psi_{\mathrm{in}}\rangle$$

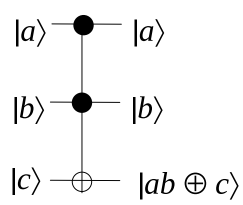
but measurement is irreversible

CNOT and Toffoli gates

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$



examples of irreversible classical gates

logic gates in a classical computer, other than NOT gate, are irreversible, e.g.:

```
AND          OR           XOR=CNOT
ab | c       ab | c       ab | c
--------     --------     --------
00 | 0       00 | 0       00 | 0
01 | 0       01 | 1       01 | 1
10 | 0       10 | 1       10 | 1
11 | 1       11 | 1       11 | 0
```

how to make these gates reversible?

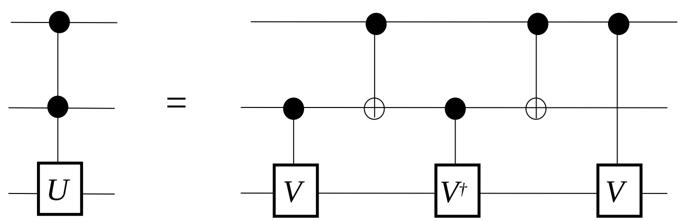
keep input(s) together with the standard output, e.g.:

```
R-AND         R-OR          R-XOR
ab | abc      ab | abc      ab | abc    ac    bc
----------    ----------    ------------------
00 | 000      00 | 000      00 | 000    00    00
01 | 010      01 | 011      01 | 011    01    11
10 | 100      10 | 101      10 | 101    11    01
11 | 111      11 | 111      11 | 110    10    10
```

replacement for CCU gate

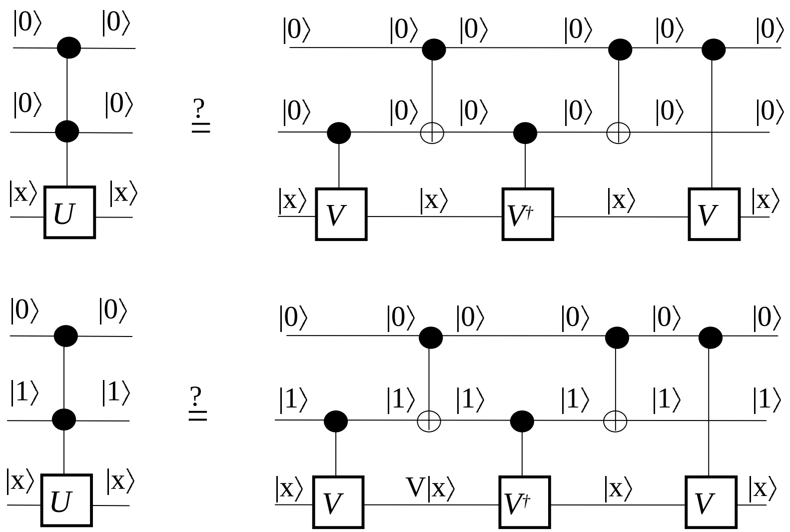
theorem of Barenco,Bennett et al. (1995)

Any CCU gate can be built from CNOT, CV, and CV† gates, where $V^2 = U$



Note: Toffoli gate is a special case of CCU

replacement for CCU gate (proof)



implementing gates in *Mathematica*

- **two-qubit states**

$\mathrm{ket}[n_1, n_2] = |n_1, n_2\rangle \rightarrow$ 4-element column vector with '1' at pos. $2n_1 + n_2 + 1$

$\mathrm{bra}[n_1, n_2] = \langle n_1, n_2| \rightarrow$ row vector

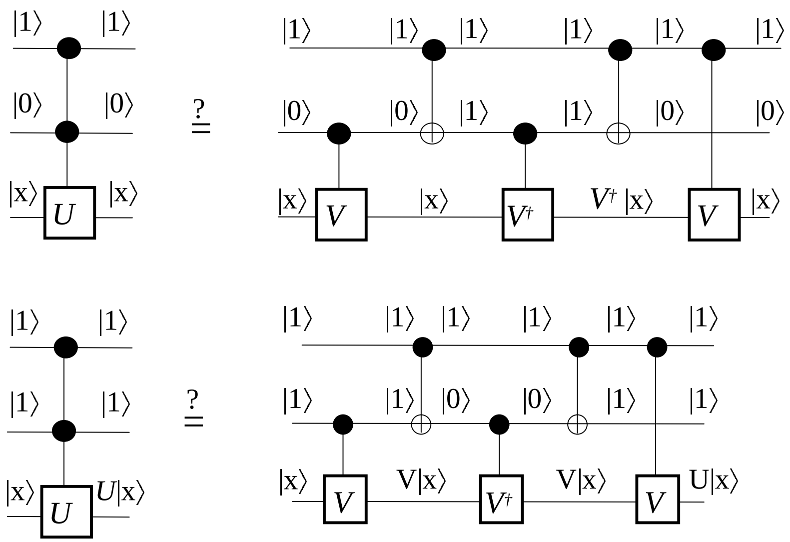
```
ket[n1_, n2_] := Module[{state},
  state = ZeroMatrix[4, 1];
  state[[2 n1 + n2 + 1, 1]] = 1;
  Return[state]]
bra[n1_, n2_] := Transpose[ket[n1, n2]]
ket[0, 0] // MF
```

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

```
ket[1, 1] // MF
```

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

replacement for CCU gate (proof)



CNOT gate – $\mathrm{cnot} = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|$

```
cnot :=
 ket[0, 0].bra[0, 0] + ket[0, 1].bra[0, 1] + ket[1, 1].bra[1, 0] + ket[1, 0].bra[1, 1]
cnot // MF
```

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

CV gate – control unitary $V = \begin{bmatrix} v_{0,0} & v_{0,1} \\ v_{1,0} & v_{1,1} \end{bmatrix}$

$\mathrm{cv} = |00\rangle\langle 00| + |01\rangle\langle 01| + v_{0,0}|10\rangle\langle 10| + v_{0,1}|10\rangle\langle 11| + v_{1,0}|11\rangle\langle 10| + v_{1,1}|11\rangle\langle 11|$

```
cv :=
 ket[0, 0].bra[0, 0] + ket[0, 1].bra[0, 1] +
  v0,0 ket[1, 0].bra[1, 0] + v0,1 ket[1, 0].bra[1, 1] +
  v1,0 ket[1, 1].bra[1, 0] + v1,1 ket[1, 1].bra[1, 1]
cv // MF
```

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & v_{0,0} & v_{0,1} \\ 0 & 0 & v_{1,0} & v_{1,1} \end{pmatrix}$$

• three-qubit states

$\mathrm{KET}[n_1, n_2, n_3] = |n_1, n_2, n_3\rangle \to 2^3$-element column vector with '1' at position $4n_1 + 2n_2 + n_3 + 1$

$\mathrm{BRA}[n_1, n_2, n_3] = \langle n_1, n_2, n_3| \to$ row vector

```
KET[n1_, n2_, n3_] := Module[{state},
  state = ZeroMatrix[8, 1];
  state[[4 n1 + 2 n2 + n3 + 1, 1]] = 1;
  Return[state]]
BRA[n1_, n2_, n3_] := Transpose[KET[n1, n2, n3]]
KET[0, 0, 0] // MF
```

$$\begin{pmatrix}1\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}$$

```
BRA[0, 0, 1] // MF
```

$$\begin{pmatrix}0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\end{pmatrix}$$

```
BRA[1, 1, 1] // MF
```

$$\begin{pmatrix}0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\end{pmatrix}$$

control gates for 3 qubits

1. CNOT$_{23}$=kron(id,cnot) where $\mathrm{id} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$

or $\mathrm{CNOT}_{23} = |000\rangle\langle000| + |001\rangle\langle001| + |011\rangle\langle010| + |010\rangle\langle011| + |100\rangle\langle100| + |101\rangle\langle101| + |111\rangle\langle110| + |110\rangle\langle111|$

```
CNOT23 :=
 KET[0, 0, 0].BRA[0, 0, 0] + KET[0, 0, 1].BRA[0, 0, 1] +
  KET[0, 1, 1].BRA[0, 1, 0] + KET[0, 1, 0].BRA[0, 1, 1] + KET[1, 0, 0].BRA[1, 0, 0] +
  KET[1, 0, 1].BRA[1, 0, 1] + KET[1, 1, 1].BRA[1, 1, 0] + KET[1, 1, 0].BRA[1, 1, 1]

CNOT23 // MF
```

$$\begin{pmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0\end{pmatrix}$$

2. CNOT$_{12}$=kron(cnot,id) – analogously

3. CV$_{23}$=kron(id,cv)

```
CV23new := Kron[id, cv]
CV23new // MF
```

$$\begin{pmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&v_{0,0}&v_{0,1}&0&0&0&0\\0&0&v_{1,0}&v_{1,1}&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&v_{0,0}&v_{0,1}\\0&0&0&0&0&0&v_{1,0}&v_{1,1}\end{pmatrix}$$

or explicitly

```
CV23 :=
 KET[0, 0, 0].BRA[0, 0, 0] + KET[0, 0, 1].BRA[0, 0, 1] +
  v0,0 KET[0, 1, 0].BRA[0, 1, 0] + v0,1 KET[0, 1, 0].BRA[0, 1, 1] +
  v1,0 KET[0, 1, 1].BRA[0, 1, 0] + v1,1 KET[0, 1, 1].BRA[0, 1, 1] +
  KET[1, 0, 0].BRA[1, 0, 0] + KET[1, 0, 1].BRA[1, 0, 1] +
  v0,0 KET[1, 1, 0].BRA[1, 1, 0] + v0,1 KET[1, 1, 0].BRA[1, 1, 1] +
  v1,0 KET[1, 1, 1].BRA[1, 1, 0] + v1,1 KET[1, 1, 1].BRA[1, 1, 1]

CV23 // MF
```

$$\begin{pmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&v_{0,0}&v_{0,1}&0&0&0&0\\0&0&v_{1,0}&v_{1,1}&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&v_{0,0}&v_{0,1}\\0&0&0&0&0&0&v_{1,0}&v_{1,1}\end{pmatrix}$$

4. CV$_{13}$ gate

$$\begin{aligned}\mathrm{CV}_{13} &= |000\rangle\langle 000| + |001\rangle\langle 001| + |010\rangle\langle 010| + |011\rangle\langle 011| \\ &+v_{0,0}|100\rangle\langle 100| + v_{0,1}|100\rangle\langle 101| + v_{1,0}|101\rangle\langle 100| + v_{1,1}|101\rangle\langle 101| \\ &+v_{0,0}|110\rangle\langle 110| + v_{0,1}|110\rangle\langle 111| + v_{1,0}|111\rangle\langle 110| + v_{1,1}|111\rangle\langle 111|\end{aligned}$$

```
CV13 :=
 KET[0, 0, 0].BRA[0, 0, 0] + KET[0, 0, 1].BRA[0, 0, 1] +
  KET[0, 1, 0].BRA[0, 1, 0] + KET[0, 1, 1].BRA[0, 1, 1] +
  v0,0 KET[1, 0, 0].BRA[1, 0, 0] + v0,1 KET[1, 0, 0].BRA[1, 0, 1] +
  v1,0 KET[1, 0, 1].BRA[1, 0, 0] + v1,1 KET[1, 0, 1].BRA[1, 0, 1] +
  v0,0 KET[1, 1, 0].BRA[1, 1, 0] + v0,1 KET[1, 1, 0].BRA[1, 1, 1] +
  v1,0 KET[1, 1, 1].BRA[1, 1, 0] + v1,1 KET[1, 1, 1].BRA[1, 1, 1]

CV13 // MF
```

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & v_{0,0} & v_{0,1} & 0 & 0 \\ 0 & 0 & 0 & 0 & v_{1,0} & v_{1,1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & v_{0,0} & v_{0,1} \\ 0 & 0 & 0 & 0 & 0 & 0 & v_{1,0} & v_{1,1} \end{pmatrix}$$

tricky way to calculate CV$_{13}$

CV$_{13}$= SWAP$_{12}$ CV$_{23}$ SWAP$_{12}$ = kron(swap,id) CV$_{23}$ kron(swap,id)

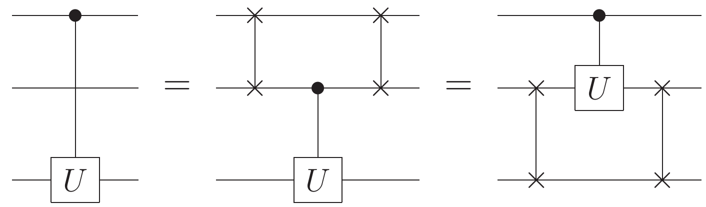
```
CV13new := Kron[swap, id].CV23.Kron[swap, id]
CV13new // MF
```

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & v_{0,0} & v_{0,1} & 0 & 0 \\ 0 & 0 & 0 & 0 & v_{1,0} & v_{1,1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & v_{0,0} & v_{0,1} \\ 0 & 0 & 0 & 0 & 0 & 0 & v_{1,0} & v_{1,1} \end{pmatrix}$$

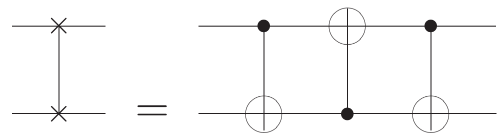
```
test = Max[CV13 - CV13new]

0
```

or CV$_{13}$=SWAP$_{23}$ CV$_{12}$ SWAP$_{23}$ $= \cdots$

substitution circuits for CU$_{13}$ gate



substitution circuit for SWAP gate



5. CCU gate ($U = V^2$)

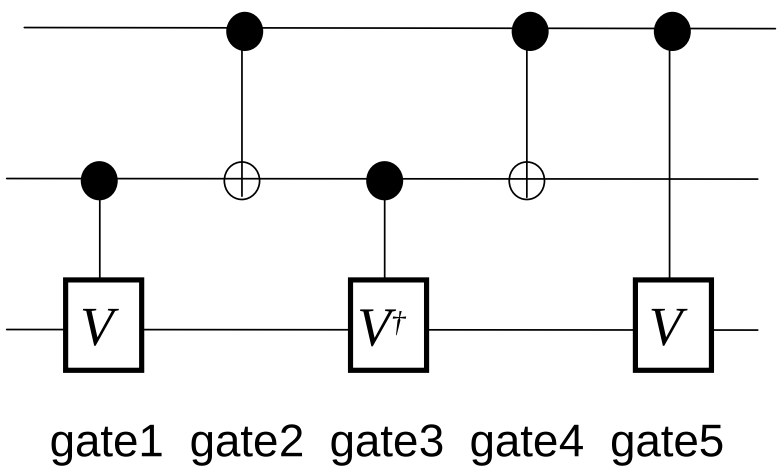
$$\text{CCU} := \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & u_{0,0} & u_{0,1} \\ 0 & 0 & 0 & 0 & 0 & 0 & u_{1,0} & u_{1,1} \end{pmatrix}$$

$$\begin{pmatrix} u_{0,0} & u_{0,1} \\ u_{1,0} & u_{1,1} \end{pmatrix} = \begin{pmatrix} v_{0,0} & v_{0,1} \\ v_{1,0} & v_{1,1} \end{pmatrix} . \begin{pmatrix} v_{0,0} & v_{0,1} \\ v_{1,0} & v_{1,1} \end{pmatrix};$$

$$\begin{pmatrix} u_{0,0} & u_{0,1} \\ u_{1,0} & u_{1,1} \end{pmatrix} \text{ // MF}$$

$$\begin{pmatrix} v_{0,0}^2 + v_{0,1} v_{1,0} & v_{0,0} v_{0,1} + v_{0,1} v_{1,1} \\ v_{0,0} v_{1,0} + v_{1,0} v_{1,1} & v_{0,1} v_{1,0} + v_{1,1}^2 \end{pmatrix}$$

a substitution circuit for CCU gate



substitution circuit for CCU gate

$$\texttt{swap} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}; \; \texttt{cnot} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix};$$

$$\texttt{cv} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & v_{0,0} & v_{0,1} \\ 0 & 0 & v_{1,0} & v_{1,1} \end{pmatrix}; \; \texttt{id = IdentityMatrix[2];}$$

```
gate1 := Kron[id, cv]
gate2 := Kron[cnot, id]
gate3 := Kron[id, hc[cv]]
gate4 := gate2
gate5 := Kron[swap, id].gate1.Kron[swap, id]
CCU1temp := gate5.gate4.gate3.gate2.gate1
```


properties of unitary matrices

a matrix is unitary iff its row and column vectors are orthonormal

thus for

$$V = \begin{bmatrix} v_{0,0} & v_{0,1} \\ v_{1,0} & v_{1,1} \end{bmatrix}$$

we have

$$v_{0,0}^* v_{0,1} + v_{1,0}^* v_{1,1} = 0$$

$$v_{0,0}^* v_{0,0} + v_{0,1}^* v_{0,1} = 1$$

etc.

```
r1 := {Conjugate[v0,0] v0,0 + Conjugate[v1,0] v1,0 → 1}
r2 := {Conjugate[v0,0] v0,0 + Conjugate[v0,1] v0,1 → 1}
r3 := {Conjugate[v0,1] v0,1 + Conjugate[v1,1] v1,1 → 1}
r4 := {Conjugate[v1,0] v1,0 + Conjugate[v1,1] v1,1 → 1}
r5 := {Conjugate[v0,0] v0,1 + Conjugate[v1,0] v1,1 → 0}
r6 := {Conjugate[v0,0] v1,0 + Conjugate[v0,1] v1,1 → 0}
r7 := {Conjugate[v0,1] v0,0 + Conjugate[v1,1] v1,0 → 0}
r8 := {Conjugate[v1,0] v0,0 + Conjugate[v1,1] v0,1 → 0}
```


...finally

```
CCU1 := CCU1temp /. r1 /. r2 /. r3 /. r4 /. r5 /. r6 /. r7 /. r8
CCU1 // MF
```

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & v_{0,0}^2 + v_{0,1} v_{1,0} & v_{0,0} v_{0,1} + v_{0,1} v_{1,1} \\ 0 & 0 & 0 & 0 & 0 & 0 & v_{0,0} v_{1,0} + v_{1,0} v_{1,1} & v_{0,1} v_{1,0} + v_{1,1}^2 \end{pmatrix}$$

```
test = Max[CCU - CCU1] // MF
0
```

we have shown that our gate CCU_1 simulates the original CCU gate

or more explicitly

```
CCU2temp := CV13.Kron[cnot, id].hc[CV23].Kron[cnot, id].CV23

CCU2 := CCU2temp /. r1 /. r2 /. r3 /. r4 /. r5 /. r6 /. r7 /. r8
CCU2 // MF
```

$$\begin{pmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&v_{0,0}^2+v_{0,1}v_{1,0}&v_{0,0}v_{0,1}+v_{0,1}v_{1,1}\\ 0&0&0&0&0&0&v_{0,0}v_{1,0}+v_{1,0}v_{1,1}&v_{0,1}v_{1,0}+v_{1,1}^2 \end{pmatrix}$$

```
test = Max[CCU - CCU2] // MF

0
```


Introduction to quantum error-correction codes

quantum vs classical errors

correction of bit-flip and phase-flip errors

Shor's ECC

Steane's ECC

fault-tolerant gates

a note

without quantum ECCs construction of
practical quantum computers would be impossible

errors in classical computers

bit-flip errors

$0 \to 1$ & $1 \to 0$

errors in quantum computers

1. **bit-flip errors = amplitude errors**

$|0\rangle \to |1\rangle$ & $|1\rangle \to |0\rangle$

2. **phase-flip errors = phase errors**

$|0\rangle \to |0\rangle$ & $|1\rangle \to -|1\rangle$

e.g. $|+\rangle \to |-\rangle$ & $|-\rangle \to |+\rangle$ (orthogonal)

3. **small errors**

$$a|0\rangle + b|1\rangle \to \sqrt{a^2+\epsilon}|0\rangle + \sqrt{b^2-\epsilon}|1\rangle$$

which can also correspond to
removing the qubit and replacing it with garbage!

thus

there is a **continuous set of quantum errors**

error-correcting code (ECC)

quantum states are very fragile to decoherence and dissipation,

thus we need a quantum ECC – an analog of classical ECC

can we really correct quantum errors?

1. **errors are continuous**

there are infinitely many quantum errors

2. **measurement destroys quantum information**

qubits cannot be measured without disturbing quantum information they carry,

i.e., by measuring

$$a|0\rangle + b|1\rangle$$

we get either $|0\rangle$ with probability $|a|^2$ or $|1\rangle$ with probability $|b|^2$

3. **no cloning**

quantum information cannot be copied with perfect fidelity

quantum repetition code

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

$$\begin{aligned}\hat{U}^{12}_{\text{CNOT}}|\psi\rangle|0\rangle &= \hat{U}^{12}_{\text{CNOT}}(a|00\rangle + b|10\rangle) \\ &= a|0, 0\oplus 0\rangle + b|1, 0\oplus 1\rangle \\ &= \underline{a|00\rangle + b|11\rangle}\end{aligned}$$

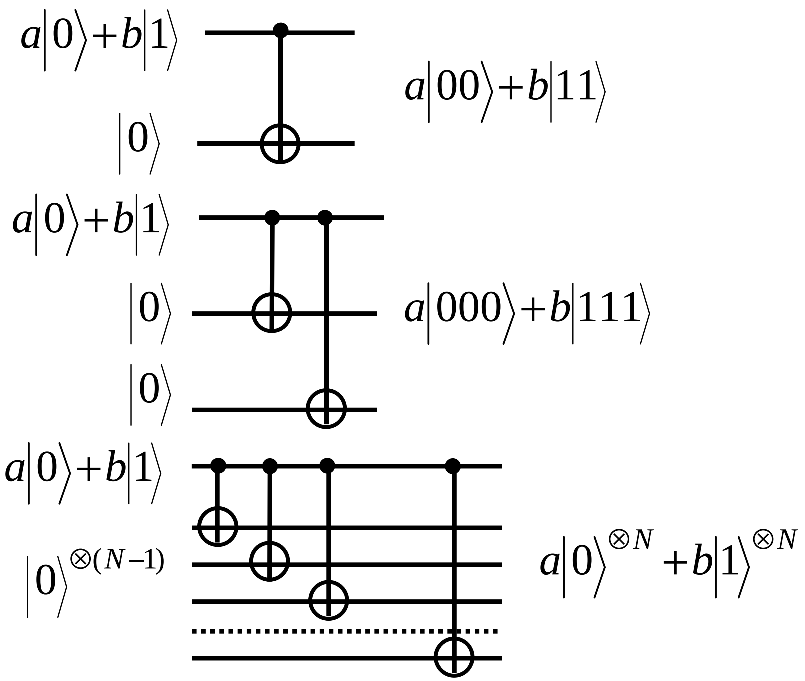
$$\begin{aligned}\hat{U}^{13}_{\text{CNOT}}\hat{U}^{12}_{\text{CNOT}}|\psi\rangle|0\rangle|0\rangle &= \hat{U}^{13}_{\text{CNOT}}(a|00\rangle + b|11\rangle)|0\rangle \\ &= a|0, 0, 0\oplus 0\rangle + b|1, 1, 0\oplus 1\rangle \\ &= \underline{a|000\rangle + b|111\rangle}\end{aligned}$$

note that

$$\hat{U}^{13}_{\text{CNOT}}\hat{U}^{12}_{\text{CNOT}} = \hat{U}^{12}_{\text{CNOT}}\hat{U}^{13}_{\text{CNOT}}$$

in general

$$\prod_{i=2}^{N}\hat{U}^{1n}_{\text{CNOT}}(a|0\rangle + b|1\rangle)|0\rangle^{\otimes(N-1)} = \underline{a|0\rangle^{\otimes N} + b|1\rangle^{\otimes N}}$$



bit-flip error

$$|\psi_0\rangle = a|000\rangle + b|111\rangle \longrightarrow \boxed{\text{3rd bit flip}} \longrightarrow |\psi_1\rangle = a|00\underline{1}\rangle + b|11\underline{0}\rangle$$

error detection = error syndrome diagnosis/measurement

$$|\psi_2\rangle = |\psi_1\rangle|00\rangle = a|00100\rangle + b|11000\rangle$$

$$\begin{aligned}|\psi_3\rangle &= \hat{U}^{24}_{\text{CNOT}}\hat{U}^{14}_{\text{CNOT}}|\psi_2\rangle \\ &= a|\underline{0}, \underline{0}, 1, 0\oplus 0\oplus 0, 0\rangle + b|\underline{1}, \underline{1}, 0, 0\oplus 1\oplus 1, 0\rangle \\ &= a|0, 0, 1, 0, 0\rangle + b|1, 1, 0, 0, 0\rangle = |\psi_2\rangle \quad (\textbf{sic}!)\end{aligned}$$

$$\begin{aligned}|\psi_4\rangle &= \hat{U}^{35}_{\text{CNOT}}\hat{U}^{25}_{\text{CNOT}}|\psi_3\rangle \\ &= a|0, \underline{0}, \underline{1}, 0, 0\oplus 0\oplus 1\rangle + b|1, \underline{1}, \underline{0}, 0, 0\oplus 0\oplus 1\rangle \\ &= a|0, 0, 1, \underline{0, 1}\rangle + b|1, 1, 0, \underline{0, 1}\rangle \\ &= \Big(a|0, 0, 1\rangle + b|1, 1, 0\rangle\Big)\otimes|0, 1\rangle\end{aligned}$$

so let us measure modes 4 & 5:

$$|\psi_5\rangle = {}_{45}\langle M', M''|\psi_4\rangle = a|0, 0, 1\rangle + b|1, 1, 0\rangle$$

in our case the measurement result (i.e. error syndrome) is:

$$M' = 0, M'' = 1$$

error correction = recovery

so we know that we have to flip the 3rd qubit

$$|\psi_6\rangle = \hat{X}_3|\psi_5\rangle = a|0, 0, \underline{0}\rangle + b|1, 1, \underline{1}\rangle = |\psi_0\rangle$$

Analogously, we can find a proper action for other measurement results:

error syndrome $\Longrightarrow$ error correction

$$\begin{aligned}M' &= 0, M'' = 1 \Longrightarrow |\psi_0\rangle = \hat{X}_3|\psi_5\rangle \\ M' &= 1, M'' = 0 \Longrightarrow |\psi_0\rangle = \hat{X}_2|\psi_5\rangle \\ M' &= 1, M'' = 1 \Longrightarrow |\psi_0\rangle = \hat{X}_1|\psi_5\rangle \\ M' &= 0, M'' = 0 \Longrightarrow |\psi_0\rangle = |\psi_5\rangle\end{aligned}$$

so in general

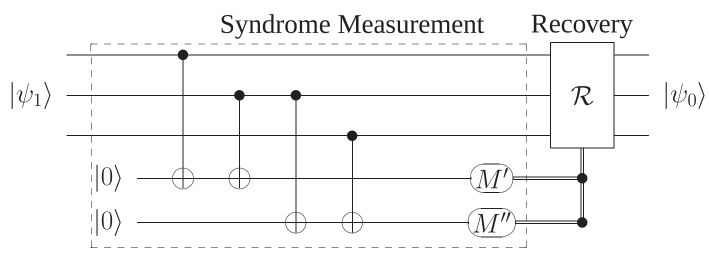
$$|\psi_0\rangle = \hat{X}_{|3M''-2M'|}|\psi_5\rangle, \text{ where } \hat{X}_0 = \hat{I},$$

bit-flip error $|\psi_0\rangle \to |\psi_1\rangle$

$$|\psi_0\rangle = a|000\rangle + b|111\rangle$$

$$|\psi_1\rangle = a|001\rangle + b|110\rangle, a|010\rangle + b|101\rangle, a|100\rangle + b|011\rangle \text{ or } a|000\rangle + b|111\rangle$$

bit-flip error correction $|\psi_1\rangle \to |\psi_0\rangle$



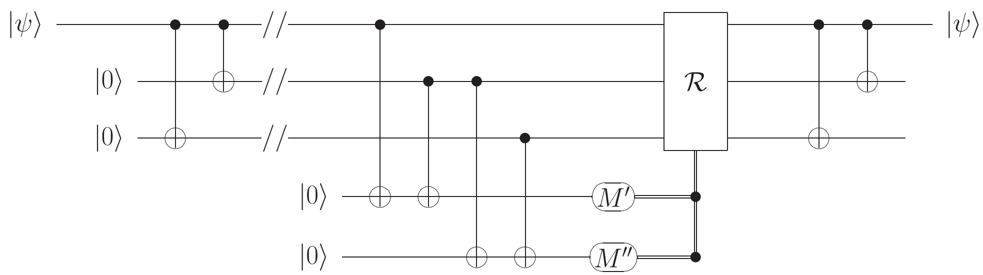
$$|\psi_0\rangle = \hat{X}_{|3M''-2M'|}\Big({}_{45}\langle M', M''|\hat{U}^{35}_{\text{CNOT}}\hat{U}^{25}_{\text{CNOT}}\hat{U}^{24}_{\text{CNOT}}\hat{U}^{14}_{\text{CNOT}}|\psi_1\rangle|00\rangle\Big)$$

a typical error correction code (ECC)

$|\psi\rangle$ — encode — // — syndrome detect — error correct — decode — $|\psi\rangle$

where $-//-$ denotes quantum channel where an error can occur

example: a quantum bit-flip ECC



phase vs amplitude errors

$$\begin{aligned}\hat{H}\hat{\sigma}_z\hat{H} &= \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\\ &= \frac{1}{2}\begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\\ &= \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} = \hat{\sigma}_x\end{aligned}$$

$$\hat{H}\hat{\sigma}_x\hat{H} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} = \hat{\sigma}_z$$

thus

a phase error (phase flip) in a rotated basis

appears as an amplitude error (bit flip) and vice versa.

phase-flip error

$$a|0\rangle + b|1\rangle \to \boxed{\text{phase flip}} \to a|0\rangle - b|1\rangle$$

so

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \to \boxed{\text{phase flip}} \to |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$|-\rangle \to \boxed{\text{phase flip}} \to |+\rangle$$

initial encoding

$$\begin{aligned}a|0\rangle + b|1\rangle &\to |\psi_0\rangle = a|000\rangle + b|111\rangle\\ &\to |\psi_0'\rangle = a|+++\rangle + b|---\rangle\end{aligned}$$

or explicitly

$$\begin{aligned}|\psi_0\rangle &= \hat{H}^{\otimes 3}\hat{U}^{13}_{\text{CNOT}}\hat{U}^{12}_{\text{CNOT}}(a|0\rangle + b|1\rangle)\\ &= \hat{H}_1\hat{H}_2\hat{H}_3(a|000\rangle + b|111\rangle)\\ &= a|+++\rangle + b|---\rangle\end{aligned}$$

encoded initial state

$$|\psi_0'\rangle = a|+++\rangle + b|---\rangle$$

phase-flip error $|\psi_0'\rangle \rightarrow |\psi_1'\rangle$

$$|\psi_1'\rangle = a|++-\rangle + b|--+\rangle$$

or $a|+-+\rangle + b|-+-\rangle$

or $a|-++\rangle + b|+--\rangle$

or $a|+++\rangle + b|---\rangle$

apply Hadamard gates to $|\psi_1'\rangle \rightarrow |\psi_1\rangle$

$$|\psi_1\rangle = \hat{H}^{\otimes 3}|\psi_1'\rangle = \hat{H}_1\hat{H}_2\hat{H}_3(a|++-\rangle + b|--+\rangle) = a|001\rangle + b|110\rangle$$

and analogously

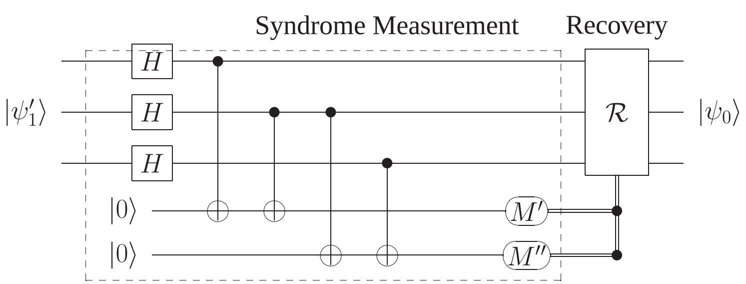
$$a|+-+\rangle + b|-+-\rangle \rightarrow a|010\rangle + b|101\rangle$$

$$a|-++\rangle + b|+--\rangle \rightarrow a|100\rangle + b|011\rangle$$

$$a|+++\rangle + b|---\rangle \rightarrow a|000\rangle + b|111\rangle$$

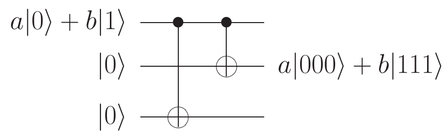
so now our standard bit-flip ECC can be applied

phase-flip error correction $|\psi_1'\rangle \rightarrow |\psi_0\rangle$

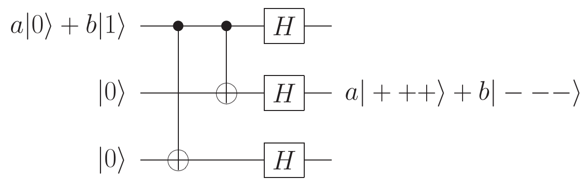


$$|\psi_0\rangle = \hat{X}_{|3M''-2M'|}\Big({}_{45}\langle M', M''|\hat{U}^{35}_{\mathrm{CNOT}}\hat{U}^{25}_{\mathrm{CNOT}}\hat{U}^{24}_{\mathrm{CNOT}}\hat{U}^{14}_{\mathrm{CNOT}}\hat{H}^{\otimes 3}|\psi_1\rangle|00\rangle\Big)$$

encoding qubit against bit-flip error

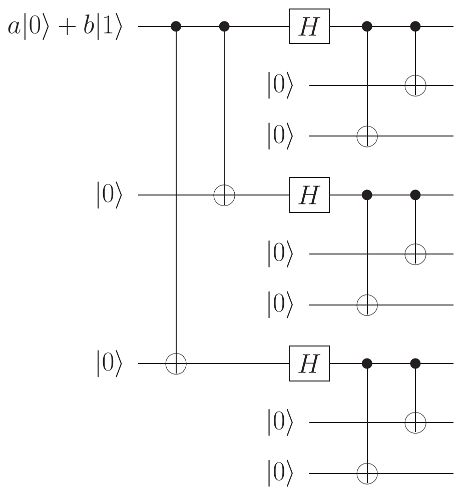


encoding qubit against phase-flip error



How to encode qubit against both errors?

encoding code for Shor's nine-qubit ECC



first real error correction code against both bit-flip and phase-flip **single** error

encoding code for Shor's nine-qubit ECC

$$
\begin{aligned}
|0\rangle \;&\rightarrow\; |000\rangle \\
&\rightarrow\; |+++\rangle = \frac{1}{2^{3/2}}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \\
&\rightarrow\; \frac{1}{2^{3/2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) \equiv |\mathbf{0}\rangle_{\mathrm{L}}
\end{aligned}
$$

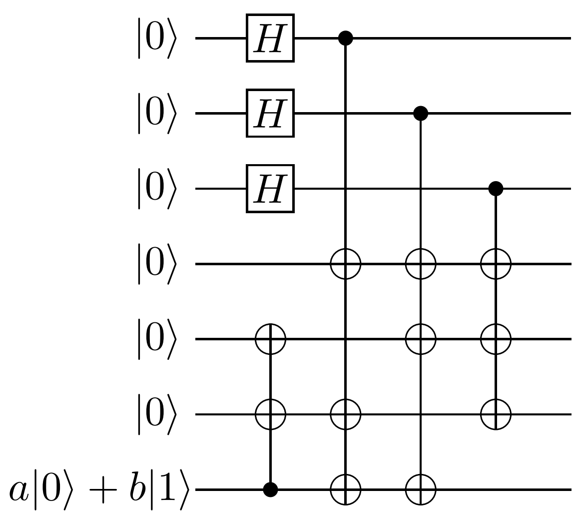
$$
\begin{aligned}
|1\rangle \;&\rightarrow\; |111\rangle \\
&\rightarrow\; |---\rangle = \frac{1}{2^{3/2}}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)(|0\rangle - |1\rangle) \\
&\rightarrow\; \frac{1}{2^{3/2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle) \equiv |\mathbf{1}\rangle_{\mathrm{L}}
\end{aligned}
$$

$$a|0\rangle + b|1\rangle \longrightarrow a|0\rangle_{\mathrm{L}} + b|1\rangle_{\mathrm{L}}$$

Note that:

- the corrections of bit and phase flip errors are independent
- thus Shor's code can correct combined bit and phase flips on a **single** qubit
- there are other more concise ECCs

encoding code for Steane's seven-qubit ECC



$$a|0\rangle_L + b|1\rangle_L$$

encoding code for Steane's seven-qubit ECC

let

$$|\psi\rangle = |0\rangle$$

$$|\psi_0\rangle \;=\; |0\rangle^{\otimes 6}|\psi\rangle$$

step 1:

$$|\psi_1\rangle = \hat{H}_1\hat{H}_2\hat{H}_3|0\rangle^{\otimes 6}|\psi_0\rangle = |+,+,+,0,0,0,0\rangle$$

step 2:

$$|\psi_2\rangle = \hat{U}^{76}_{CNOT}\hat{U}^{75}_{CNOT}|\psi_1\rangle = |\psi_1\rangle$$

step 3:

$$
\begin{aligned}
|\psi_3\rangle \;&=\; \hat{U}^{14}_{CNOT}\hat{U}^{16}_{CNOT}\hat{U}^{17}_{CNOT}|\psi_2\rangle \\
&=\; \frac{1}{\sqrt{2}}(|\underline{0},+,+,0,0,0,0\rangle + |\underline{1},+,+,0\oplus 1,0,0\oplus 1,0\oplus 1\rangle) \\
&=\; \frac{1}{\sqrt{2}}(|0,+,+,0,0,0,0\rangle + |1,+,+,1,0,1,1\rangle)
\end{aligned}
$$

step 4:

$$
\begin{aligned}
|\psi_4\rangle \;&=\; \hat{U}^{24}_{CNOT}\hat{U}^{25}_{CNOT}\hat{U}^{27}_{CNOT}|\psi_3\rangle \\
&=\; \frac{1}{2}(|0,\underline{0},+,0,0,0,0\rangle + |0,\underline{1},+,0\oplus 1,0\oplus 1,0,0\oplus 1\rangle \\
&\quad +|1,\underline{0},+,1,0,1,1\rangle + |1,\underline{1},+,1\oplus 1,0\oplus 1,1,1\oplus 1\rangle) \\
&=\; \frac{1}{2}(|0,0,+,0,0,0,0\rangle + |0,1,+,\underline{1},\underline{1},0,\underline{1}\rangle \\
&\quad +|1,0,+,1,0,1,\underline{1}\rangle + |1,1,+,\underline{0},\underline{1},1,\underline{0}\rangle)
\end{aligned}
$$

final step 5:

$$|\psi_5\rangle = \hat{U}^{34}_{CNOT}\hat{U}^{35}_{CNOT}\hat{U}^{36}_{CNOT}|\psi_4\rangle$$

$$
\begin{aligned}
=\; \frac{1}{\sqrt{8}}&(|0,0,\underline{0},0,0,0,0\rangle + |0,0,\underline{1},0\oplus 1,0\oplus 1,0\oplus 1,0\rangle \\
&+|0,1,\underline{0},1,1,0,1\rangle + |0,1,\underline{1},1\oplus 1,1\oplus 1,0\oplus 1,1\rangle \\
&+|1,0,\underline{0},1,0,1,1\rangle + |1,0,\underline{1},1\oplus 1,0\oplus 1,1\oplus 1,1\rangle \\
&+|1,1,\underline{0},0,1,1,0\rangle + |1,1,\underline{1},0\oplus 1,1\oplus 1,1\oplus 1,0\rangle)
\end{aligned}
$$

so finally

$$|\mathbf{0}\rangle_{\mathbf{L}} \equiv |\psi_5\rangle = \frac{1}{\sqrt{8}}(|0000000\rangle + |0011110\rangle + |0101101\rangle + |0110011\rangle + |1001011\rangle + |1010101\rangle + |1100110\rangle + |1111000\rangle) = \frac{1}{\sqrt{8}} \sum_{\text{even } \nu\in\text{Hamming}} |\nu\rangle$$

Analogously

$$|\psi\rangle = |1\rangle \rightarrow |\psi_5\rangle \equiv |1\rangle_L$$

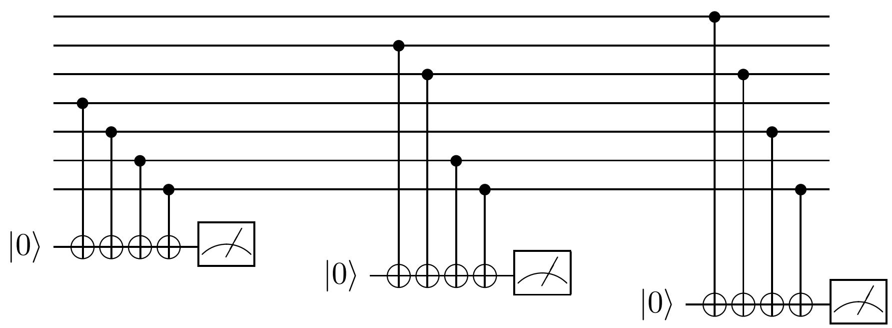
where

$$|\mathbf{1}\rangle_{\mathbf{L}} = \frac{1}{\sqrt{8}}(|1111111\rangle + |1110000\rangle + |1001100\rangle + |1000011\rangle + |0101010\rangle + |0100101\rangle + |0011001\rangle + |0010110\rangle) = \frac{1}{\sqrt{8}} \sum_{\text{odd } \nu\in\text{Hamming}} |\nu\rangle$$

Thus, in general

$$a|0\rangle + b|1\rangle \rightarrow a|0\rangle_L + b|1\rangle_L$$

bit-flip syndrome detection in Steane's 7-qubit ECC



phase-flip syndrome detection

- the same circuit but with extra Hadamard gates, as for Shor's code

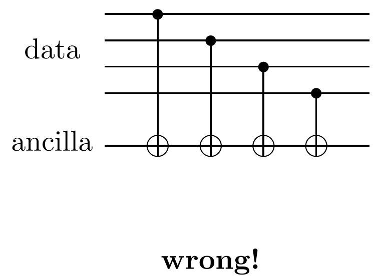
fault-tolerant syndrome detection

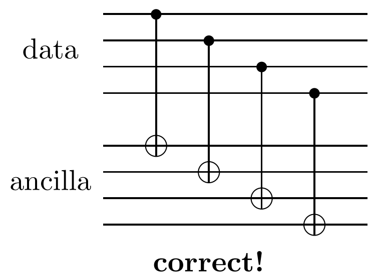
to make the circuit fault tolerant, each ancilla qubit must be replaced by four qubits in a suitable state.

fault-tolerant device

- a device that works effectively even when its elementary components are imperfect.

fault-intolerant and fault-tolerant circuits





most general single-qubit error

the most general single-qubit unitary error transformation (apart from irrelevant global phase factor) can be expanded to order ϵ as

$$\hat{U}_{\text{error}} = \epsilon_i \hat{I} + \hat{\mathcal{O}}(\epsilon) = \epsilon_i \hat{I} + \epsilon_x \hat{\sigma}_x + \epsilon_y \hat{\sigma}_y + \epsilon_z \hat{\sigma}_z$$

discrete set of quantum errors

fundamental result of quantum error correction theory:

correcting just a discrete set of errors
(bit flip, phase flip and combined bit-phase flip)
a quantum error-correcting codes can correct a continuous set of errors.

Shor's and Steane's ECCs

- they protect not only against bit and phase flip errors but against arbitrary errors affecting only a single qubit
- by measuring the error syndrome, the state collapses into one of the four states

$\hat{\sigma}_x|\psi\rangle$, $\hat{\sigma}_y|\psi\rangle$, $\hat{\sigma}_z|\psi\rangle$, $|\psi\rangle$

which are correctable with the codes.

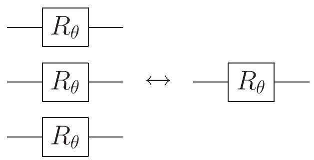
fault-tolerant memory

so far we have analyzed coding for
fault-tolerant storing of quantum information, but we also need:

fault-tolerant gates

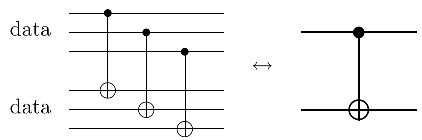
1. fault-tolerant single qubit-gates

can be applied bitwise with majority vote



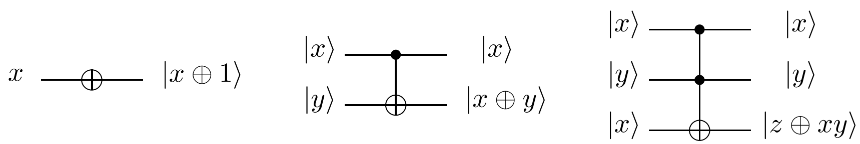
2. fault-tolerant CNOT (XOR) = transversal CNOT

can also be applied bitwise with majority vote



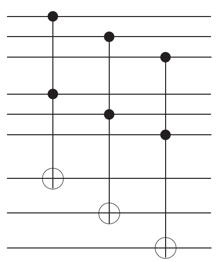
3. fault-tolerant Toffoli gate

Toffoli gate = controlled-controlled-NOT (CCNOT)

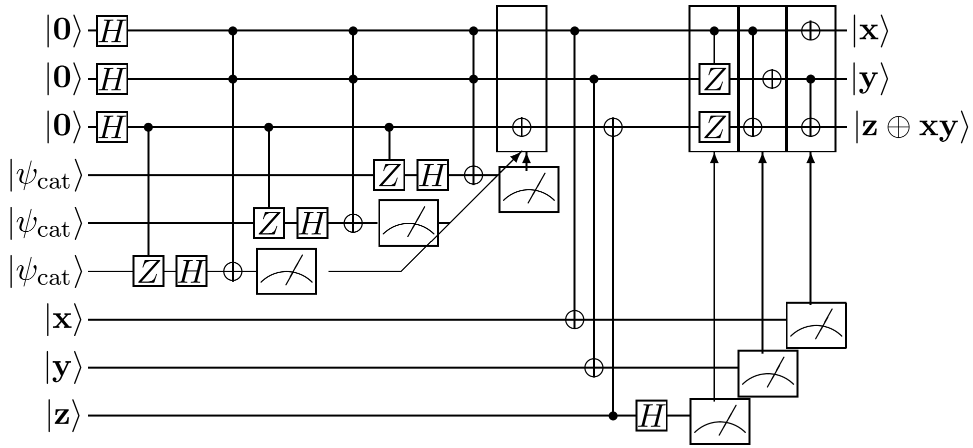


NOT CNOT Toffoli gate

naive solution but not fault-tolerant



Shor's construction of fault-tolerant Toffoli gate



- each line represents a block of 7 qubits!
- $|\boldsymbol{\psi}_{\rm cat}\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes 7} + |1\rangle^{\otimes 7})$, $|\mathbf{0}\rangle = |0\rangle^{\otimes 7}$, $|\mathbf{1}\rangle = |1\rangle^{\otimes 7}$, $|\mathbf{x}\rangle = |x\rangle^{\otimes 7}$, etc.
- gates are implemented transversally
- if a given measurement outcome is 1, the arrow points to the set of gates to be applied; no action is taken if the outcome is 0.

Error correction codes
(part II)

perfect ECC with the smallest number of ancillas

requirements for scalable QIP

error-threshold theorem

Note: for convenience we neglect normalizations

Hilbert space for ECC

subspaces corresponding to different errors should be orthogonal

thus the total Hilbert space for ECC should be large enough to contain all the orthogonal subspaces.

number of subspaces is $2(3n+1)$

Orthogonality requires a subspace for each of the three errors every qubit can suffer and another one for the unperturbed logical state.

We must double this to have enough space to accommodate both logical states and their erroneous descendants.

minimum number of encoded qubits is $n=5$ for ECC

$$2(3n+1) \le 2^n \quad \Rightarrow \quad 26 \not\le 16 \text{ for } n=4 \quad \& \quad 32 \le 32 \text{ for } n=5$$

number of encoded qubits for ECC

$n=9$ – Shor ECC

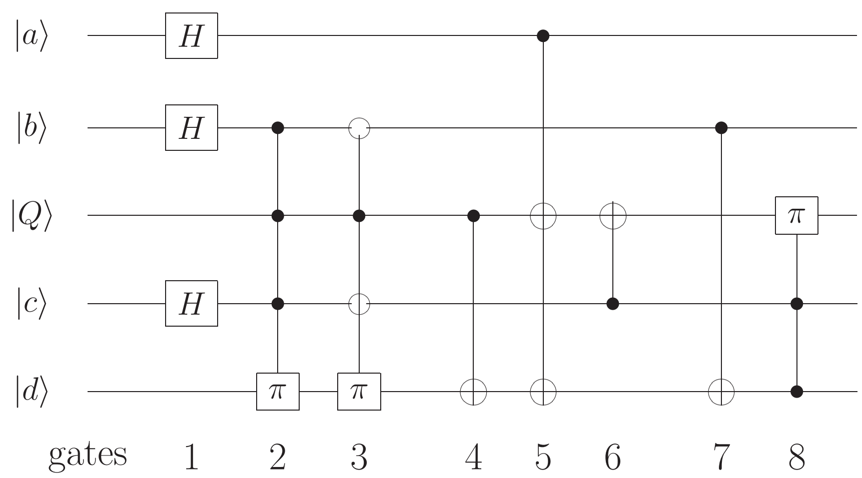
$n=7$ – Steane ECC

$n=5$ – Los Alamos ECC $\quad \Rightarrow \quad$ it requires the minimum number of ancillas

Los Alamos ECC

[Laflamme, Miquel, Paz, Zurek (1996)]

1. 5-bit encoder



encoded qubits

$$|0\rangle_L = \quad |B_1\rangle|00\rangle - |B_3\rangle|11\rangle + |B_5\rangle|01\rangle + |B_7\rangle|10\rangle$$
$$|1\rangle_L = -|B_2\rangle|11\rangle - |B_4\rangle|00\rangle - |B_6\rangle|10\rangle + |B_8\rangle|01\rangle$$

in terms of the (unnormalized) 3-qubit Bell states:

$$|B_{\substack{1\\2}}\rangle = |000\rangle \pm |111\rangle$$
$$|B_{\substack{3\\4}}\rangle = |100\rangle \pm |011\rangle$$
$$|B_{\substack{5\\6}}\rangle = |010\rangle \pm |101\rangle$$
$$|B_{\substack{7\\8}}\rangle = |110\rangle \pm |001\rangle$$

Other allowed encodings can be found from those by permutations of bits and coordinated signs.

Thus, all the allowed encodings have the same sign pattern: with two minus signs in one of the logical states and four in the other.

encoded qubits explicitly

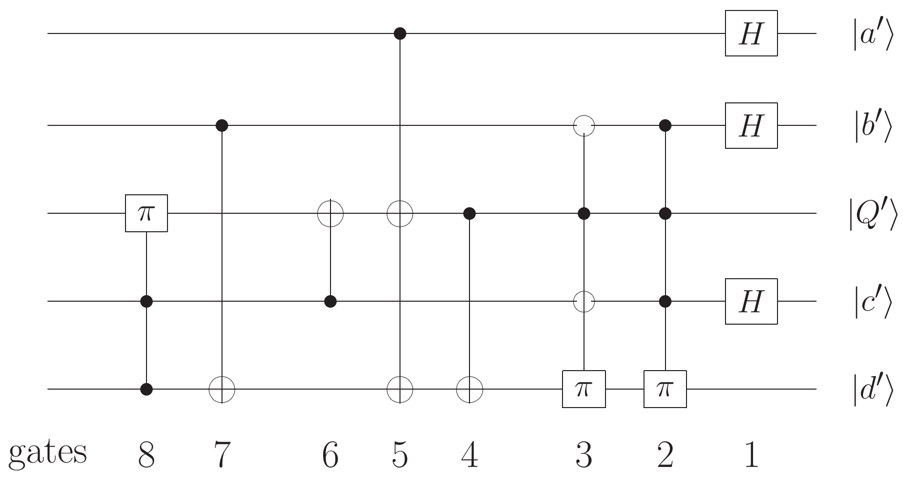
$$\begin{aligned}
|0\rangle_L &= |B_1\rangle|00\rangle - |B_3\rangle|11\rangle + |B_5\rangle|01\rangle + |B_7\rangle|10\rangle \\
&= (|000\rangle + |111\rangle)|00\rangle - (|100\rangle + |011\rangle)|11\rangle \\
&\quad +(|010\rangle + |101\rangle)|01\rangle + (|110\rangle + |001\rangle)|10\rangle \\
&= |00000\rangle + |11100\rangle - |10011\rangle - |01111\rangle \\
&\quad +|01001\rangle + |10101\rangle + |11010\rangle + |00110\rangle \\
&\quad \text{(lexicographic order)} \\
&= |00000\rangle + |00110\rangle + |01001\rangle - |01111\rangle \\
&\quad -|10011\rangle + |10101\rangle + |11010\rangle + |11100\rangle
\end{aligned}$$

$$\begin{aligned}
|1\rangle_L &= -|B_2\rangle|11\rangle - |B_4\rangle|00\rangle - |B_6\rangle|10\rangle + |B_8\rangle|01\rangle \\
&= -(|000\rangle - |111\rangle)|00\rangle - (|100\rangle - |011\rangle)|11\rangle \\
&\quad -(|010\rangle - |101\rangle)|01\rangle + (|110\rangle - |001\rangle)|10\rangle \\
&= -|00011\rangle + |11111\rangle - |10000\rangle + |01100\rangle \\
&\quad -|01010\rangle + |10110\rangle + |11001\rangle - |00101\rangle \\
&\quad \text{(lexicographic order)} \\
&= -|00011\rangle - |00101\rangle - |01010\rangle + |01100\rangle \\
&\quad -|10000\rangle + |10110\rangle + |11001\rangle + |11111\rangle
\end{aligned}$$

Los Alamos ECC

2. decoder

(reverse of the encoder)



errors and their syndromes

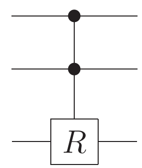
error	syndrome $\|a'b'c'd'\rangle$	resulting state $\|Q'\rangle$
none	0000	$a\|0\rangle + b\|1\rangle$
X_3Z_3	1101	$-a\|1\rangle + b\|0\rangle$
X_5Z_5	1111	$-a\|0\rangle + b\|1\rangle$
X_2	0001	$a\|0\rangle - b\|1\rangle$
Z_3	1010	
Z_5	1100	
X_2Z_2	0101	
X_5	0011	$-a\|0\rangle - b\|1\rangle$
Z_1	1000	
Z_2	0100	
Z_4	0010	
X_1	0110	$-a\|1\rangle - b\|0\rangle$
X_3	0111	
X_4	1011	
X_1Z_1	1110	
X_4Z_4	1001	

input state $|Q\rangle = a|0\rangle + b|1\rangle$, X_i – bit flip error, Z_i – phase flip error

Matlab program for Los Alamos ECC

```
I=eye(2);      % identity operator
H=[1 1;1 -1]; % Hadamard gate - for simplicity we neglect 1/sqrt(2)
R=-I;          % pi-rotation

CNOT=[
     1     0     0     0
     0     1     0     0
     0     0     0     1
     0     0     1     0
     ];

CCNOT=[
     1     0     0     0     0     0     0     0
     0     1     0     0     0     0     0     0
     0     0     1     0     0     0     0     0
     0     0     0     1     0     0     0     0
     0     0     0     0     1     0     0     0
     0     0     0     0     0     1     0     0
     0     0     0     0     0     0     0     1
     0     0     0     0     0     0     1     0
     ];
```


double-controlled rotation: CCR

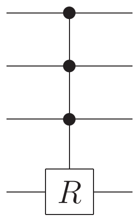


$$\hat{R} = \begin{bmatrix} R_{11} & R_{12} \\ R_{21} & R_{22} \end{bmatrix}$$

$$CCR = \hat{I} + |110\rangle\langle 110|(R_{11}-1) + |110\rangle\langle 111|R_{12} + |111\rangle\langle 110|R_{21} + |111\rangle\langle 111|(R_{22}-1)$$

```
CCR= [ 1      0      0      0      0      0      0       0
       0      1      0      0      0      0      0       0
       0      0      1      0      0      0      0       0
       0      0      0      1      0      0      0       0
       0      0      0      0      1      0      0       0
       0      0      0      0      0      1      0       0
       0      0      0      0      0      0      R(1,1) R(1,2)
       0      0      0      0      0      0      R(2,1) R(2,2)];
```

triple-controlled rotation: CCCR



$$\hat{R} = \begin{bmatrix} R_{11} & R_{12} \\ R_{21} & R_{22} \end{bmatrix}$$

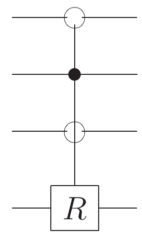
$$CCCR = \hat{I} + |1110\rangle\langle 1110|(R_{11}-1) + |1110\rangle\langle 1111|R_{12} + |1111\rangle\langle 1110|R_{21} + |1111\rangle\langle 1111|(R_{22}-1)$$

```
CCCR=eye(16)+...
  ket([1 1 1 0])*bra([1 1 1 0])*(R(1,1)-1)+...
  ket([1 1 1 0])*bra([1 1 1 1])*R(1,2)    +...
  ket([1 1 1 1])*bra([1 1 1 0])*R(2,1)    +...
  ket([1 1 1 1])*bra([1 1 1 1])*(R(2,2)-1);
```


CCCR gate explicitly

```
CCCR= [
   1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
   0  1  0  0  0  0  0  0  0  0  0  0  0  0  0  0
   0  0  1  0  0  0  0  0  0  0  0  0  0  0  0  0
   0  0  0  1  0  0  0  0  0  0  0  0  0  0  0  0
   0  0  0  0  1  0  0  0  0  0  0  0  0  0  0  0
   0  0  0  0  0  1  0  0  0  0  0  0  0  0  0  0
   0  0  0  0  0  0  1  0  0  0  0  0  0  0  0  0
   0  0  0  0  0  0  0  1  0  0  0  0  0  0  0  0
   0  0  0  0  0  0  0  0  1  0  0  0  0  0  0  0
   0  0  0  0  0  0  0  0  0  1  0  0  0  0  0  0
   0  0  0  0  0  0  0  0  0  0  1  0  0  0  0  0
   0  0  0  0  0  0  0  0  0  0  0  1  0  0  0  0
   0  0  0  0  0  0  0  0  0  0  0  0  1  0  0  0
   0  0  0  0  0  0  0  0  0  0  0  0  0  1  0  0
   0  0  0  0  0  0  0  0  0  0  0  0  0  0  R(1,1) R(1,2)
   0  0  0  0  0  0  0  0  0  0  0  0  0  0  R(2,1) R(2,2)];
```


another triple-controlled rotation: cCcR



$$\hat{R} = \begin{bmatrix} R_{11} & R_{12} \\ R_{21} & R_{22} \end{bmatrix}$$

$$cCcR = \hat{I} + |0100\rangle\langle 0100|(R_{11}-1) + |0100\rangle\langle 0101|R_{12} + |0101\rangle\langle 0100|R_{21} + |0101\rangle\langle 0101|(R_{22}-1)$$

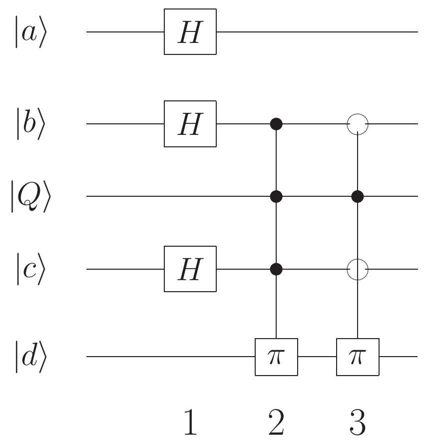
```
cCcR=eye(16)+...
  ket([0 1 0 0])*bra([0 1 0 0])*(R(1,1)-1)+...
  ket([0 1 0 0])*bra([0 1 0 1])*R(1,2)    +...
  ket([0 1 0 1])*bra([0 1 0 0])*R(2,1)    +...
  ket([0 1 0 1])*bra([0 1 0 1])*(R(2,2)-1);
```


cCcR gate explicitly

```
cCcR= [
   1  0  0  0  0      0      0  0  0  0  0  0  0  0  0  0
   0  1  0  0  0      0      0  0  0  0  0  0  0  0  0  0
   0  0  1  0  0      0      0  0  0  0  0  0  0  0  0  0
   0  0  0  1  0      0      0  0  0  0  0  0  0  0  0  0
   0  0  0  0  R(1,1) R(1,2) 0  0  0  0  0  0  0  0  0  0
   0  0  0  0  R(2,1) R(2,2) 0  0  0  0  0  0  0  0  0  0
   0  0  0  0  0      0      1  0  0  0  0  0  0  0  0  0
   0  0  0  0  0      0      0  1  0  0  0  0  0  0  0  0
   0  0  0  0  0      0      0  0  1  0  0  0  0  0  0  0
   0  0  0  0  0      0      0  0  0  1  0  0  0  0  0  0
   0  0  0  0  0      0      0  0  0  0  1  0  0  0  0  0
   0  0  0  0  0      0      0  0  0  0  0  1  0  0  0  0
   0  0  0  0  0      0      0  0  0  0  0  0  1  0  0  0
   0  0  0  0  0      0      0  0  0  0  0  0  0  1  0  0
   0  0  0  0  0      0      0  0  0  0  0  0  0  0  0  0
   0  0  0  0  0      0      0  0  0  0  0  0  0  0  0  0];
```

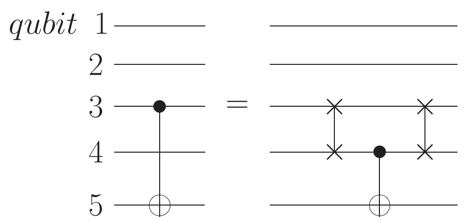
Los Alamos encoding circuit in *Matlab*

- **gates 1, 2, 3**




```
gate1=tensor_product(H,H,I,H,I);
gate2=tensor_product(I,CCCR);
gate3=tensor_product(I,cCcR);
```

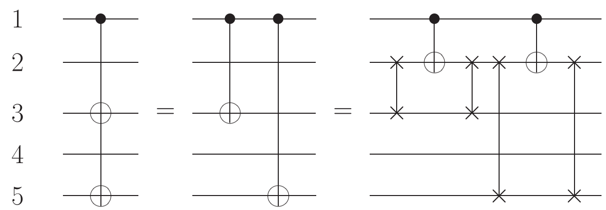

- **gate 4**




```
SWAP=[
        1 0 0 0
        0 0 1 0
        0 1 0 0
        0 0 0 1
     ];
```

```
SWAP34=tensor_product(I,I,SWAP,I);
CNOT45=tensor_product(I,I,I,CNOT);
gate4=SWAP34*CNOT45*SWAP34;
```


- **gate 5**

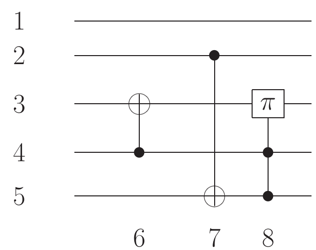



```
CNOT12=tensor_product(CNOT,I,I,I);
SWAP23=tensor_product(I,SWAP,I,I);
SWAP34=tensor_product(I,I,SWAP,I);
SWAP45=tensor_product(I,I,I,SWAP);
SWAP25=SWAP23*SWAP34*SWAP45*SWAP34*SWAP23;

gate5=SWAP23*CNOT12*SWAP23*SWAP25*CNOT12*SWAP25;
```

Alternatively, by defining a function `swap_qubits(`$\hat{U}, n_1, n_2$`)`, which temporarily swaps n_1th and n_2th qubits in a matrix $\hat{U}$, we can simply write

```
CNOT45=tensor_product(I,I,I,CNOT);
gate5 =swap_qubits(swap_qubits(CNOT45,5,3),4,1)*...
       swap_qubits(CNOT45,4,1);
```


- **gates 6,7,8**




```
gate6=swap_qubits(CNOT45,5,3);
gate7=swap_qubits(CNOT45,4,2);

gate=tensor_product(I,I,CCR);
gate8=swap_qubits(gate,5,3);
```

thus the encoding and decoding circuits are described by the operators

```
U_encoder=gate8*gate7*gate6*gate5*gate4*gate3*gate2*gate1;
U_decoder=gate1*gate2*gate3*gate4*gate5*gate6*gate7*gate8;
```

$$\hat{U}_{\text{decoder}} = \hat{U}^{\dagger}_{\text{encoder}}$$

```
          1 0 1 0 0 0 0 0 1 0 1 0 0 0 0 0 1 0 1 0 0 0 0 0 1 0 1 0 0 0 0 0
          0 1 0 1 0 0 0 0 0 1 0 1 0 0 0 0 0 1 0 1 0 0 0 0 0 1 0 1 0 0 0 0
          0 0 0 0 0 1 0 z 0 0 0 0 0 1 0 z 0 0 0 0 0 1 0 z 0 0 0 0 0 1 0 z
          0 0 0 0 z 0 1 0 0 0 0 0 z 0 1 0 0 0 0 0 z 0 1 0 0 0 0 0 z 0 1 0
          0 0 0 0 0 z 0 z 0 0 0 0 0 z 0 z 0 0 0 0 0 z 0 z 0 0 0 0 0 z 0 z
          0 0 0 0 z 0 z 0 0 0 0 0 z 0 z 0 0 0 0 0 z 0 z 0 0 0 0 0 z 0 z 0
          1 0 z 0 0 0 0 0 1 0 z 0 0 0 0 0 1 0 z 0 0 0 0 0 1 0 z 0 0 0 0 0
          0 z 0 1 0 0 0 0 0 z 0 1 0 0 0 0 0 z 0 1 0 0 0 0 0 z 0 1 0 0 0 0
          0 1 0 1 0 0 0 0 0 z 0 z 0 0 0 0 0 1 0 1 0 0 0 0 0 z 0 z 0 0 0 0
          1 0 1 0 0 0 0 0 z 0 z 0 0 0 0 0 1 0 1 0 0 0 0 0 z 0 z 0 0 0 0 0
          0 0 0 0 z 0 1 0 0 0 0 0 1 0 z 0 0 0 0 0 z 0 1 0 0 0 0 0 1 0 z 0
          0 0 0 0 0 1 0 z 0 0 0 0 0 z 0 1 0 0 0 0 0 1 0 z 0 0 0 0 0 z 0 1
          0 0 0 0 1 0 1 0 0 0 0 0 z 0 z 0 0 0 0 0 1 0 1 0 0 0 0 0 z 0 z 0
          0 0 0 0 0 1 0 1 0 0 0 0 0 z 0 z 0 0 0 0 0 1 0 1 0 0 0 0 0 z 0 z
          0 1 0 z 0 0 0 0 0 z 0 1 0 0 0 0 0 1 0 z 0 0 0 0 0 z 0 1 0 0 0 0
U_encoder= z 0 1 0 0 0 0 0 1 0 z 0 0 0 0 0 z 0 1 0 0 0 0 0 1 0 z 0 0 0 0 0
          0 0 0 0 z 0 z 0 0 0 0 0 z 0 z 0 0 0 0 0 1 0 1 0 0 0 0 0 1 0 1 0
          0 0 0 0 0 z 0 z 0 0 0 0 0 z 0 z 0 0 0 0 0 1 0 1 0 0 0 0 0 1 0 1
          0 1 0 z 0 0 0 0 0 1 0 z 0 0 0 0 0 z 0 1 0 0 0 0 0 z 0 1 0 0 0 0
          z 0 1 0 0 0 0 0 z 0 1 0 0 0 0 0 1 0 z 0 0 0 0 0 1 0 z 0 0 0 0 0
          0 1 0 1 0 0 0 0 0 1 0 1 0 0 0 0 0 z 0 z 0 0 0 0 0 z 0 z 0 0 0 0
          1 0 1 0 0 0 0 0 1 0 1 0 0 0 0 0 z 0 z 0 0 0 0 0 z 0 z 0 0 0 0 0
          0 0 0 0 1 0 z 0 0 0 0 0 1 0 z 0 0 0 0 0 z 0 1 0 0 0 0 0 z 0 1 0
          0 0 0 0 0 z 0 1 0 0 0 0 0 z 0 1 0 0 0 0 0 1 0 z 0 0 0 0 0 1 0 z
          0 0 0 0 0 1 0 1 0 0 0 0 0 z 0 z 0 0 0 0 0 z 0 z 0 0 0 0 0 1 0 1
          0 0 0 0 1 0 1 0 0 0 0 0 z 0 z 0 0 0 0 0 z 0 z 0 0 0 0 0 1 0 1 0
          1 0 z 0 0 0 0 0 z 0 1 0 0 0 0 0 z 0 1 0 0 0 0 0 1 0 z 0 0 0 0 0
          0 z 0 1 0 0 0 0 0 1 0 z 0 0 0 0 0 1 0 z 0 0 0 0 0 z 0 1 0 0 0 0
          1 0 1 0 0 0 0 0 z 0 z 0 0 0 0 0 z 0 z 0 0 0 0 0 1 0 1 0 0 0 0 0
          0 1 0 1 0 0 0 0 0 z 0 z 0 0 0 0 0 z 0 z 0 0 0 0 0 1 0 1 0 0 0 0
          0 0 0 0 0 z 0 1 0 0 0 0 0 1 0 z 0 0 0 0 0 1 0 z 0 0 0 0 0 z 0 1
          0 0 0 0 1 0 z 0 0 0 0 0 z 0 1 0 0 0 0 0 z 0 1 0 0 0 0 0 1 0 z 0
```

$(z = -1)$

input state to encoder

$|\psi_{\rm in}\rangle = a|00000\rangle + b|00100\rangle$

```
psi_in=a*ket([0 0 0 0 0])+b*ket([0 0 1 0 0])
```

or explicitly

```
psi_in'
ans = [a000b000000000000000000000000000];
```

output state

$|\psi_{\rm out}\rangle = \hat{U}_{\rm encoder}|\psi_{\rm in}\rangle$

```
psi_out=U_encoder*psi_in
```

1. encoding qubit $|0\rangle_L$

special case: $a = 1, b = 0$

```
psi_out'
ans =[100000100100000z000z010000101000]
```

```
show_state(psi_out,'|0>_L = ')
ans =|0>_L = +|00000>+|00110>+|01001>-|01111>...
             -|10011>+|10101>+|11010>+|11100>
```



```
          1 0 0 0 0 0 1 0 0 1 0 0 0 0 0 z 0 0 0 z 0 1 0 0 0 0 1 0 1 0 0 0
          0 1 0 0 0 0 0 z 1 0 0 0 0 0 1 0 0 0 1 0 1 0 0 0 0 0 0 z 0 1 0 0
          1 0 0 0 0 0 z 0 0 1 0 0 0 0 0 1 0 0 0 1 0 1 0 0 0 0 z 0 1 0 0 0
          0 1 0 0 0 0 0 1 1 0 0 0 0 0 z 0 0 0 z 0 1 0 0 0 0 0 0 1 0 1 0 0
          0 0 0 z 0 z 0 0 0 0 z 0 1 0 0 0 z 0 0 0 0 0 1 0 0 1 0 0 0 0 0 1
          0 0 1 0 z 0 0 0 0 0 0 1 0 1 0 0 0 z 0 0 0 0 0 z 1 0 0 0 0 0 z 0
          0 0 0 1 0 z 0 0 0 0 1 0 1 0 0 0 z 0 0 0 0 0 z 0 0 1 0 0 0 0 0 z
          0 0 z 0 z 0 0 0 0 0 0 z 0 1 0 0 0 z 0 0 0 0 0 1 1 0 0 0 0 0 1 0
          1 0 0 0 0 0 1 0 0 z 0 0 0 0 0 1 0 0 0 z 0 1 0 0 0 0 z 0 z 0 0 0
          0 1 0 0 0 0 0 z z 0 0 0 0 0 z 0 0 0 1 0 1 0 0 0 0 0 0 1 0 z 0 0
          1 0 0 0 0 0 z 0 0 z 0 0 0 0 0 z 0 0 0 1 0 1 0 0 0 0 1 0 z 0 0 0
          0 1 0 0 0 0 0 1 z 0 0 0 0 0 1 0 0 0 z 0 1 0 0 0 0 0 0 z 0 z 0 0
          0 0 0 z 0 z 0 0 0 0 1 0 z 0 0 0 z 0 0 0 0 0 1 0 0 z 0 0 0 0 0 z
          0 0 1 0 z 0 0 0 0 0 0 z 0 z 0 0 0 z 0 0 0 0 0 z z 0 0 0 0 0 1 0
          0 0 0 1 0 z 0 0 0 0 z 0 z 0 0 0 z 0 0 0 0 0 z 0 0 z 0 0 0 0 0 1
U_decoder= 0 0 z 0 z 0 0 0 0 0 0 1 0 z 0 0 0 z 0 0 0 0 0 1 z 0 0 0 0 0 z 0
          1 0 0 0 0 0 1 0 0 1 0 0 0 0 0 z 0 0 0 1 0 z 0 0 0 0 z 0 z 0 0 0
          0 1 0 0 0 0 0 z 1 0 0 0 0 0 1 0 0 0 z 0 z 0 0 0 0 0 0 1 0 z 0 0
          1 0 0 0 0 0 z 0 0 1 0 0 0 0 0 1 0 0 0 z 0 z 0 0 0 0 1 0 z 0 0 0
          0 1 0 0 0 0 0 1 1 0 0 0 0 0 z 0 0 0 1 0 z 0 0 0 0 0 0 z 0 z 0 0
          0 0 0 z 0 z 0 0 0 0 z 0 1 0 0 0 1 0 0 0 0 0 z 0 0 z 0 0 0 0 0 z
          0 0 1 0 z 0 0 0 0 0 0 1 0 1 0 0 0 1 0 0 0 0 0 1 z 0 0 0 0 0 1 0
          0 0 0 1 0 z 0 0 0 0 1 0 1 0 0 0 1 0 0 0 0 0 1 0 0 z 0 0 0 0 0 1
          0 0 z 0 z 0 0 0 0 0 0 z 0 1 0 0 0 1 0 0 0 0 0 z z 0 0 0 0 0 z 0
          1 0 0 0 0 0 1 0 0 z 0 0 0 0 0 1 0 0 0 1 0 z 0 0 0 0 1 0 1 0 0 0
          0 1 0 0 0 0 0 z z 0 0 0 0 0 z 0 0 0 z 0 z 0 0 0 0 0 0 z 0 1 0 0
          1 0 0 0 0 0 z 0 0 z 0 0 0 0 0 z 0 0 0 z 0 z 0 0 0 0 z 0 1 0 0 0
          0 1 0 0 0 0 0 1 z 0 0 0 0 0 1 0 0 0 1 0 z 0 0 0 0 0 0 1 0 1 0 0
          0 0 0 z 0 z 0 0 0 0 1 0 z 0 0 0 1 0 0 0 0 0 z 0 0 1 0 0 0 0 0 1
          0 0 1 0 z 0 0 0 0 0 0 z 0 z 0 0 0 1 0 0 0 0 0 1 1 0 0 0 0 0 z 0
          0 0 0 1 0 z 0 0 0 0 z 0 z 0 0 0 1 0 0 0 0 0 1 0 0 1 0 0 0 0 0 z
          0 0 z 0 z 0 0 0 0 0 0 1 0 z 0 0 0 1 0 0 0 0 0 z 1 0 0 0 0 0 1 0
```

$(z = -1)$

2. encoding qubit $|1\rangle_L$

input state to encoder: $|\psi_{\rm in}\rangle = |1\rangle$

special case for $a = 0, b = 1$

```
psi_in'
ans = [00001000000000000000000000000000];
```

output state $|\psi_{\rm out}\rangle = |1\rangle_L$

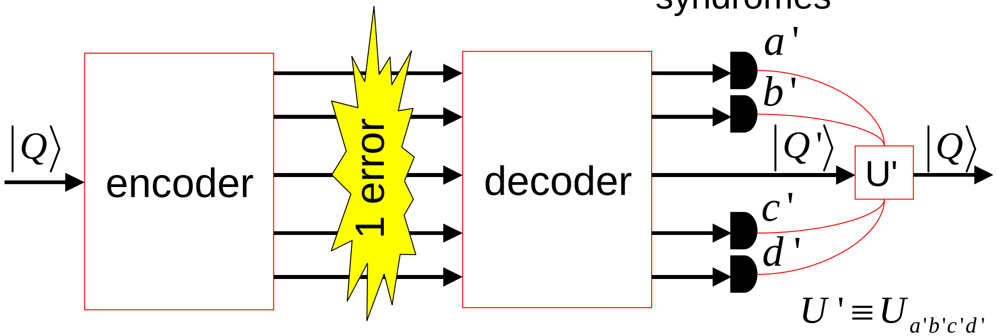
```
psi_out'
ans = [000z0z0000z01000z000001001000001]
```

or explicitly

```
show_state(psi_out,'|1>_L = ')
ans = |1>_L = -|00011>-|00101>-|01010>+|01100>...
              -|10000>+|10110>+|11001>+|11111>
```

thus we have got $|0\rangle_L$ and $|1\rangle_L$ in agreement with our definition

basic elements of the perfect ECC



Errors and their syndromes

example 1: bit flip of the 1st qubit

error

$$\hat{U}_{\text{error}} = \hat{\sigma}_x \otimes \hat{I} \otimes \hat{I} \otimes \hat{I} \otimes \hat{I}$$

```
sigma_x=[0,1;1,0];
U_error=tensor_product(sigma_x,I,I,I,I);
```

input state to encoder

$$|\psi_{\text{in}}\rangle = |abQcd\rangle = |00Q00\rangle$$

syndrome

$$|a'b'c'd'\rangle = |0110\rangle \quad \Rightarrow \quad |\psi_{\text{syndrome}}\rangle = |a'b'Q'c'd'\rangle = |01Q'10\rangle$$

transition amplitude

$$A_{Q\to Q'} = \langle\psi_{\text{syndrome}}|\hat{U}_{\text{decoder}}\hat{U}_{\text{error}}\hat{U}_{\text{encoder}}|\psi_{\text{in}}\rangle$$

```
psi_in       = ket([0 0 Q       0 0]);
psi_syndrome = ket([0 1 Q_prime 1 0]);
amplitude=psi_syndrome'*U_decoder*U_error*U_encoder*psi_in
```


transition amplitudes $|Q\rangle \longrightarrow |Q'\rangle$

$$A_{Q\to Q'}$$

$$A_{0\to 0} = 0, \quad A_{0\to 1} = -1 \quad \Rightarrow \quad |0\rangle \to -|1\rangle$$

$$A_{1\to 0} = -1, \quad A_{1\to 1} = 0 \quad \Rightarrow \quad |1\rangle \to -|0\rangle$$

so

$$|Q\rangle = a|0\rangle + b|1\rangle \to |Q'\rangle = -b|0\rangle - a|1\rangle$$

How to correct it?

$$|Q'\rangle \to \boxed{\hat{R}(\pi)\hat{\sigma}_x} \to |Q\rangle$$

example 2: phase flip of the 3rd qubit

error

$$\hat{U}_{\text{error}} = \hat{I} \otimes \hat{I} \otimes \hat{\sigma}_z \otimes \hat{I} \otimes \hat{I}$$

```
sigma_z=[1,0;0,-1]
U_error=tensor_product(I,I,sigma_z,I,I);
```

syndrome

```
psi_syndrome=ket([1 0 Q_prime 1 0]);
```

transition amplitudes $|Q\rangle \longrightarrow |Q'\rangle$

$$A_{0\to 0} = 1, \quad A_{0\to 1} = 0 \quad \Rightarrow \quad |0\rangle \to |0\rangle$$

$$A_{1\to 0} = 0, \quad A_{1\to 1} = -1 \quad \Rightarrow \quad |1\rangle \to -|1\rangle$$

so

$$|Q\rangle = a|0\rangle + b|1\rangle \to |Q'\rangle = a|0\rangle - b|1\rangle$$

How to correct it?

$$|Q'\rangle \to \boxed{\hat{\sigma}_z} \to |Q\rangle$$

Requirements for scalable QIP

[Knill, Laflamme, Zurek et al., 2002]

1. **Scalable physical systems:**

   the ability to support any number of independent qubits.

2. **State preparation:**

   the ability to prepare any qubit (or at least large fraction of them) in the standard initial state $|0\rangle$.

3. **Measurement:**

   the ability to measure any qubit (or at least large fraction of them) in the logical basis.

   Note: sometimes the **standard projective measurement** can be replaced by **weak measurements** that return a noisy number whose expectation is the probability that a qubit is in the state $|1\rangle$.

4. **Errors:**

   The error probability per gate must be below a **threshold** and satisfy **independence** and **locality** properties.

   • For the most **pessimistic** independent, local error models, the error threshold is above $\sim 10^{-6}$.

   For some **special error models**, the threshold is substantially higher.

   For example:

   • For the **independent depolarizing error model**, it is believed to be better than $\sim 10^{-4}$.

   • For the **independent 'erasure' error model**, where error events are always detected, the threshold is above .01.

   • The threshold is also above .01 when the goal is only to **transmit quantum information** through noisy quantum channels.

5. **Quantum control:**

   the ability to implement a **universal set** of unitary quantum gates acting on a small number (usually at most **two** at a time) of qubits.

   • For most accuracy thresholds, it is necessary to be able to apply the quantum control in parallel to any number of disjoint pairs of qubits. This **parallelism** requirement can be weakened if a nearly noiseless quantum **memory** is available.

   • The **universality** assumption can be substantially weakened by replacing some or all unitary quantum gates with operations to prepare special states or by having additional measurement capabilities.

accuracy-threshold theorem

Assuming the above requirements for scalable QIP:

> If the error per gate is less than a **threshold**,
> then it is possible to efficiently quantum compute arbitrarily accurately.

This is one of the most important results in quantum ECC and fault-tolerant computation.

Introduction to quantum algorithms (part I)

quantum algorithms and classical cryptography

public key cryptography (PKC)

quantum algorithms and cryptography

1985 Deutsch (Deutsch-Jozsa / DJ) algorithm:
How to see both sides of a coin simultaneously?

1994 Shor algorithm for number factorization:
How to break cryptosystems of
RSA, Rabin, Williams, Blum-Goldwasser,…?

1994 Shor algorithm for finding discrete logarithms:
How to break ElGamal cryptosystem?

1997 Grover algorithm for searching databases:
How to search the keys more effectively?

symmetric algorithms

cleartext
↓
plaintext
↓ Encryption using key k
ciphertext ↓ key distribution
↓ Decryption using the same key k
plaintext
↓
cleartext

public-key cryptography (PKC)
= asymmetric cryptography
= non-secret encryption

invented by Ellis (1970, British CESG)

and independently by Diffie & Hellman (1976)

two keys in PKC

1. public, open key
2. private, confidential key

- without additional information, it is not always possible to decrypt by repeating encryption operations in reverse order

f(in) = out, but f^{-1}(out) = ?

example

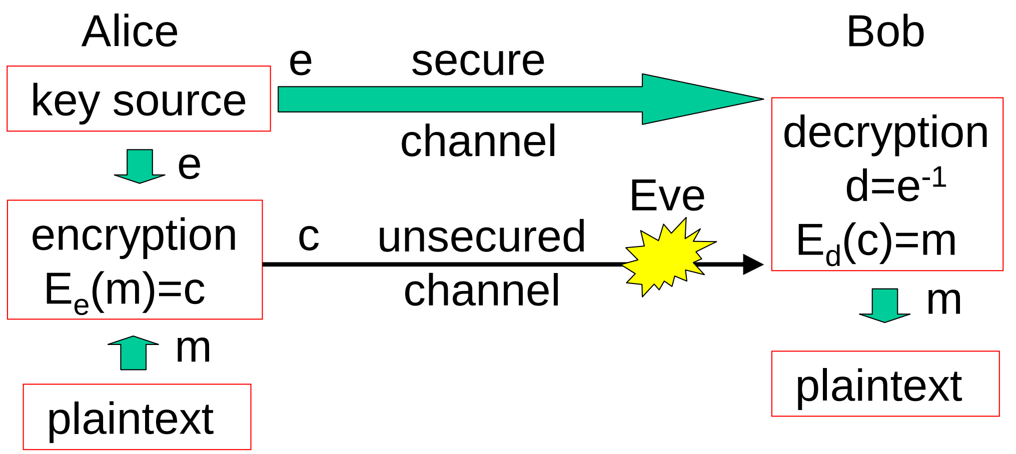
y = 17 mod 3 => y = 2 (unique result)

x mod 3 = 2 => x = 2, 5, 8, 11 ,14 , **17**, 20, ... (not unique result)

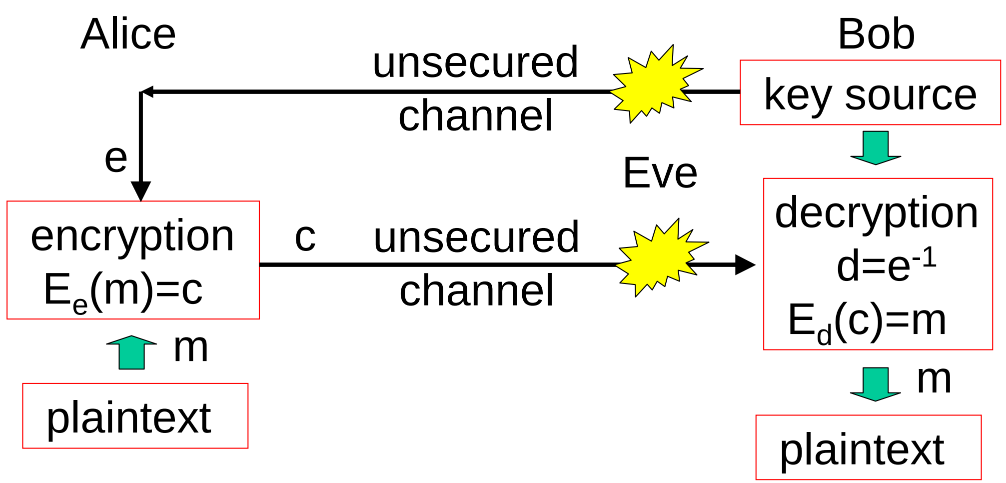
asymmetric algorithms
= public-key algorithms

cleartext
↓
plaintext
↓ Encryption using key k_1 (public key)
ciphertext
↓ Decryption using key k_2 (private key)
plaintext
↓
cleartext

Encryption with a secure channel for key exchange



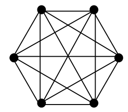
Encryption with a unsecured channel for key exchange



Why do we need PKC?
Number of keys

a problem of huge number of keys for symmetric algorithms.

- How many keys should be generated for N correspondents if everyone wants to communicate with all others using symmetric algorithms?



$$n_{\rm sym}(N) = \binom{N}{2} = \frac{N(N-1)}{2}$$

- How many keys are required for 6 or 1 milion correspondents?

$$n_{\rm sym}(6) = 15$$

$$n_{\rm sym}(10^6) \approx \frac{10^{12}}{2}$$

- How many keys are required asymmetric algorithms?

$$n_{\rm asym}(N) = 2N$$

popular public-key encryption schemes based on integer factorization problem

public-key encryption scheme	computational problem
RSA (Rivest-Shamir-Adleman & Cocks)	integer factorization problem
Rabin	integer factorization problem
Williams	integer factorization problem
Blum-Goldwasser probabilistic	integer factorization problem
Goldwasser-Micali probabilistic	quadratic residuosity problem or integer factorization problem
ElGamal	discrete logarithm problem or integer factorization problem
generalized ElGamal	generalized discrete logarithm problem or integer factorization problem

popular public-key encryption schemes
not based on integer factorization problem

public-key encryption scheme	computational problem
McEliece	linear code decoding problem or error-correction-code problem
Merkle-Hellman	knapsack subset sum problem *cracked by Shamir & Zippel!*
Graham-Shamir	knapsack subset sum problem *cracked!*
Lu-Lee	knapsack subset sum problem *cracked by Adleman & Rivest!*
Goodman-McAuley	knapsack subset sum problem *cracked!*
Powerline System (a simple version of Chor-Rivest)	knapsack subset sum problem *cracked by Lenstra!*
Chor-Rivest	knapsack subset sum problem *publicly not cracked!*

“easy” and “hard” computational problems

should be interpreted relative to a specified frame of reference.

easy = computationally feasible

- in polynomial time and space
- practically, within a certain number of machine operations or time units – perhaps seconds or milliseconds.

hard = computationally infeasible

- require super-polynomial time or space
- practically, exceeding the specified bound on the number of operations or memory corresponding to a specified security parameter

hard problems in PKC

by having only one key it is *practically* impossible to calculate the other key using *practically* available computers over *practically* long period of time.

Motivation for Shor’s Algorithm
– effectiveness of classical integer factorization methods

What is the time or number of bit operations required to factorize n?

1. **direct method**

$\sim \sqrt{n} = \exp(\frac{1}{2}\log n)$

2. **Monte Carlo method (Pollard method)**

$\sim n^{1/4}\log^3 n$

3,4. **Fermat method** and **quadratic sieve method**

$\sim \exp(c\sqrt{r\log r})$, where $r \sim \log n$ is the number of bits

thus

$\sim \exp(c\sqrt{\log n(\log\log n)})$

5. **number field sieve method**

$\sim \exp(c\sqrt[3]{\log n(\log\log n)^2})$

This is the fastest publicly available ;-) classical method for $r \geq 150$.

effectiveness of classical factorization methods

exponential in time, $\exp(\log \mathrm{n})$

effectiveness of quantum factorization methods

polynomial in time, $\mathrm{poly}(\log \mathrm{n})$

- original Shor algorithm

$\sim (\log n)^3$

- optimized Shor algorithm

$\sim (\log n)^2 \log\log n$

and $\log n$ steps of post processing on a classical computer.

our estimations

Thus, we estimate numbers of operations required to factorize n as:

$$N_{\mathrm{Shor}}(n) = c_1(\log n)^2\log(\log n) + c_2\log n$$
$$N_{\mathrm{clas}}(n) = c_3\exp[c(\log n)^{1/3}(\log\log n)^{2/3}]$$

with $c = 2$ in the fastest version of number field sieve method due to Lenstra

for simplicity, we choose: $c_3 = 1$

examples of factorization times

MIPS = millions of instructions per second

- 1-10 MIPS in a modest PC
- hundreds-thousands of MIPS in a supercomputer
- say, $N' = 10^6$ MIPS are available in contemporary computers

time required to factorize n

```
t(n)= N(n)  /N'  /60  /60    /24   /365
            sec  min  hours  days  years
```

examples

1. $n = 10^{130} \quad \Rightarrow \quad N_{\text{clas}} \sim 3.5 \cdot 10^{12}$ MIPS → 40.5 days ≈ 1 month
2. $n = 10^{150} \quad \Rightarrow \quad N_{\text{clas}} \sim 5.9 \cdot 10^{13}$ MIPS → 687.5 days ≈ 2 years
3. $n = 10^{300} \quad \Rightarrow \quad N_{\text{clas}} \sim 7.0 \cdot 10^{20}$ MIPS → 22.5 mln years

How old is the universe?

$T_{\text{universe}} \sim 1.25 \cdot 10^{10} = 12.5$ billion years

What is the largest factorizable integer within T_{universe}?

1. **direct method**

$N = 10^{60} \quad \Rightarrow \quad T \approx 3.17 \cdot 10^{10} > T_{\text{universe}}$

2. **Monte Carlo method (Pollard method)**

$N = 10^{91} \quad \Rightarrow \quad T \approx 1.6 \cdot 10^{10} > T_{\text{universe}}$

3,4. **Fermat method** and **quadratic sieve method**

$N = 10^{94} \quad \Rightarrow \quad T \approx 1.36 \cdot 10^{10} > T_{\text{universe}}$

5. **number field sieve method**

$N = 10^{400} \quad \Rightarrow \quad T \approx 8.1 \cdot 10^{10} > T_{\text{universe}}$

$N = 10^{375} \quad \Rightarrow \quad T \approx 1.18 \cdot 10^{10} < T_{\text{universe}}$

Introduction to quantum algorithms (part II)

classical RSA algorithm

quantum Deutsch algorithm

quantum Deutsch-Jozsa (DJ) algorithm

quantum Hadamard transform

quantum Fourier transform

Rivest-Shamir-Adleman (RSA) algorithm (1978)
I. generation of RSA keys (by Bob)

1. choose two large primes $p \neq q$
2. calculate

   $n = pq \quad$ and $\quad \phi = (p-1)(q-1)$
3. choose randomly an integer e $(1 < e < \phi)$ coprime to ϕ,

   i.e. their greatest common divisor is one, GCD$(e, \phi) = 1$.
4. using the extended Euclidean algorithm, calculate d $(1 < d < \phi)$ such that

   $ed \equiv 1 \bmod \phi$
5. thus

public key - (n, e)

private key - d

- **cryptographic terms:** n - modulus

  e – encryption exponent

  d – decryption exponent

II. RSA encryption (by Alice)

encrypt your message with the public key (n, e)

1. change cleartext into plaintext represented by an integer

$$m \in \langle 0, n-1 \rangle$$

2. calculate

$$c = m^e \bmod n$$

3. send a cipher c to Bob

III. RSA decryption (by Bob)

use your private key d to calculate

$$m = c^d \bmod n$$

A note

It has been revealed only very recently that the RSA algorithm has been devised already in 1973 by **Cocks** for the British security agency CESG.

extended Euclidean algorithm

GCD(a,b) = d =ax+by   x,y,d=?

```
initial  x1=y2=0;  x2=y1=1
while  b>0
        q = Int(a/b)
        r  = a - q b
        x1 = x2 -q x1 ;   x2 = x1
        y1 = y2 -q y1 ;   y2 = y1
        a = b
        b = r
return (d,x,y)=(a, x2, y2)
```

a,b,x,y,d - integers

how to calculate the greatest common divisor (GCD)? Euclidean algorithm

GCD(116,42) = ?

116 mod 42 = 32

42 mod 32 = 10

32 mod 10 = 2

10 mod 2 = 0

Answer: 2

GCD(116,42) = d = ax + by ?

q	a	b	x_2	x_1	y_2	y_1	
-	116	42	1	0	0	1	initial values
2	42	32	0	1	1	-2	

2 =[116/42]

32 =116 mod 42

1 =1-2*0

-2 =0-2*1

QCD(116,42) = d = ax + by ?

q	a	b	x_2	x_1	y_2	y_1
-	116	42	1	0	0	1
2	42	32	0	1	1	-2
1	32	10	1	-1	-2	3
3	10	2	-1	4	3	-11
5	2	0	4	-21	-11	58
answer:	d		x		y	

inverse of an integer modulo 9

problem: 8^{-1} mod 9 = ?

8y=1 mod 9 => 9x + 8y =1 mod 9

q	a	b	y_2	y_1
-	9	8	0	1
1	8	1	1	-1
8	1	0	-1	.

so 9*1 + 8*(-1)=1 & y=-1=8 mod 9
thus 8 is the inverse of itself mod 9
$8=8^{-1}$ mod 9
8*8 = 1 mod 9

multiplicative or modular inverse of an integer

problem: 4^{-1} mod 9 = ?

4y=1 mod 9 => 9x + 4y =1 mod 9

q	a	b	y_2	y_1
-	9	4	0	1
2	4	1	1	-2
4	1	0	-2	.

so 9*1 + 4*(-2)=1 & y=-2=7 mod 9
thus 7 is the inverse of 4 mod 9
4*7=1 mod 9

inverse of integers mod 9

2^{-1} mod 9 = 5
5^{-1} mod 9 = 2
1^{-1} mod 9 = 1
3^{-1} mod 9 = ?

3y=1 mod 9
9x + 3y =1 mod 9
3(3x + y) =1 mod 9 => no solution

6^{-1} mod 9 = ? => no solution

all invertible elements modulo 9
Z^*_9={1,2,4,5,7,8}
n is invertible ⇔ GCD(n,9)=1

How to calculate powers modulo *n*?

$b = a^k \bmod n = ?$ if $n \in I; a, k \in Z_n$

Algorithm

if $k = 0$ then $b = 1$

else begin

$A = a$

convert k into binary form $k = \sum_{i=0}^{j} k_i 2^i$

$b = A^{k_0}$

for $i = 1$ to j do begin

$A = A^2 \bmod n$

$b = b \cdot A^{k_i} \bmod n$

end

end

return(b)

- *Mathematica:* b=PowerMod[a,k,n]

Example of RSA application

I. RSA key generation

Bob chooses p=11, q=17, e=13

(artificially small numbers so completely insecure)

1. Bob calculates

$n = pq = 11 \cdot 17 = 187$

$\phi = (p-1)(q-1) = 10 \cdot 16 = 160$

2. Bob checks whether ϕ are e are coprime:

- inefficient direct method

```
160 | 2
 80 | 2
 40 | 2
 20 | 2
 10 | 2
  5 | 5
  1 |
```

GCD(ϕ, e) =GCD$(160, 13)$ =GCD$(2^5 \cdot 5, 13) = 1$ $\Rightarrow$ OK

- efficient Euclidean algorithm

```
160 mod 13 = 4
 13 mod  4 = 1
  4 mod #1 = 0
```

$\Rightarrow$ GCD$(160, 13) = 1$

3. Bob calculates d using the extended Euclidean algorithm

q'	ϕ	e	y_2	y_1
-	160	13	0	1
12	13	4	1	-12
3	4	1	-12	37
4	1	0	37	.

$\Rightarrow$ $d = 37$

4. he double checks that d is the multiplicative inverse of e:

$de = 13 \cdot 37 = 481 \equiv 1 \pmod{160}$

5. so Bob has generated the keys:

public key $(n, e) = (187, 13)$

private key $d = 37$

or vice versa **public key** $(n, d) = (187, 37)$

private key $e = 13$

II. RSA encryption

Assume that Alice wants to encrypt the following cleartext: “AM” :-)

using, for example, the following public alphabet:

01 A	02 Ą	03 B	04 C	05 Ć	06 D	07 E	08 Ę	09 F	10 G
11 H	12 I	13 J	14 K	15 L	16 Ł	17 M	18 N	19 Ń	20 O
21 Ó	22 P	23 q	24 R	25 S	26 Ś	27 T	28 U	29 v	30 W
31 X	32 Y	33 Z	34 Ż	35 Ź	36 _	37 -	38 ?	39 ,	40 .

1. Alice converts her cleartext into the plaintext:

$m = (01, 17) = 117$

2. Alice calculates cipher using the public key $(n, e) = (187, 13)$:

$c = m^e \bmod n = 117^{13} \bmod 187 = ?$

$13 = (1101)_2$

i	0	1	2	3	
e_i	1	0	1	1	
A^2	117	$117^2 \equiv 38$	$38^2 \equiv 135$	$135^2 \equiv 86$	(mod 187)
c	117	117	117*135≡87	87*86≡2	(mod 187)

so the cipher is $c = 2$

- *Mathematica:* PowerMod[117, 13, 187]$\hookrightarrow$ 2

III. RSA decryption

1. Bob calculates $m = c^d \bmod n = 2^{37} \bmod 187$

$d = 37 = (100101)_2$

i	0	1	2	3	4	5	
d_i	1	0	1	0	0	1	
A^2	2	4	16	$16^2 \equiv 69$	$69^2 \equiv 86$	$86^2 \equiv 103$	(mod 187)
m	2	2	32	32	32	32*103 ≡ 117	(mod 187)

2. thus he finds Alice's message to be

$m = 117 = (01, 17) =$ „AM" $\square$

lengths of public keys

1. The above PKC examples were given for **artificially small** numbers and thus such cryptosystems are not secure at all.
2. To insure security of a PKC system, the lengths of public keys should be of **hundreds of decimal digits**.
3. To determine the required key length you should consider:
   - intended security
   - lifetime of the key
   - current state-of-the-art of factoring.
4. The wise cryptographer is **ultra-conservative** when choosing public-key key lengths as **history** teaches us a lot:
   - "I shall be surprised if anyone regularly factors numbers of size 10^{80} without special form during the present century" (R. Guy, 1976).
   - "Factoring a 125-digit number would take 40 quadrillion years", tj. $4 \cdot 10^{19}$ lat (R. Rivest, 1977).
   - ... but already in 1994 a 129-digit number was factorized.

Recommended lengths of public keys

to be secure against attacks of
(a) a single person, (b) private agencies, (c) national security agencies:

```
       length in bits   =>      length in decimal digits
year   (a)   (b)   (c)          (a)   (b)   (c)
1995   768  1280  1536          231   386   463
2000  1024  1280  1536          308   386   463
2005  1280  1536  2048          386   463   617
2010  1280  1536  2048          386   463   617
2015  1536  2048  2048          463   617   617
```

[Bruce Schneier: "Applied Cryptography"]

- American National Security Agency (NSA) recommends key lengths from 512 up to 1024 bits (so from 154 do 308 decimal digits) in their Digital Signature Standard (DSS).

integer length (number of digits)

length L_b of integer n with base b is given by

$L_b = [\![\log_b n]\!] + 1 = [\![\ln n / \ln b]\!] + 1$

How Eve can crack the RSA cryptosystem?

By factorizing n:

If Eve can factorize $n = pq$ then she can calculate $\phi = (p-1)(q-1)$

and thus can calculate Bob's private key d

Why is the RSA believed to be secure for large integers?

There is seemingly no efficient

(i.e., polynomial-time and polynomial-space)

classical algorithm for integer factorization.

RSA hypothesis (1978)

Any general method of cracking the RSA cryptosystem

which enables finding private key d from public key (n, e)

requires an efficient algorithm for integer factorization.

Note

There is still no proof of this hypothesis.

RSA and majority of public-key cryptosystems would be **insecure** if we could implement efficiently:

- **Shor**'s algorithm
  on a large quantum computer

or

- **Adleman**'s algorithm
  on a DNA computer.

a Deutsch problem

Given an oracle (black box) that computes **a Boolean function** $f(x) : \{0,1\} \to \{0,1\}$

How many questions one should ask the oracle to check whether f is constant or balanced?

or

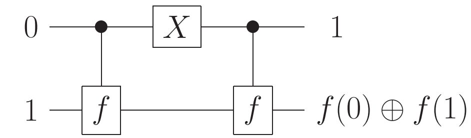
Can you check whether a coin is real or fake by a single observation?

balanced and constant functions

constant	$f_1(0) = 0$	$f_1(1) = 0$
	$f_2(0) = 1$	$f_2(1) = 1$
balanced	$f_3(0) = 0$	$f_3(1) = 1$
	$f_4(0) = 1$	$f_4(1) = 0$

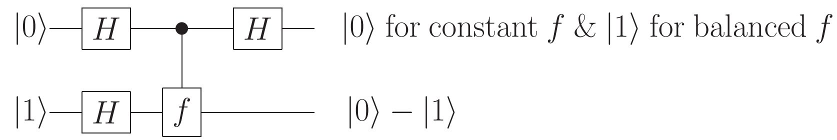
classical solution

2 queries + 1 auxiliary operation

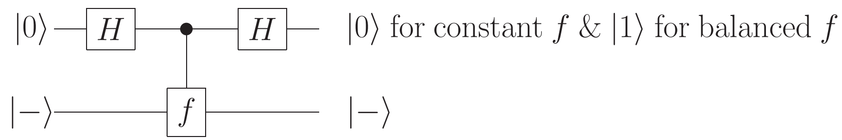


quantum solution

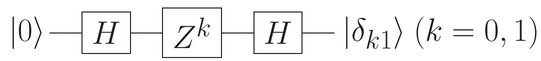
1 query + 3 auxiliary operations



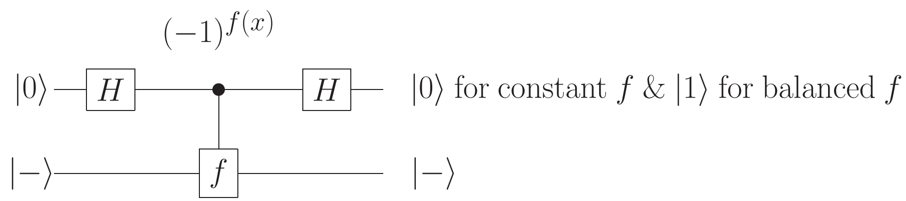
or 1 query + 2 auxiliary operations



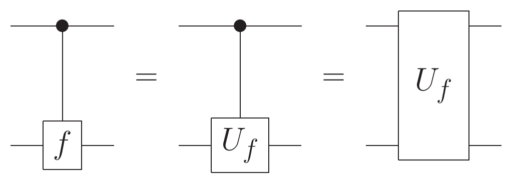
main idea



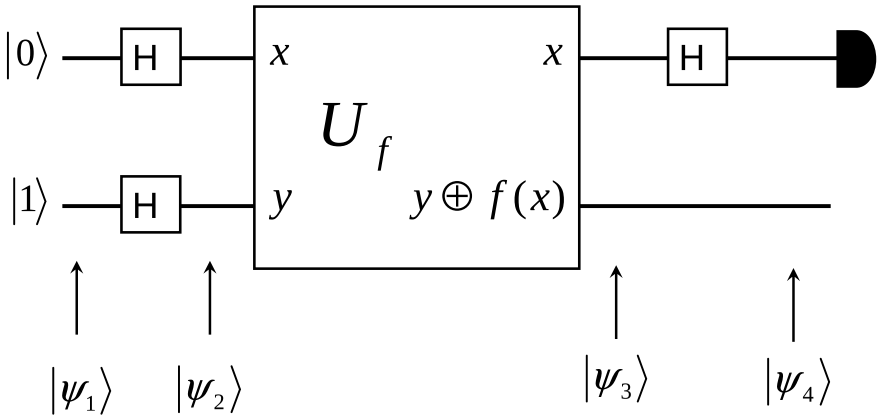
or



different symbols for the same gate



Deutsch algorithm



Deutsch algorithm

1. prepare input state

$$|\psi_1\rangle = |0\rangle|1\rangle$$

2. apply Hadamard gates (create equal superposition)

$$\begin{aligned}|\psi_2\rangle &= \hat{H}^{\otimes 2}|\psi_1\rangle = |+\rangle|-\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} \\ &= \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)\end{aligned}$$

3. apply $\hat{U}_f$ gate

$$|x\rangle|y\rangle \rightarrow \boxed{\hat{U}_f} \rightarrow |x\rangle|y \oplus f(x)\rangle$$

$$\begin{aligned}|\psi_3\rangle &= \hat{U}_f|\psi_2\rangle \\ &\sim \hat{U}_f|00\rangle - \hat{U}_f|01\rangle + \hat{U}_f|10\rangle - \hat{U}_f|11\rangle \\ &= |0, 0 \oplus f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, 0 \oplus f(1)\rangle - |1, 1 \oplus f(1)\rangle\end{aligned}$$

We neglect normalization thus sign '$\sim$' is used.

case I: $f(0) = f(1) = 0$

$$\begin{aligned}|\psi_3\rangle &\sim |0, 0 \oplus 0\rangle - |0, 1 \oplus 0\rangle + |1, 0 \oplus 0\rangle - |1, 1 \oplus 0\rangle \\ &= |0, 0\rangle - |0, 1\rangle + |1, 0\rangle - |1, 1\rangle \\ &= |0\rangle(|0\rangle - |1\rangle) + |1\rangle(|0\rangle - |1\rangle) \\ &\sim |+\rangle|-\rangle\end{aligned}$$

case II: $f(0) = f(1) = 1$

$$\begin{aligned}|\psi_3\rangle &\sim |0, 0 \oplus 1\rangle - |0, 1 \oplus 1\rangle + |1, 0 \oplus 1\rangle - |1, 1 \oplus 1\rangle \\ &= |0, 1\rangle - |0, 0\rangle + |1, 1\rangle - |1, 0\rangle \\ &= -|0\rangle(|0\rangle - |1\rangle) - |1\rangle(|0\rangle - |1\rangle) \\ &\sim -|+\rangle|-\rangle\end{aligned}$$

so

$$f(0) = f(1) \Rightarrow |\psi_3\rangle = \pm|+\rangle|-\rangle$$

case III: $f(0) = 0, f(1) = 1$

$$\begin{aligned}|\psi_3\rangle &\sim |0, 0 \oplus f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, 0 \oplus f(1)\rangle - |1, 1 \oplus f(1)\rangle \\ &= |0, 0 \oplus 0\rangle - |0, 1 \oplus 0\rangle + |1, 0 \oplus 1\rangle - |1, 1 \oplus 1\rangle \\ &= |0, 0\rangle - |0, 1\rangle + |1, 1\rangle - |1, 0\rangle \\ &= |0\rangle(|0\rangle - |1\rangle) + |1\rangle(|1\rangle - |0\rangle) \\ &\sim |0\rangle|-\rangle - |1\rangle|-\rangle \\ &\sim |-\rangle|-\rangle\end{aligned}$$

case IV: $f(0) = 1, f(1) = 0$

$$\begin{aligned}|\psi_3\rangle &\sim |0, 0 \oplus f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, 0 \oplus f(1)\rangle - |1, 1 \oplus f(1)\rangle \\ &= |0, 0 \oplus 1\rangle - |0, 1 \oplus 1\rangle + |1, 0 \oplus 0\rangle - |1, 1 \oplus 0\rangle \\ &= |0, 1\rangle - |0, 0\rangle + |1, 0\rangle - |1, 1\rangle \\ &= -|0\rangle(|0\rangle - |1\rangle) - |1\rangle(|1\rangle - |0\rangle) \\ &\sim -|-\rangle|-\rangle\end{aligned}$$

so

$$f(0) \neq f(1) \Rightarrow |\psi_3\rangle = \pm|-\rangle|-\rangle$$

4. apply Hadamard gates

$$|\psi_4\rangle = \hat{H} \otimes \hat{I}|\psi_3\rangle$$

cases I & II:

$$f(0) = f(1) \Rightarrow |\psi_4\rangle = \pm\hat{H} \otimes \hat{I}|+\rangle|-\rangle = \pm|0\rangle|-\rangle = \pm|f(0) \oplus f(1)\rangle|-\rangle$$

cases III & IV:

$$f(0) \neq f(1) \Rightarrow |\psi_4\rangle = \pm\hat{H} \otimes \hat{I}|-\rangle|-\rangle = \pm|1\rangle|-\rangle = \pm|f(0) \oplus f(1)\rangle|-\rangle$$

thus we have for any case:

$$|\psi_4\rangle = \pm|f(0) \oplus f(1)\rangle|-\rangle \equiv |x\rangle|y\rangle$$

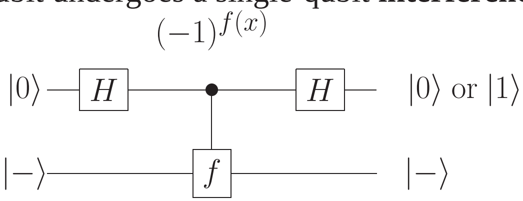
5. measure only the 1st register

$$\begin{aligned} x &= 0 \Rightarrow f(0) = f(1) \\ x &= 1 \Rightarrow f(0) \neq f(1) \end{aligned}$$

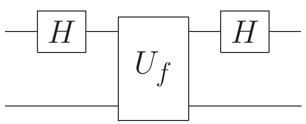
QED

Some remarks on Deutsch algorithm

- top qubit undergoes a single-qubit **interference**

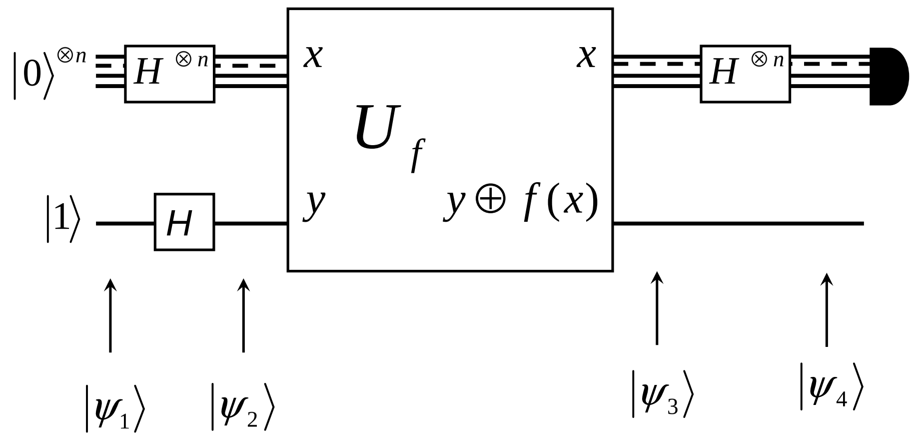


- **relative phases** are introduced by the function evaluation
- lower qubit is an **ancilla** – it is not measured and can be discarded after function evaluation
- a **sequence of gates**
  Hadamard - function evaluation - Hadamard



is a common pattern in quantum algorithms

Deutsch-Jozsa (DJ) algorithm



Deutsch-Jozsa (DJ) algorithm for 3 qubits

1. prepare input state

$$|\psi_1\rangle = |0\rangle^{\otimes 2}|1\rangle = |001\rangle$$

2. apply Hadamard gates

$$\begin{aligned} |\psi_2\rangle &= \hat{H}^{\otimes(2+1)}|\psi_1\rangle \\ &= |+\rangle^{\otimes 2}|-\rangle \\ &= \frac{|0\rangle + |1\rangle}{\sqrt{2}}\frac{|0\rangle + |1\rangle}{\sqrt{2}}\frac{|0\rangle - |1\rangle}{\sqrt{2}} \\ &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)\frac{|0\rangle - |1\rangle}{\sqrt{2}} \\ &\sim |000\rangle + |010\rangle + |100\rangle + |110\rangle \\ &\quad -(|001\rangle + |011\rangle + |101\rangle + |111\rangle) \end{aligned}$$

3. apply $\hat{U}_f$ gate

$$\begin{aligned}|\psi_3\rangle \sim\ & |00, 0\oplus f(00)\rangle + |01, 0\oplus f(01)\rangle \\ & +|10, 0\oplus f(10)\rangle + |11, 0\oplus f(11)\rangle \\ & -\Big(|00, 1\oplus f(00)\rangle + |01, 1\oplus f(01)\rangle \\ & +|10, 1\oplus f(10)\rangle + |11, 1\oplus f(11)\rangle\Big)\end{aligned}$$

4. apply Hadamard gates

$$|\psi_4\rangle = \hat{H}^{\otimes 2}\otimes \hat{I}|\psi_3\rangle$$

***. let's analyze all cases for different functions f**

number of cases

$N_{\text{cases}} = C_0^4 + C_4^4 + C_2^4 = 1+1+6 = 8$

where $|\{00, 01, 10, 11\}| = 4$

C_n^m – binomial coefficient

case 1: (trivial)

$$f(00) = f(01) = f(10) = f(11) = 0$$

$$|\psi_4\rangle = (\hat{I}\otimes\hat{H})|\psi_1\rangle = |00-\rangle$$

case 2: (trivial)

$$f(00) = f(01) = f(10) = f(11) = 1$$

$$\begin{aligned}|\psi_3\rangle &= \hat{U}_f|\psi_2\rangle \\ &= \hat{U}_f\Big(|00\rangle + |10\rangle + |01\rangle + |11\rangle\Big)\Big(|0\rangle - |1\rangle\Big) \\ &= \Big(|00\rangle + |10\rangle + |01\rangle + |11\rangle\Big)\Big(|1\rangle - |0\rangle\Big) \\ &= -|\psi_2\rangle\end{aligned}$$

so

$$|\psi_4\rangle = -(\hat{I}\otimes\hat{H})|\psi_1\rangle = -|00-\rangle$$

case 3:

$$f(00) = 0, f(01) = 0, f(10) = 1, f(11) = 1$$

$$\begin{aligned}|\psi_3\rangle \sim\ & |00, 0\oplus 0\rangle + |01, 0\oplus 0\rangle + |10, 0\oplus 1\rangle + |11, 0\oplus 1\rangle \\ & -(|00, 1\oplus 0\rangle + |01, 1\oplus 0\rangle + |10, 1\oplus 1\rangle + |11, 1\oplus 1\rangle)\end{aligned}$$

$$\begin{aligned}&= |000\rangle + |010\rangle + |101\rangle + |111\rangle \\ &\quad -(|001\rangle + |011\rangle + |100\rangle + |110\rangle) \\ &= (|00\rangle - |10\rangle + |01\rangle - |11\rangle)(|0\rangle - |1\rangle) \\ &= (|0\rangle - |1\rangle)(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \\ &\sim |-,+,-\rangle\end{aligned}$$

so

$$|\psi_4\rangle = (\hat{H}^{\otimes 2}\otimes\hat{I})|\psi_3\rangle \sim (\hat{H}^{\otimes 2}\otimes\hat{I})|-,+,-\rangle = |1,0,-\rangle$$

all cases in DJ algorithm for 3 qubits

case	f(00)	f(01)	f(10)	f(11)	$\|x_1, x_2, y\rangle$	$\|\mathbf{x}, y\rangle$	answer
1.	0	0	0	0	$\|00-\rangle$	$\|0-\rangle$	constant
2.	1	1	1	1	$\|00-\rangle$	$\|0-\rangle$	
3.	0	0	1	1	$\|10-\rangle$	$\|2-\rangle$	
4.	0	1	0	1	$\|01-\rangle$	$\|1-\rangle$	
5.	0	1	1	0	$\|11-\rangle$	$\|3-\rangle$	balanced
6.	1	0	0	1	$\|11-\rangle$	$\|3-\rangle$	
7.	1	0	1	0	$\|01-\rangle$	$\|1-\rangle$	
8.	1	1	0	0	$\|10-\rangle$	$\|2-\rangle$	

$$\mathbf{x} \equiv (x_1, x_2) \cong 2x_1 + x_2$$

5. measure x

if $x = 0 \quad \Rightarrow \quad f(x)$ is constant

if $x > 0 \quad \Rightarrow \quad f(x)$ is balanced

Matlab program

```
H=[1 1;1 -1];Norm=1/8;
f=[
0 0 0 0
1 1 1 1
0 0 1 1
0 1 0 1
0 1 1 0
1 0 0 1
1 0 1 0
1 1 0 0
];
for n=1:8,

f00=f(n,1);f01=f(n,2);f10=f(n,3);f11=f(n,4);

psi3=ket([0,0,f00])+ket([0,1,f01])+ket([1,0,f10])+ket([1,1,f11])+...
 -(ket([0,0,1-f00])+ket([0,1,1-f01])+ket([1,0,1-f10])+ket([1,1,1-f11]));

psi4=Norm*tensor_product(H,H,H)*psi3; % for clarity we add extra H gate
vector2ket(psi4)

end;
```


quantum Hadamard transform

1. How to generate equal (equally-weighted) superposition

$$\begin{aligned}\hat{H}^{\otimes 2}|00\rangle &= \frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}} \\ &= \frac{1}{2}(|00\rangle+|01\rangle+|10\rangle+|11\rangle) \\ &\equiv \frac{1}{2}\sum_{\mathbf{x}\in\{0,1\}^2}|\mathbf{x}\rangle \\ &\equiv \frac{1}{2}\sum_{\mathbf{x}=0}^{3}|\mathbf{x}\rangle\end{aligned}$$

in general

$$\hat{H}^{\otimes n}|0\rangle^{\otimes n} = \hat{H}^{\otimes n}|\mathbf{0}\rangle = \frac{1}{\sqrt{N}}\sum_{\mathbf{x}}|\mathbf{x}\rangle$$

where $N = 2^n$ and $x = 2^n x_1 + 2^{n-1}x_2 + \ldots x_n$

$$\sum_{\mathbf{x}} = \sum_{\mathbf{x}\in\{0,1\}^n} = \sum_{x_1=0}^{1}\sum_{x_2=0}^{1}\ldots\sum_{x_n=0}^{1} = \sum_{x=0}^{N-1}$$

2. How to compactly write the quantum Hadamard transform

- **for a single qubit**

$$\begin{aligned}\hat{H}|0\rangle &= \frac{|0\rangle+|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\sum_{z=0}^{1}(-1)^{0\cdot z}|z\rangle \\ \hat{H}|1\rangle &= \frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\sum_{z=0}^{1}(-1)^{1\cdot z}|z\rangle\end{aligned}$$

combining together

$$\hat{H}|x_1\rangle = \frac{1}{\sqrt{2}}\sum_{z_1=0}^{1}(-1)^{x_1\cdot z_1}|z_1\rangle$$

- **for two qubits**

$$\begin{aligned}\hat{H}^{\otimes 2}|x_1x_2\rangle &= \left(\frac{1}{\sqrt{2}}\sum_{z_1=0}^{1}(-1)^{x_1\cdot z_1}|z_1\rangle\right)\left(\frac{1}{\sqrt{2}}\sum_{z_2=0}^{1}(-1)^{x_2\cdot z_2}|z_2\rangle\right) \\ &= \frac{1}{\sqrt{2^2}}\sum_{z_1=0}^{1}\sum_{z_2=0}^{1}(-1)^{x_1\cdot z_1+x_2\cdot z_2}|z_1z_2\rangle\end{aligned}$$

- thus in general **for n qubits**

$$\hat{H}^{\otimes n}|x_1x_2...x_n\rangle = \frac{1}{\sqrt{N}}\sum_{z_1,z_2,...,z_n=0}^{1}(-1)^{x_1\cdot z_1+x_2\cdot z_2+...+x_n\cdot z_n}|z_1z_2...z_n\rangle$$

where $N = 2^n$ is the Hilbert-space dimension

or compactly

$$\hat{H}^{\otimes n}|\mathbf{x}\rangle = \frac{1}{\sqrt{N}}\sum_{\mathbf{z}}(-1)^{\langle\mathbf{x}|\mathbf{z}\rangle}|\mathbf{z}\rangle$$

where

$$\begin{aligned}\mathbf{x} &= (x_1,x_2,...,x_n), \quad |\mathbf{x}\rangle = |x_1,x_2,...,x_n\rangle \\ \mathbf{z} &= (z_1,z_2,...,z_n), \quad |\mathbf{z}\rangle = |z_1,z_2,...,z_n\rangle\end{aligned}$$

and

$$\langle\mathbf{x}|\mathbf{z}\rangle \equiv \mathbf{x}\cdot\mathbf{z} = x_1z_1 + x_2z_2 + ... + x_nz_n$$

is the scalar product.

DJ algorithm for n qubits

1. **initialize** $(n+1)$-qubit state

$$|\psi_1\rangle = |0\rangle^{\otimes n}|1\rangle$$

2. generate equal superposition by applying **Hadamard** gates

$$|\psi_2\rangle = \hat{H}^{\otimes(n+1)}|\psi_1\rangle = (\hat{H}^{\otimes n}|0\rangle^{\otimes n})|-\rangle = \frac{1}{\sqrt{N}}\sum_{\mathbf{x}}|\mathbf{x}\rangle|-\rangle$$

3. **calculate** f by applying $\hat{U}_f$ gate

$$|\psi_3\rangle = \hat{U}_f|\psi_2\rangle = \frac{1}{\sqrt{N}}\sum_{\mathbf{x}}(-1)^{f(\mathbf{x})}|\mathbf{x}\rangle|-\rangle$$

DJ algorithm for n qubits

4. apply **Hadamard** gate

$$|\psi_4\rangle = (\hat{H}^{\otimes n}\otimes\hat{I})|\psi_3\rangle$$

$$\begin{aligned}\hat{H}^{\otimes n}|\mathbf{x}\rangle &= \frac{1}{\sqrt{N}}\sum_{\mathbf{x}}(-1)^{f(\mathbf{x})}\left(\hat{H}^{\otimes n}|\mathbf{x}\rangle\right)|-\rangle \\ &= \frac{1}{N}\sum_{\mathbf{x}}\sum_{\mathbf{z}}(-1)^{\langle\mathbf{x}|\mathbf{z}\rangle+f(\mathbf{x})}|\mathbf{z}\rangle|-\rangle\end{aligned}$$

5. **measure** $|\mathbf{z}\rangle$:

$$\begin{aligned}\mathbf{z} &= 0 \Rightarrow f(\mathbf{x}) \quad \text{is constant} \\ \mathbf{z} &> 0 \Rightarrow f(\mathbf{x}) \quad \text{is balanced}\end{aligned}$$

quantum Fourier transform (QFT)

- **QFT on group $(Z_2)^n$**
= quantum Hadamard transform

$$QFT'|\mathbf{x}\rangle = \hat{H}^{\otimes n}|\mathbf{x}\rangle = \frac{1}{\sqrt{N}}\sum_{\mathbf{y}}(-1)^{\langle\mathbf{x}|\mathbf{y}\rangle}|\mathbf{y}\rangle, \quad (N = 2^n)$$

group Z_2 = the set $\{0,1\}$ with addition modulo 2 ($\oplus$)

group $(Z_2)^n$ = the set $\{0,1\}^n$ with addition modulo 2 ($\oplus$) bit by bit

- **QFT on group Z_N**

$$QFT|\mathbf{x}\rangle = \frac{1}{\sqrt{N}}\sum_{\mathbf{y}}\exp\left(\frac{2\pi i}{N}\mathbf{xy}\right)|\mathbf{y}\rangle$$

or just without the bold face:

$$QFT|x\rangle = \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}\exp\left(\frac{2\pi i}{N}xy\right)|y\rangle$$

group Z_N = the set $\{0,1,\ldots,N-1\}^n$ with addition modulo N ($\oplus$)

Quantum Fourier Transform

$$|x\rangle \rightarrow \boxed{QFT} \rightarrow \frac{1}{\sqrt{N}}\sum_{z=0}^{N-1}\exp\left(\frac{2\pi i}{N}xy\right)|y\rangle$$

or compactly

$$|x\rangle \rightarrow \boxed{QFT} \rightarrow \frac{1}{\sqrt{N}}\sum_{z=0}^{N-1}\beta^{xy}|y\rangle$$

where

$$\beta = \exp\left(\frac{2\pi i}{N}\right)$$

QFT of arbitrary pure state of n qubits

$$|\psi\rangle = \sum_{x=0}^{N-1}c_x|x\rangle \rightarrow \boxed{QFT} \rightarrow \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}c_x\beta^{xy}|y\rangle$$

Quantum Fourier Transform in matrix representation

$$|\psi\rangle = \sum_{x=0}^{N-1} c_x |x\rangle$$

$$QFT|\psi\rangle = \frac{1}{\sqrt{s+1}} \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \beta & \beta^2 & \dots & \beta^s \\ 1 & \beta^2 & \beta^4 & \dots & \beta^{2s} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta^s & \beta^{2s} & \dots & \beta^{ss} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_s \end{bmatrix}$$

where

$\beta = \exp\left(\frac{2\pi i}{N}\right)$

$s = N - 1 = 2^n - 1$

example: QFT of a Bell state

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}[1001]^T$$

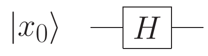
$$N = 2^2 = 4 \Rightarrow s = 3, \quad \beta = \exp\left(i\frac{\pi}{2}\right) = i$$

$$QFT = \frac{1}{\sqrt{4}} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \beta & \beta^2 & \beta^3 \\ 1 & \beta^2 & \beta^4 & \beta^6 \\ 1 & \beta^3 & \beta^6 & \beta^9 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$$

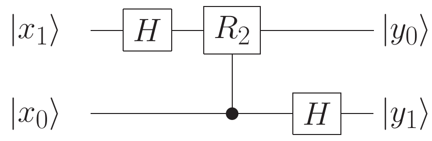
$$\begin{aligned} QFT|\psi\rangle &= QFT\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{2\sqrt{2}} \begin{bmatrix} 2 \\ 1-i \\ 0 \\ 1+i \end{bmatrix} \\ &= \frac{1}{\sqrt{2}}|00\rangle + \frac{e^{-i\pi/4}}{2}|01\rangle + \frac{e^{i\pi/4}}{2}|11\rangle \end{aligned}$$

Circuits for QFT

QFT for n=1



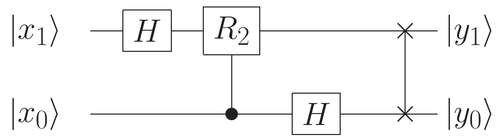
QFT for n=2



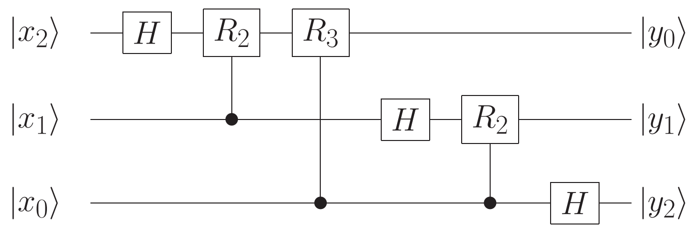
where

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad R_k = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 \\ 0 & \exp\left(\frac{2\pi}{2^k} i\right) \end{bmatrix}$$

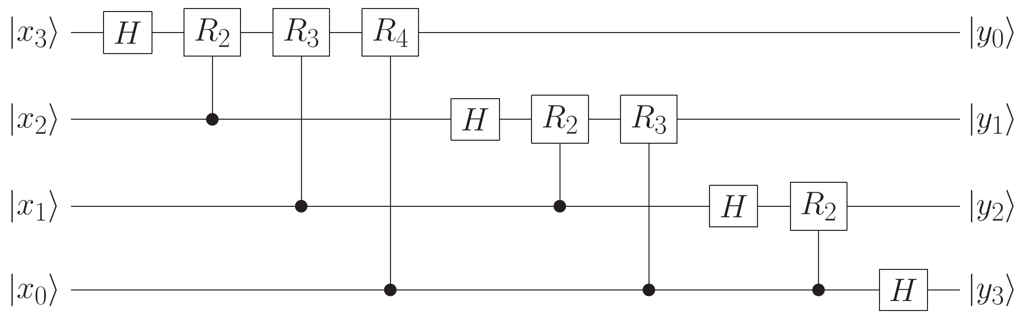
including SWAP



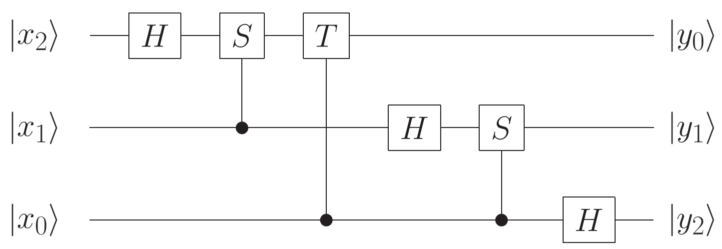
QFT for n=3



QFT for n=4



Seemingly another implementation of QFT for n=3



given in terms of the phase gate (S gate) and $\pi/8$ (sic!) gate (T gate)

$$\hat{S} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \quad \hat{T} = \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix}$$

but it is exactly our scheme as

$$\hat{R}_2 = \hat{S}, \quad \hat{R}_3 = \hat{T}$$

Introduction to quantum algorithms (part III)

Grover's algorithm for searching database

Shor's algorithm for integer factorization

problem for Grover's algorithm

(the needle in a haystack problem)

assumptions

- given an **oracle** which calculates $f(x)$:

$$f(x) = 1 \text{ if } x = x_0$$

$$f(x) = 0 \text{ if } x \neq x_0$$

- $f(x)$ can be calculated using ordinary (reversible) computer code.

problem

find the element x_0 in the least number of oracle queries.

average number of evaluations of f

classically – $N/2$

quantumly – ???

examples

- searching a phone book for a name and phone number
- searching a database for a key to crack a cryptosystem

oracle queries

1. oracle query in DJ algorithm

$$\hat{U}_f = |x\rangle|y\rangle \overset{f}{\mapsto} |x\rangle|x \oplus y\rangle$$

a note

in fact, the content of the **target register** $|y\rangle$ is unchanged in the DJ algorithm and $f(x)$ is encoded in the sign of the **control register** $|x\rangle$.

2. oracle query in Grover's algorithm

$$\hat{U}_f|x\rangle = (-1)^{f(x)}|x\rangle$$

or

$$\hat{U}_f = 1 - 2|x_0\rangle\langle x_0|$$

it is just equivalent to the query in DJ algorithm

two types of quantum oracles

oracle = a black-box unitary operation

1. **quantum oracle $\hat{U}_f$ of a Boolean function**

$$f : \{0,1\} \to \{0,1\}$$

$$\boxed{|x\rangle|y\rangle \to \boxed{U_f} \to |x\rangle|y \oplus f(x)\rangle}$$

2. **quantum phase-oracle $\hat{U}'_f$**

$$\boxed{|x\rangle \to \boxed{U'_f} \to (-1)^{f(x)}|x\rangle}$$

Note:

$$\boxed{|y\rangle = |-\rangle \quad \Rightarrow \quad \hat{U}_f \to \hat{U}'_f}$$

n-Qubit Grover's algorithm

PROBLEM:

find x_0 among $N = 2^n$ elements encoded by n-qubits

ALGORITHM:

I. **Initialization**

prepare n qubits in state

$$|\psi_I\rangle = |0\rangle^{\otimes n}$$

II. **Generation of equally-weighted superposition**

apply Hadamard gate $\hat{H}^{\otimes n}$ to all qubits to get

$$|\psi_{II}\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle.$$

III. **Grover iteration**

repeat the following subroutine $\mathrm{Int}(\pi\sqrt{N}/4)$ times:

1. Call the **oracle** to flip the phase of eigenstate $|x_0\rangle$:

$$f_{x_0} : |x\rangle \mapsto (1 - 2\delta_{x_0,x})|x\rangle,$$

   where $\delta_{y,x}$ is Kronecker delta.

2. Apply **Hadamard** gate $\hat{H}^{\otimes n}$.
3. **Flip** the phase of all eigenstates $|x\rangle$ except $|0\rangle$:

$$f_0 : |x\rangle \mapsto -(1 - 2\delta_{0,x})|x\rangle.$$

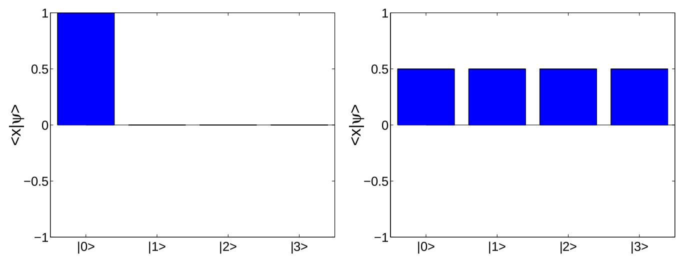
4. Apply **Hadamard** gate $\hat{H}^{\otimes n}$.

Note:

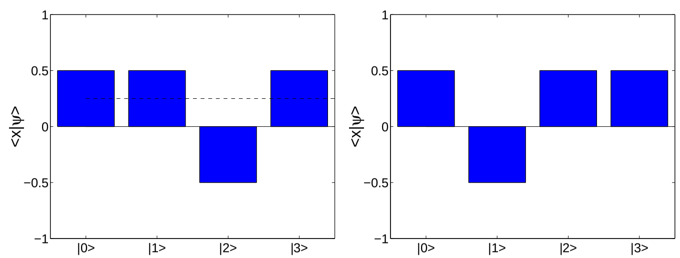
operations 2,3,4 are called the **inversion about the average**

two-qubit Grover's search of $|x_0\rangle = |2\rangle$

initialization / Hadamard gate

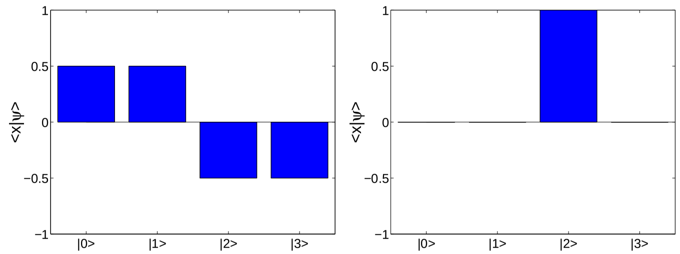


1. oracle phase flip of $|x_0\rangle$ / 2. Hadamard gate



two-qubit Grover's search of $|x_0\rangle = |2\rangle$

3. phase flip of all $|x\rangle$ except $|0\rangle$ 4. Hadamard gate



- end of 1st Grover iteration

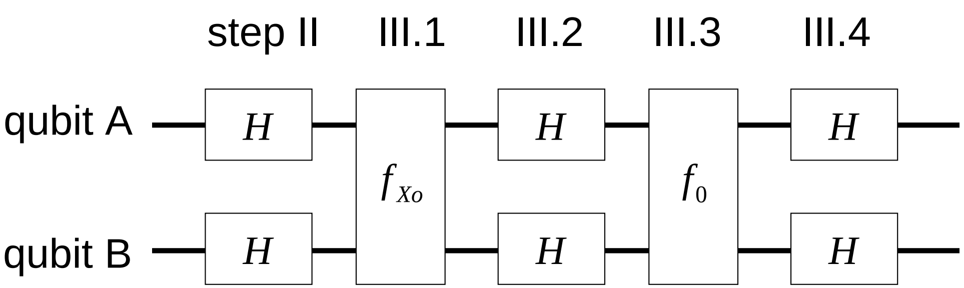
recommended number of repetitions (or queries)

$$N_{\text{queries}} = \text{Int}(\pi\sqrt{N}/4)$$

where $N = 2^n = 4$ so

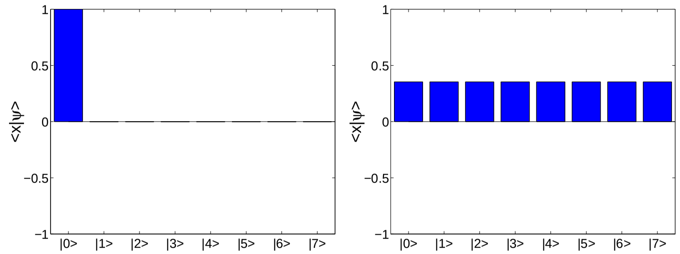
$$N_{\text{queries}} = 1$$

quantum circuit for two-qubit Grover's search

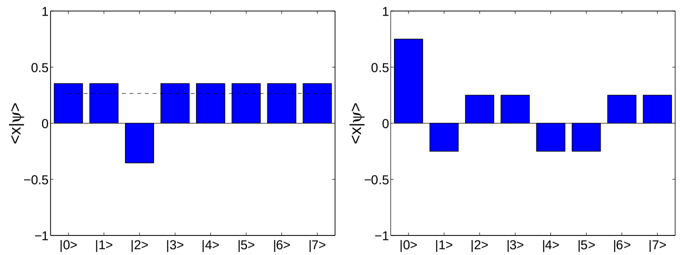


three-qubit Grover's search of $|x_0\rangle = |2\rangle$

initialization   Hadamard gate

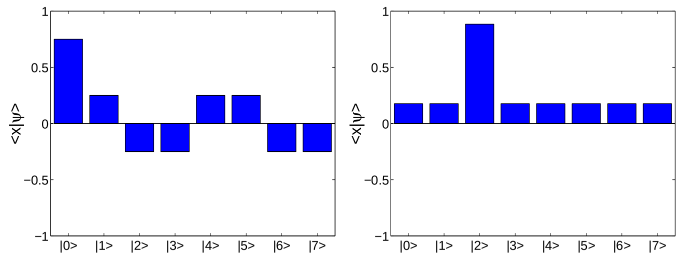


I.1 oracle phase flip of $|x_0\rangle$ I.2 Hadamard gate

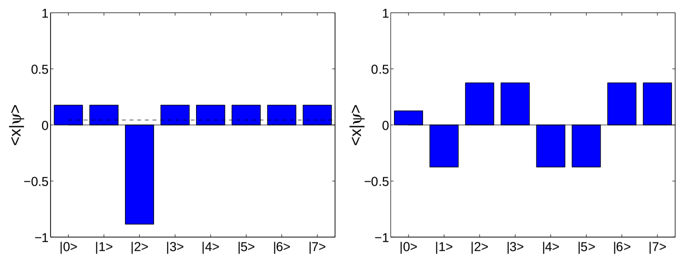


three-qubit Grover's search of $|x_0\rangle = |2\rangle$

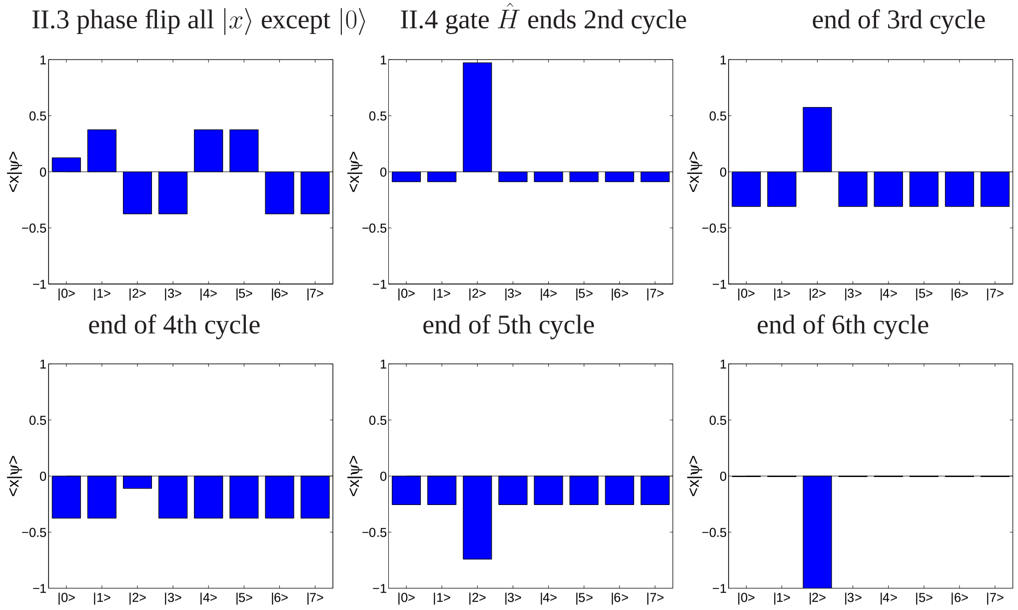
I.3 phase flip of all $|x\rangle$ except $|0\rangle$ I.4 Hadamard gate - end of 1st cycle



II.1 oracle phase flip of $|x_0\rangle$ II.2 Hadamard gate



three-qubit Grover's search of $|x_0\rangle = |2\rangle$



numerical data for three-qubit Grover's search of $|x_0\rangle = |5\rangle$

state

$$|\psi^{(k)}\rangle = c_0^{(k)}|000\rangle + c_1^{(k)}|001\rangle + c_2^{(k)}|010\rangle + c_3^{(k)}|011\rangle$$
$$+c_4^{(k)}|100\rangle + c_5^{(k)}|101\rangle + c_6^{(k)}|110\rangle + c_7^{(k)}|111\rangle$$

after the kth Grover we get:

$\lvert\psi^{(k)}\rangle =$[	c_0	c_1	c_2	c_3	c_4	c_5	c_6	c_7]
$\lvert\psi^{(1)}\rangle =$[	.18	.18	.18	.18	.18	.88	.18	.18]
$\lvert\psi^{(2)}\rangle =$[	-.09	-.09	-.09	-.09	-.09	.97	-.09	-.09]
$\lvert\psi^{(3)}\rangle =$[	-.31	-.31	-.31	-.31	-.31	.57	-.31	-.31]
$\lvert\psi^{(4)}\rangle =$[	-.38	-.38	-.38	-.38	-.38	-.11	-.38	-.38]
$\lvert\psi^{(5)}\rangle =$[	-.25	-.25	-.25	-.25	-.25	-.74	-.25	-.25]
$\lvert\psi^{(6)}\rangle =$[	-.01	-.01	-.01	-.01	-.01	-1.00	-.01	-.01]

after the 6th iteration we get

$$c_5^{(6)} = \langle 110|\psi^{(6)}\rangle = .99989\cdots \approx 1$$

The most popular cryptosystems and their cryptoanalysis

1. **DES (Data Encryption Standard) $\leftrightarrow$ Grover's algorithm**
   - symmetric
   - applied for encryption and decryption
   - American and international cryptographic standard
   - used by US army
2. **RSA (Rivest-Shamir-Adleman) $\leftrightarrow$ Shor's algorithm**
   - asymmetric
   - applied for encryption/decryption and digital signatures
3. **DSA (Digital Signature Algorithm) $\leftrightarrow$ Shor's algorithm**
   - asymmetric
   - applied for digital signatures
   - it is the Digital Signature Standard (DSS) of US Federal Government

Grover's algorithm and cryptography

Attack on DES

requires basically to search among $N = 2^{56} = 7.2 \times 10^{16}$ possible keys.

What is the time required to find the correct DES key?

assuming that 1 mln keys per second can be checked than

- classical computer needs 1,000 years
- quantum computer needs about 4 minutes

Mathematica: Sqrt[2^56]/10.^6/60 $\hookrightarrow$ 4.47 min

How many oracle queries are required to search an N-element database?

$\mathcal{O}(N)$	classical search algorithms
$\mathcal{O}(\sqrt{N})$	Grover's algorithm

Quantum speedup

$\boxed{\textbf{Grover's search is quadratically faster than classical search}}$

Note: It speeds up any kind of database search.

However the maximum advantage is gained in unsorted databases.

Can we find faster quantum-search algorithms?

Shor's algorithm is exponentially faster than classical ones,

so it possible to find also a search algorithm that fast?

Optimality theorem:

The search problem cannot be solved in less than $\mathcal{O}\left(\sqrt{N}\right)$ iterations.

$\Rightarrow$ $\boxed{\textbf{Grover's algorithm is optimal!}}$

But can we find an algorithm that would run, say, twice faster?

Possibly yes, but it is not the issue of the optimality theorem.

quantum entanglement and quantum speed-up

Q: Quantum entanglement is a key resource for QIP. But do we need it for quantum speed-up in e.g. Grover's algorithm?

A: "Entanglement is neither necessary for Grover's algorithm itself, nor for its efficiency." [Bhattacharya et al., 2002]

Q: Really?

A: Inversion about the average amplitude is a classical process.

Q: Can Grover's algorithm be implemented classically?

A: Grover's algorithm has already been experimentally implemented using classical Fourier optics.

quantum entanglement and database size

Q: Is entanglement useful for Grover's algorithm at all?

A: Yes. Lack of entanglement limits the database size, which scales linearly with the beam diameter D (or D^2 for a 2D version)

$\Rightarrow$ number of qubits scales only as $\propto \log_2 D$

assume D equal to the size of the universe, $\sim 10^{26} m$

$\Rightarrow$ it is equivalent to $\propto 86$ qubits.

This limitation exists for any database containing classical information.

Q: Anyway, it seems that entanglement is not necessary for quadratic speed-up.

But do we need it for exponential speed-up?

A: Most probably, yes.

How to implement Grover's algorithm classically?

via classical optical interference

A classical implementation of Grover's search

[Amsterdam's experiment of Bhattacharya et al. (2002)]

- quantum probability amplitudes

  $\hookrightarrow$ a transverse laser **beam profile**

  = a complex electric field amplitude $E(x)$
- quantum states, which label items of the database

  $\hookrightarrow$ continuous **coordinate** x
- sought item x_0

  $\hookrightarrow$ **narrow area** around the "item position" x_0

- quantum Hadamard transform

  $\hookrightarrow$ classical **Fourier transform** implemented by lenses

  specifically: spherical, achromatic doublet lenses

  with focal lengths $f_1 = 40$ cm, $f_2 = 60$ cm

- oracle $\hat{U}_f(x_0)$, which marks the item x_0

  by phase flipping all $|x\rangle$ except $|x_0\rangle$

  $\hookrightarrow$ phase plate (called the **oracle plate**)

  which imprints a **phase profile** $\Phi_{x_0}(x)$ on the beam

  $E(x) \longrightarrow E(x)\exp[i\Phi_{x_0}(x)]$

  $\Phi_{x_0}(x) = \phi$ if x is in a narrow area around x_0

  $\Phi_{x_0}(x) = 0$ elsewhere.

- each Grover's iteration

  $\hookrightarrow$ a **roundtrip** of a pulse between the cavity mirrors

  specifically: T=13.5ns

- gate $\hat{U}_f(0)$ which marks $|0\rangle$ by phase flipping all $|x\rangle$ except $|0\rangle$

  $\hookrightarrow$ phase plate (called the **IAA plate**) like the oracle plate

  which imprints **phase profile** in the Fourier plane

  (IAA = inversion about the average amplitude)

  $E(x) \longrightarrow E(x)\exp[i\Phi_0(x')]$

  $\Phi_0(x') = \phi$ if x' is in a narrow area around 0

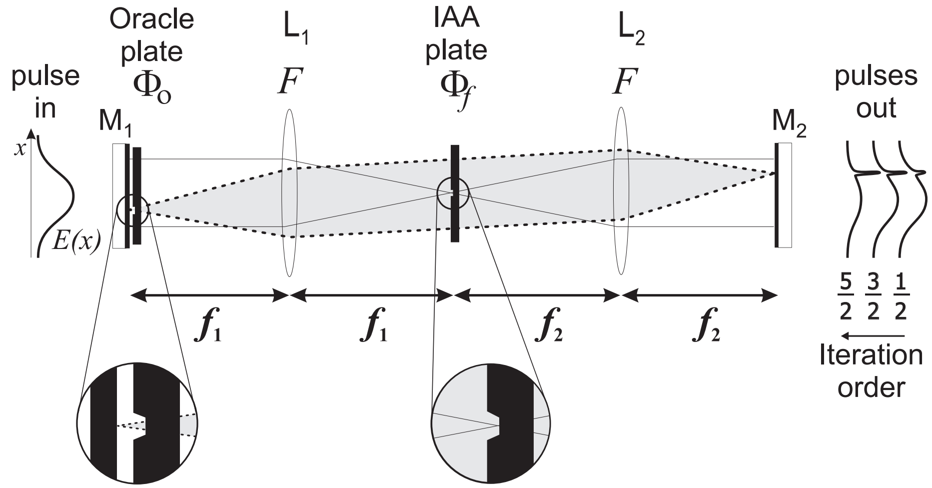
  $\Phi_0(x') = 0$ elsewhere.

- readout

$\hookrightarrow$ after each roundtrip, a **moving photodiode** records light transmitted through one of the mirrors with transmission of 2%

classical implementation of Grover's search

Amsterdam's experiment of Bhattacharya et al. (2002)

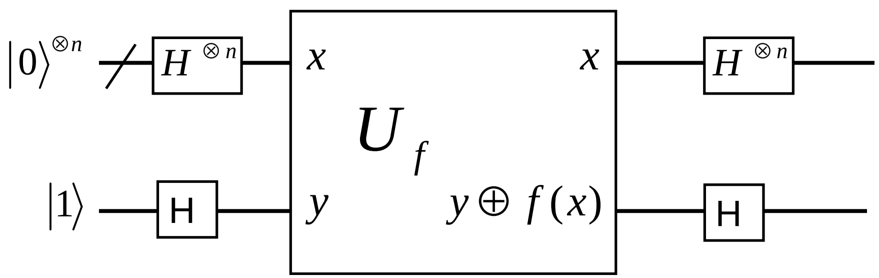


IAA – inversion about the average amplitude, $M_{1,2}$ – mirrors, $f_{1,2}$ – focal lengths

F – Fourier transform (instead of Hadamard transform) via lenses $L_{1,2}$

quantum DJ algorithm
is a common quantum subroutine

used in:
- Simon algorithm
- Grover algorithm
- Bernstein-Vazirani algorithm
- and others



Simon's problem (1994)

it is an oracle problem closely related to Shor's algorithm

GIVEN:

$f:\{0,1\}^n \to \{0,1\}^n$ – a 2-to-1 function such that

$$\forall \mathbf{x} \neq \mathbf{y}: \; f(\mathbf{x}) = f(\mathbf{y}) \Leftrightarrow \mathbf{y} = \mathbf{x} \oplus \mathbf{r},$$

$\mathbf{r}$ – a fixed n-bit string called the **function's period**

TASK:

find period $\mathbf{r}$.

How many oracle queries are required to find period r?

exponential number	classically
polynomial number	quantumly

Simon's algorithm - step by step

- initial state

$$|\psi_0\rangle = |0\rangle^{\otimes n}|0\rangle^{\otimes n} \equiv |\mathbf{0}\rangle|\mathbf{0}\rangle$$

- apply n Hadamard gates to the first n qubits:

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}\rangle|\mathbf{0}\rangle.$$

where $|\mathbf{x}\rangle \equiv |x_1, x_2, \cdots, x_n\rangle$

- apply quantum oracle:

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}\rangle|f(\mathbf{x})\rangle.$$

- measure the last n qubits and obtain a certain $f(\mathbf{x}') \in \{0,1\}^n$, which yields the ($n$-qubit) state:

$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}}(|\mathbf{x}'\rangle + |\mathbf{x}' \oplus \mathbf{r}\rangle).$$

- apply n Hadamard gates to the n qubits:

$$|\psi_4\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{\mathbf{y}\in\{0,1\}^n} \left[(-1)^{\mathbf{x}'\cdot\mathbf{y}} + (-1)^{(\mathbf{x}'\oplus\mathbf{r})\cdot\mathbf{y}}\right]|\mathbf{y}\rangle$$
$$= \frac{1}{\sqrt{2^{n-1}}} \sum_{\mathbf{r}\cdot\mathbf{y}=0} (-1)^{\mathbf{x}'\cdot\mathbf{y}}|\mathbf{y}\rangle.$$

- measure $|\psi_4\rangle$ to get $\mathbf{y}$ such that $\mathbf{r}\cdot\mathbf{y} = 0$.
- repeat the above steps a polynomial number of times to get, with high probability, n linearly-independent values $\mathbf{y} = \{y_1, y_2, \ldots, y_n\}$ such that $\mathbf{y}\cdot\mathbf{r} = \mathbf{r}$, which determines $\mathbf{r}$.

multiplicative order of an integer

$$k = ord(x,n) \equiv ord(x)$$

multiplicative order of x is the smallest integer k for which

$$1 = x^k \bmod n$$

Mathematica: MultiplicativeOrder[x,n]

example

$ord(8,21) = ?$

$8^1 \mod 21 = 8$

$8^2 \mod 21 = 64 \mod 21 = 64 - 3\cdot 21 = 1$

$\Rightarrow \quad ord(8,21) = 2$

another example

$$2^1 \mod 21 = 2$$
$$2^2 \mod 21 = 4$$
$$2^3 \mod 21 = 8$$
$$2^4 \mod 21 = 16$$
$$2^5 \mod 21 = 32 \mod 21 = 11$$
$$2^6 \mod 21 = 22 \mod 21 = 1$$

orders of all elements modulo 21

x =	1	2	4	5	8	10	11	13	16	17	19	20
ord(x,21) =	1	6	3	6	2	6	6	2	3	6	6	2

complexity of algorithms for order calculation

- exponential time using known classical algorithms
- polynomial time using quantum phase estimation (a part of Shor's algorithm)

Continued fractions (CF)

$$\boxed{a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{K + a_N}}} \equiv \{a_0, a_1, a_2, K, a_N\}}$$

How to calculate CF for number r ?

1. split r into integer part $[[r]]$ and fractional part $f = r - [[r]]$
2. stop if $f = 0$
3. calculate $1/f$ and return to step 1.

Note: The procedure will halt iff r is rational.

Example: CF for r=11/9

$$\boxed{\frac{11}{9} = 1 + \frac{2}{9} = 1 + \frac{1}{\frac{9}{2}} = 1 + \frac{1}{4+\frac{1}{2}} \equiv \{1, 4, 2\}}$$

Mathematica: ContinuedFraction[11/9] $\hookrightarrow$ {1,4,2}

Example: CF for 3.245

3	3.245 - 3 = 0.245	1 / 0.245 = 4.082
4	4.082 - 4 = 0.082	1 / 0.082 = 12.250
12	12.250 - 12 = 0.250	1 / 0.250 = 4.000
4	4.000 - 4 = 0.000	

$$3.245 = 3 + \frac{1}{4 + \frac{1}{12 + \frac{1}{4}}} = \{3, 4, 12, 4\}$$

Mathematica: ContinuedFraction[3245/1000] $\hookrightarrow$ {3, 4, 12, 4}

A convergent of CF

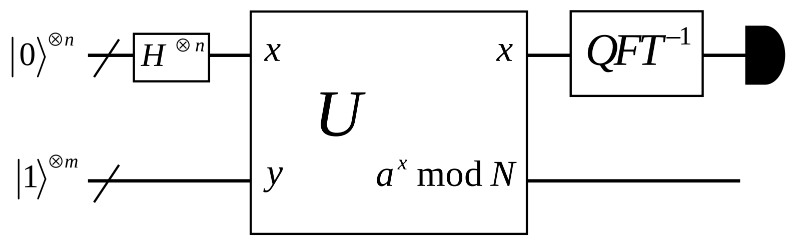
The nth convergent, denoted by $\{a_0, a_1, ..., a_n\}$,

is a truncated CF $x = \{a_0, a_1, ..., a_n, ..., a_N\}$.

Useful criterion for Shor's algorithm

$\left|\frac{p}{q} - x\right| < \frac{1}{2q^2} \quad \Rightarrow \quad \frac{p}{q}$ is a convergent of CF and $\mathrm{GCD}(p, q) = 1$

Shor's factorization algorithm



Basic steps of Shor's algorithm:

1. Hadamard transform
2. Modular exponentiation
3. Quantum Fourier transform
4. Measurement

Shor's algorithm to factorize an integer N

1. If N is even then return factor $f = 2$.
2. Test classically whether $N \neq a^b$.
3. Choose randomly an integer a ($1 < a < N$) and apply the Euclidean algorithm to check whether a and N are coprime, i.e. GCD$(a, N) = 1$
   If not then choose another a.

4. Prepare two registers:
   register #2 has $n_2 = \lceil \log_2 N \rceil$ qubits
   (this is the number of qubits to store N);
   register #1 has $n_1 = 2n_2$ qubits
   (in optimized versions of the algorithm, n_1 can be smaller).

5. Initialize both registers:

$$|\psi_1\rangle = |0\rangle^{\otimes n_1} |1\rangle^{\otimes n_2}$$

6. Apply Hadamard gates to register # 1:
   i.e. create an equally-weighted superposition

$$|\psi_2\rangle = \hat{H}^{\otimes n_1} |\psi_1\rangle = \frac{1}{\sqrt{N_1}} \sum_{x=0}^{N_1 - 1} |x, 15\rangle$$

   where $N_1 = 2^{n_1}$.

7. Apply modular exponential gate to register # 2:

$$|\psi_3\rangle = \hat{U}_{\text{mod.exp}} |\psi_2\rangle$$

$a^{R_1} \mod 15$

R_1	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	...	$\|N_1 - 1\rangle$
R_2	$\|a^0 \mod N\rangle$	$\|a^1 \mod N\rangle$	$\|a^2 \mod N\rangle$	...	$\|a^{N_1 - 1} \mod N\rangle$

8. Measure register #2 to get some state $|x'\rangle$:

$$|\psi_4\rangle = \mathcal{N}_2 \langle x' | \psi_3 \rangle$$

   where $\mathcal{N}$ is an (unimportant) renormalization constant.

9. Apply QFT† on the register # 1:

$$|\psi_5\rangle = QFT^\dagger |\psi_4\rangle$$

   and measure it.

10. Apply the classical method of continued fractions to find period r.

11. If r is even and $\frac{r}{2} \neq -1 (\mod N)$
    then calculate f =GCD$(a^{r/2} \pm 1, N)$
    If $f \neq 1$ or $f \neq N$ then return f.
    Otherwise repeat the algorithm.

How to factorize N=15?

1. choose x such that
   1<x<N-1, GCD(x,N)=1 e.g. x=11
2. find multiplicative order r=ord(x):
   11^1 11^2 11^3 11^4 11^5 11^6
   11 1 11 1 11 1 (mod N) so r=2
3. find y: y^2=1 mod N
   since x^r=1 mod N then $y=x^{r/2}$=11
4. calculate GCD(y+1,N)=GCD(12,15)=3
   GCD(y-1,N) =GCD(10,15)=5

so 15=3*5

Example 1: Factorize $N = 15$

1. N is odd $\Rightarrow$ OK
2. $N \neq a^b$ $\Rightarrow$ OK
3. let's, e.g., choose $a = 7$ (unlucky choice) and apply
   Euclidean algorithm to check whether a and N are coprime:
   GCD(7,15) = 1 $\Rightarrow$ OK
4. find the required dimension of registers (number qubits):
   register # 2: $n_2 = \lceil \log_2 N \rceil = \lceil 3.906 \rceil = 4$
   register # 1: $n_1 = 2n_2 = 8$
   Mathematica: Ceiling[Log[2, 15]] $\hookrightarrow$ 4
5. initialize both registers:
   $|\psi_1\rangle = |0\rangle^{\otimes n_1}|1\rangle^{\otimes n_2} = |00000000\rangle|1111\rangle \equiv |\mathbf{0}\rangle|15\rangle$
   Mathematica: 2^^1111 $\hookrightarrow$ 15

6. apply Hadamard gates to register # 1:
   i.e. create equally-weighted superposition

$$|\psi_2\rangle = \hat{H}^{\otimes n_1}|\psi_1\rangle = \frac{1}{\sqrt{N_1}}\sum_{x=0}^{N_1-1}|y, 15\rangle$$

   where $N_1 = 2^{n_1} = 256$

7. apply modular exponential gate to register # 2:
   $|\psi_3\rangle = \hat{U}_{\mathrm{mod.exp}}|\psi_2\rangle$
   $a^{R_1} \mod 15$

R_1	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert 2\rangle$	...	$\lvert 255\rangle$
R_2	$\lvert 7^0 \mod N\rangle = \lvert 1\rangle$	$\lvert 7^1 \mod N\rangle = \lvert 7\rangle$	$\lvert 7^2 \mod N\rangle = \lvert 49\rangle \equiv \lvert 4\rangle$	... ...	$\lvert 7^{255} \mod N\rangle = \lvert 13\rangle$

so *Mathematica:* PowerMod[a^x, 15]

R_1	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert 2\rangle$	$\lvert 3\rangle$	$\lvert 4\rangle$	$\lvert 5\rangle$	$\lvert 6\rangle$	$\lvert 7\rangle$	$\lvert 8\rangle$	$\lvert 9\rangle$	$\lvert 10\rangle$	$\lvert 11\rangle$	...
R_2	$\lvert 1\rangle$	$\lvert 7\rangle$	$\lvert 4\rangle$	$\lvert 13\rangle$	$\lvert 1\rangle$	$\lvert 7\rangle$	$\lvert 4\rangle$	$\lvert 13\rangle$	$\lvert 1\rangle$	$\lvert 7\rangle$	$\lvert 4\rangle$	$\lvert 13\rangle$	...

8. measure register #2:
   for example, we get the state $|13\rangle$:

R_1				$\lvert 3\rangle$				$\lvert 7\rangle$				$\lvert 11\rangle$	...
R_2				$\lvert 13\rangle$				$\lvert 13\rangle$				$\lvert 13\rangle$	...

   $|\psi_4\rangle = \mathcal{N}\ {}_2\langle 13|\psi_3\rangle = \mathcal{N}(|3\rangle_1 + |7\rangle_1 + |11\rangle_1 + \ldots)$
   where $\mathcal{N}$ is a renormalization constant

9. apply QFT† on the register # 1:
   $|\psi_5\rangle = QFT^\dagger|\psi_4\rangle = \frac{1}{2}(|0\rangle_1 - |64\rangle_1 + |128\rangle_1 - |192\rangle_1)$

10. apply the classical continued fraction method
    (which reduces to a trivial case now) to find the period r
    $\frac{64}{256} = \frac{1}{4}$ $\Rightarrow$ $r = 4$

11. r is even and $\frac{r}{2} \neq -1 \mod N$ $\Rightarrow$
    GCD($13^{r/2} + 1, 15$) = GCD($13^2 + 1, 15$)
    = GCD($169 + 1, 15$) = GCD($17 \times 2 \times 5, 3 \times 5$) = 5

    GCD($13^{r/2} - 1, 15$) = GCD($168, 15$) = 3
    these are the sought factors :-)

12. final test $3 \times 5 = 15$ $\Rightarrow$ OK

lucky, unlucky and bad choices of a modulo N=15

condition: GCD(a,N)=1

```
 a  a^2  a^3  a^4  ...                               a^14(mod N)
 2    4    8    1  2  4  8  1  2  4  8  1  2            4 unlucky
 3    9   12    6  3  9 12  6  3  9 12  6  3            9 wrong
 4    1    4    1  4  1  4  1  4  1  4  1  4            1 lucky
 5   10    5   10  5 10  5 10  5 10  5 10  5           10 wrong
 6    6    6    6  6  6  6  6  6  6  6  6  6            6 wrong
 7    4   13    1  7  4 13  1  7  4 13  1  7            4 unlucky
 8    4    2    1  8  4  2  1  8  4  2  1  8            4 ...
 9    6    9    6  9  6  9  6  9  6  9  6  9            6
10   10   10   10 10 10 10 10 10 10 10 10 10           10
11    1   11    1 11  1 11  1 11  1 11  1 11            1
12    9    3    6 12  9  3  6 12  9  3  6 12            9
13    4    7    1 13  4  7  1 13  4  7  1 13            4
14    1   14    1 14  1 14  1 14  1 14  1 14            1
```

a=2, 7, 8, 13	$\Rightarrow$	long period	$\Rightarrow$	unlucky choice	$\Rightarrow$	harder factorization
a=4, 11, 14	$\Rightarrow$	short period	$\Rightarrow$	lucky choice	$\Rightarrow$	easier factorization
a=3,5,6,9,10,12	$\Rightarrow$	GCD$(x, N) \neq 1$	$\Rightarrow$	bad choice	$\Rightarrow$	excluded

Example 2: Factorize again $N = 15$ but for $a = 11$

1–2. *ditto*

3. we choose $a = 11$ (lucky choice)

   GCD(11,15) = 1 $\quad\Rightarrow\quad$ OK

4–6. *ditto*

7. apply modular exponential gate to register # 2:

   $|\psi_3\rangle = \hat{U}_{\text{mod.exp}}|\psi_2\rangle$

   $a^{R_1} \mod 15$

R_1	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	...	$\|255\rangle$
R_2	$\|11^0 \mod N\rangle = \|1\rangle$	$\|11^1 \mod N\rangle = \|11\rangle$	$\|11^2 \mod N\rangle = \|121\rangle \equiv \|1\rangle$	... ...	$\|11^{255} \mod N\rangle = \|11\rangle$

so

R_1	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	$\|3\rangle$	$\|4\rangle$	$\|5\rangle$	$\|6\rangle$	$\|7\rangle$	$\|8\rangle$	...
R_2	$\|1\rangle$	$\|11\rangle$	$\|1\rangle$	$\|11\rangle$	$\|1\rangle$	$\|11\rangle$	$\|1\rangle$	$\|11\rangle$	$\|1\rangle$	...

8. measure register #2:

   for example, we get state $|11\rangle$:

R_1		$\|1\rangle$		$\|3\rangle$		$\|5\rangle$	...
R_2		$\|11\rangle$		$\|11\rangle$		$\|11\rangle$	...

   $|\psi_4\rangle = \mathcal{N}\ {}_2\langle 11|\psi_3\rangle = \mathcal{N}(|1\rangle_1 + |3\rangle_1 + |5\rangle_1 + ...)$

   where $\mathcal{N}$ is a renormalization constant

9. apply QFT† on the register # 1:

   $|\psi_5\rangle = QFT^\dagger|\psi_4\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1 + |128\rangle_1)$

10. apply the classical continued fraction method

    to find period r

    $\frac{128}{256} = \frac{1}{2} \quad\Rightarrow\quad r = 2$

11. r is even and $\frac{r}{2} \neq -1 \mod N \quad\Rightarrow$

GCD($11^{r/2}$ + 1, 15) = GCD(11 + 1, 15) = GCD(3× 4, 3× 5) = 3

GCD($11^{r/2}$-1, 15) = GCD(10, 15) = 5

which are the sought factors.

Note 1:

To find period r, one usually has to apply the complete classical continued fraction method.

Note 2:

Shor's algorithm resembles Simon's algorithm.

Actually, Shor has found his algorithm by generalizing Simon's algorithm, i.e. by replacing Simon's Hadamard transforms (Fourier transform over Z_2^n) by Fourier transform over Z_N.

Example: Find period r from $\frac{65}{256}$

Mathematica:

```
x = 65/256;
criterion[a_, b_, x_] := Abs[a/b - x] < 1/(2 b^2);
ContinuedFraction[x] // InputForm
{0, 3, 1, 15, 4}
```

$$\{0,3,1,15,4\} \equiv 0+\frac{1}{3+\frac{1}{1+\frac{1}{15+\frac{1}{4}}}}=\frac{65}{256}$$

```
FromContinuedFraction[{0, 3, 1, 15, 4}]
65/256
```


1st convergent of the continued fraction

$$\{0,3\} \equiv 0+\frac{1}{3}=\frac{1}{3}\equiv\frac{a}{b}$$

$$\Rightarrow \quad \left|\frac{a}{b}-x\right|=\left|\frac{1}{3}-\frac{65}{256}\right|=0.079\cdots \not< \frac{1}{2b^2}=\frac{1}{18}=0.055\cdots$$

```
FromContinuedFraction[{0, 3}]
1/3
criterion[1, 3, x]
False
```

$\Rightarrow$ PERIOD $r \neq 3$

2nd convergent of the continued fraction

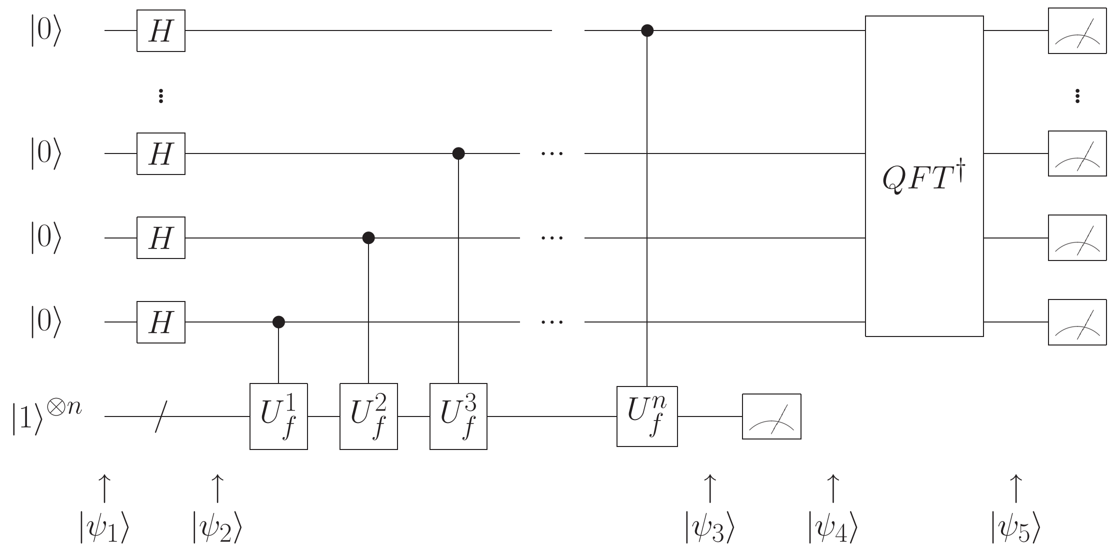
$$\{0,3,1\} \equiv 0+\frac{1}{3+\frac{1}{1}}=\frac{1}{4}\equiv\frac{a}{b}$$

$$\Rightarrow \quad \left|\frac{a}{b}-x\right|=\left|\frac{1}{4}-\frac{65}{256}\right|=\frac{1}{256}<\frac{1}{2b^2}=\frac{1}{32} \quad \text{TRUE}$$

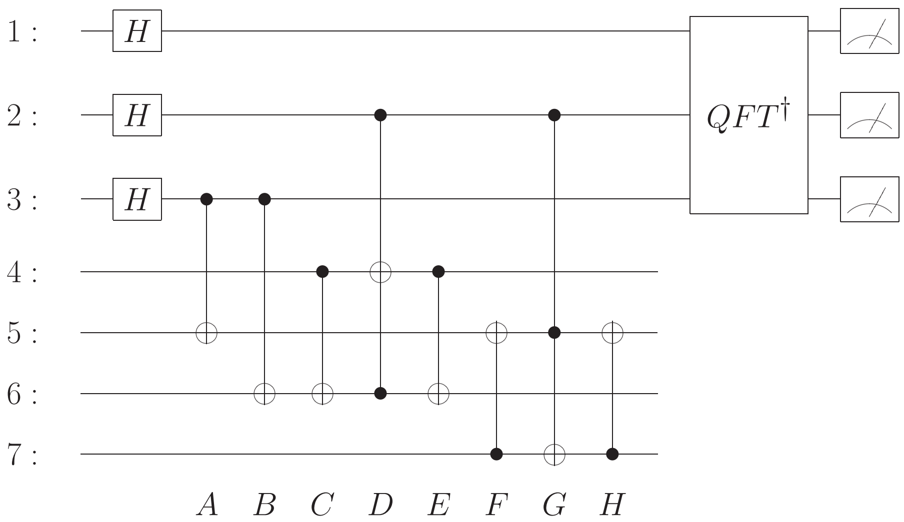
```
FromContinuedFraction[{0, 3, 1}]
1/4
criterion[1, 4, x]
True
```

$\Rightarrow$ PERIOD $r = 4$

Quantum circuit for Shor's factorization algorithm

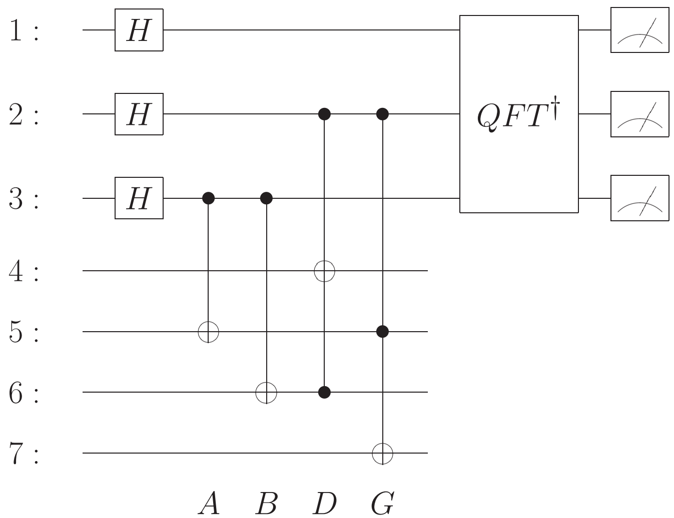


7-qubit circuit for Shor's factorization of $N = 15$



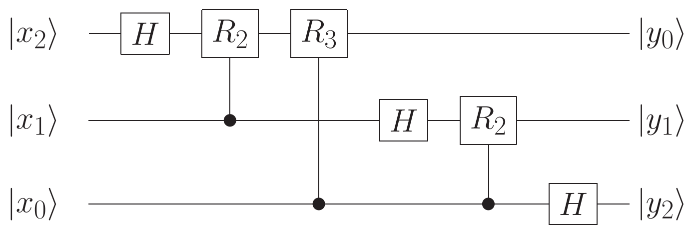
optimized version of the 7-qubit circuit for Shor's factorization of $N = 15$

(gates C, E, F, H are removed)

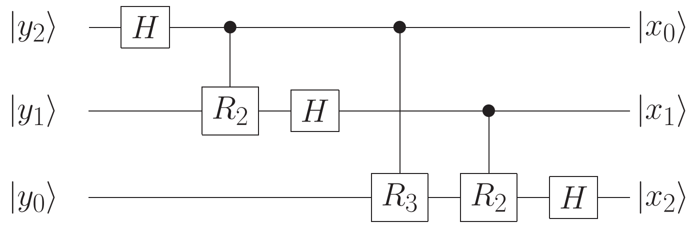


Quantum Fourier transform and its inverse for 3 qubits

QFT



QFT^{-1}=QFT†



where the rotations are $R_2 = R(90^0), R_3 = R(45^0)$

Outline

1. Generalized projective measurements
2. Positive operator valued measure (POVM)
3. Kraus representation
4. Damping channels for a single qubit
5. Imperfect photocount detectors
6. Bell-state and GHZ-state analyzers
7. Fidelity and other measures of quality of the state generation
8. Entanglement measures

von Neumann-type projective measurement

is represented by complete, orthonormal set of states $|\mu\rangle$

$$P_\mu = \mathrm{Tr}\{|\mu\rangle\langle\mu|\rho_{\mathrm{sys}}\}$$

where

P_μ – probability that the system is in state $|\mu\rangle$

= probability of the measurement outcome μ

$|\mu\rangle\langle\mu|$ – measurement operator or projection operator

also called the **projection valued (PV) measure**

- measurement operators, corresponding to nonorthogonal states, do not commute and are therefore not simultaneously observable

Generalized projective measurement

- Let's prepare an **auxiliary quantum system (ancilla)** in a known state $\hat{\rho}_{\mathrm{aux}}$

The **combined, uncorrelated state** of the original quantum system and the ancilla is

$$(\rho_{\mathrm{sys}} \otimes \rho_{\mathrm{aux}})_{mM,nN} = (\rho_{\mathrm{sys}})_{mn}(\rho_{\mathrm{aux}})_{MN}$$

A maximal test is then performed in the combined Hilbert space $\mathcal{K}$.

Different outcomes correspond to orthogonal and complete projectors $|\mu\rangle\langle\mu|$

- **probability of outcome** μ:

$$P_\mu = \mathrm{Tr}[|\mu\rangle\langle\mu|(\rho_{\mathrm{sys}} \otimes \rho_{\mathrm{aux}})] = \sum_{m,n,M,N} (|\mu\rangle\langle\mu|)_{mM,nN}(\rho_{\mathrm{sys}})_{mn}(\rho_{\mathrm{aux}})_{MN}$$

which be rewritten as

$$P_\mu = \mathrm{Tr}(A_\mu \rho_{\mathrm{sys}})$$

where

$$(A_\mu)_{mn} = \sum_{M,N} (|\mu\rangle\langle\mu|)_{mM,nN}(\rho_{\mathrm{aux}})_{MN}$$

positive operator valued measures (POVM) = set of A_μ's

which are positive Hermitian operators acting on original Hilbert space

$$\sum_\mu A_\mu = 1$$

- probability that a quantum system is in a particular state is given by the expectation value of the POVM operator corresponding to that state

$$P_\mu = \mathrm{Tr}(A_\mu \rho_{\mathrm{sys}})$$

Advantages of POVM over PV measures

- the number of **available outcomes** may differ from the number of available preparations (of a given state) and the dimension of the Hilbert space.
- POVM allow the possibility of measurement outcomes associated with **nonorthogonal states**.
- POVM allow extraction of **more mutual information** that can the usual von Neumann-type projective measurement

How to distinguish conclusively between two non-orthogonal states?

(at leat sometimes)

Cryptographic example of POVM

non-orthogonal linear polarization states $|u\rangle$ and $|v\rangle$

$$\langle u|v\rangle = \cos\theta$$

where θ the angle between polarization vectors

Can you distinguish whether qubit is in state $|u\rangle$ or $|v\rangle$?

general state

$$|\psi\rangle = \alpha|u\rangle + \beta|v\rangle$$

POVM operators

are not projective measurements

$$A_u = \frac{1-|u\rangle\langle u|}{1+\langle u|v\rangle}, \quad A_v = \frac{1-|v\rangle\langle v|}{1+\langle u|v\rangle}$$

$$A_? = 1 - A_u - A_v \quad \Rightarrow \quad \text{inconclusive measurement}$$

probabilities of measurements

$$P_i = \langle\psi|A_i|\psi\rangle$$

$$\Rightarrow \quad P_u = |\alpha|^2(1-\cos\theta), \quad P_v = |\beta|^2(1-\cos\theta), \quad P_? = |\alpha+\beta|^2\cos\theta$$

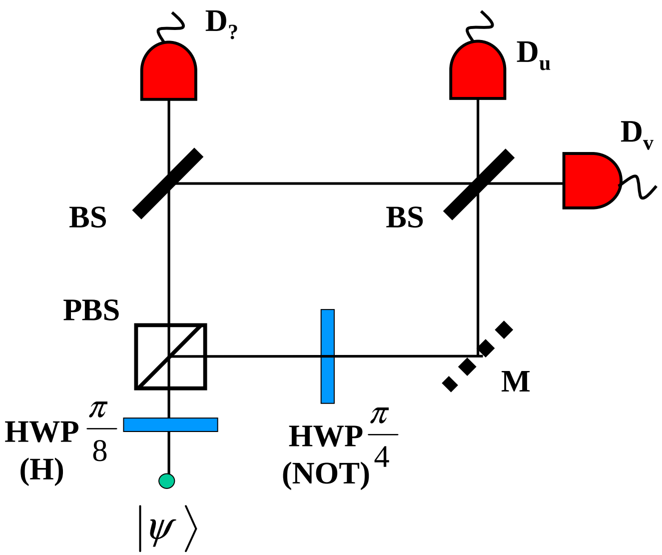
special input states

$$|\psi\rangle = |u\rangle \quad \Rightarrow \quad P_v = 0 \quad \Rightarrow \quad \text{detector } D_v \text{ will not click}$$

$$|\psi\rangle = |v\rangle \quad \Rightarrow \quad P_u = 0 \quad \Rightarrow \quad \text{detector } D_u \text{ will not click}$$

an optical implementation of POVM

optical implementation of POVM



Neumark's theorem

One can extend the Hilbert space $\mathcal{H}$ of states, in which the A_μ are defined, in such a way that there exists, in the extended space $\mathcal{K}$, a set of orthogonal and complete projectors $|\mu\rangle\langle\mu|$ such that A_μ is the result of projecting $|\mu\rangle\langle\mu|$ from $\mathcal{K}$ into $\mathcal{H}$.

physical implication

There always exists an experimentally realizable procedure generating any desired POVM represented by given matrices A_μ

most general measurement operator

It is also generally thought that a POVM belongs to the most general test to which a quantum system may be subjected.

analogy

a pure state of the bipartite system AB may behave like
a mixed states when we observe subsystem A alone,

similarly

an orthonormal measurement of the system AB may be
a nonorthonormal POVM on A alone

Kraus representation = operator sum representation

an elegant representation to describe open system dynamics

basic idea

- The final state of an open system cannot be described by a unitary transformation of the initial state.
- So let's analyze evolution of **both the system and environment**:

$$\rho(0) = \rho_S(0)\otimes\rho_E(0) \longrightarrow \rho_{SE}(t) = U(t)\rho_S(0)\otimes\rho_E(0)U^\dagger(t)$$

- **reduced density matrix**

$$\rho_S(t) = \mathrm{Tr}_E\,\{\rho_{SE}(t)\} = \sum_{\{k_i\}}\langle\{k_i\}|\rho_{SE}(t)|\{k_i\}\rangle$$

where $|\{k_i\}\rangle \equiv |k_1\cdots k_i\cdots\rangle = \Pi_i \otimes |k_i\rangle$
is an orthonormal basis of the environment Hilbert space

- alternatively, the evolution can be given in the so-called **Kraus representation**

$$\rho_S(t) = \sum_{k=0}^{\infty} A_k(t)\rho_S(0)A_k^\dagger(t)$$

in terms of **Kraus operators**

$$A_k(t) = \sum_{\{k_i\}}^{k}{}' \langle\{k_i\}|U(t)|\{0\}\rangle$$

where $\sum'$ stands for summation under the condition $\sum_i k_i = k$

- **completeness relation**

$$\sum_k A_k^\dagger(t)A_k(t) = I$$

- **drawback**

it seems extremely difficult to use K.r. if the environment is at $T > 0$

Example of Kraus representation

depolarizing channel

i.e. the qubit remains intact with probability $1-p$

and error (bit flip and/or phase flip) occurs with probability p

evolution of single qubit in depolarizing channel

$$U_{SE} : |\psi\rangle_S \otimes |0\rangle_E \rightarrow \sqrt{1-p}|\psi\rangle_S \otimes |0\rangle_E + \sqrt{\frac{p}{3}}\Big[\sigma_x|\psi\rangle_S \otimes |1\rangle_E + \sigma_y|\psi\rangle_S \otimes |2\rangle_E + \sigma_z|\psi\rangle_S \otimes |3\rangle_E\Big]$$

Kraus operators

$$A_\mu = {}_E\langle\mu|U_{SE}|0\rangle_E$$

so

$$A_0 = \sqrt{1-p}, \quad A_1 = A_2 = A_3 = \frac{p}{3}$$

POVM from Kraus representation

POVM modifies a density matrix as follows

$$\rho_s \rightarrow \sum_\mu \sqrt{F_\mu}\rho_s\sqrt{F_\mu}$$

where

$$F_\mu = A_\mu^\dagger A_\mu$$

and A_μ are **Kraus operators**

three types of errors

1. **bit flip error**

$$|0\rangle \rightarrow |1\rangle, \quad |1\rangle \rightarrow |0\rangle$$
$$|\psi\rangle \rightarrow \hat{\sigma}_x|\psi\rangle$$

2. **phase flip error**

$$|0\rangle \rightarrow |0\rangle, \quad |1\rangle \rightarrow -|1\rangle$$
$$|\psi\rangle \rightarrow \hat{\sigma}_z|\psi\rangle$$

3. **both errors**

$$|0\rangle \rightarrow i|1\rangle, \quad |1\rangle \rightarrow -i|0\rangle$$
$$|\psi\rangle \rightarrow \hat{\sigma}_y|\psi\rangle$$

where the σ_k are the **Pauli operators**

$$\hat{\sigma}_x \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \hat{\sigma}_y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \hat{\sigma}_z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

damping channels for a single qubit

1. amplitude-damping channel

$$|0\rangle_S|0\rangle_E \rightarrow |0\rangle_S|0\rangle_E$$

$$|1\rangle_S|0\rangle_E \rightarrow \sqrt{1-p}|1\rangle_S|0\rangle_E + \sqrt{p}|0\rangle_S|1\rangle_E$$

2. phase-damping channel

$$|0\rangle_S|0\rangle_E \rightarrow \sqrt{1-p}|0\rangle_S|0\rangle_E + \sqrt{p}|0\rangle_S|1\rangle_E$$

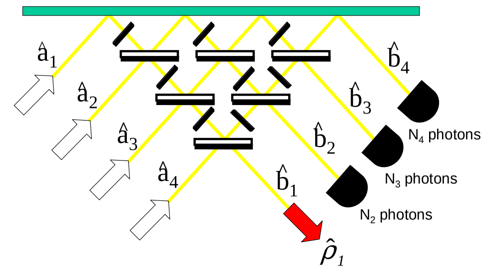
$$|1\rangle_S|0\rangle_E \rightarrow \sqrt{1-p}|1\rangle_S|0\rangle_E + \sqrt{p}|1\rangle_S|2\rangle_E$$

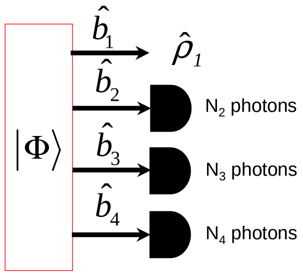
- it is a „caricature" model of decoherence in real systems
- no bit flip in system!

3. depolarizing channel

$$|\psi\rangle_S|0\rangle_E \rightarrow \sqrt{1-p}|\psi\rangle_S|0\rangle_E + \sqrt{\frac{p}{3}}\left[\sigma_x|\psi\rangle_S|1\rangle_E + \sigma_y|\psi\rangle_S|2\rangle_E + \sigma_z|\psi\rangle_S|3\rangle_E\right]$$

conditional measurements using imperfect photocounters





$$\hat{\rho}_1 = \mathcal{N}\,\mathrm{Tr}_{(b_2,b_3,b_4)}\left(\hat{\Pi}^{(b_2)}_{N_2}\hat{\Pi}^{(b_3)}_{N_3}\hat{\Pi}^{(b_4)}_{N_4}|\Phi\rangle\langle\Phi|\right)$$

$\hat{\Pi}^{(b_k)}_{N_k}$	POVM for the kth imperfect photocounter detecting N_k photons
$\lvert\Phi\rangle$	four-mode state before the measurements
$\hat{\rho}_1$	single-mode state after the measurements
$\mathcal{N}$	renormalization constant

POVM for photocount detectors (I)

- **Perfectly-Resolving Photon Counter**

$$\hat{\Pi}_N = \sum_{m=0}^{\infty}\sum_{n=0}^{N} e^{-\nu}\frac{\nu^{(N-n)}}{(N-n)!}\eta^n(1-\eta)^{m-n}C_n^m|m\rangle\langle m|$$

η – inefficiency

ν – dark count rate

- **Conventional Photon Counter (CPC)**

$$\hat{\Pi}_0^c = \sum_{m=0}^{\infty} e^{-\nu}(1-\eta)^m|m\rangle\langle m| \quad \text{(No clicks)}$$

$$\hat{\Pi}_1^c = 1-\hat{\Pi}_0^c \quad \text{(Click)}$$

• Dark count rate ~ $100-1000\ \mathrm{s}^{-1}$

POVM for photocount detectors (II)

- **single-photon counter**

$$\hat{\Pi}_0^{vl} = \sum_{m=0}^{\infty} e^{-\nu}(1-\eta)^m|m\rangle\langle m| \quad \text{(no clicks)}$$

$$\hat{\Pi}_1^{vl} = \sum_{m=0}^{\infty}\sum_{n=0}^{1} e^{-\nu}\frac{\nu^{(1-n)}}{(1-n)!}\eta^n(1-\eta)^{m-n}C_n^m|m\rangle\langle m| \quad \text{(1 click)}$$

$$\hat{\Pi}_2^{vl} = 1-\hat{\Pi}_0^{vl}-\hat{\Pi}_1^{vl} \quad \text{(2 clicks)}$$

• high dark count rate ~ $10^4\ \mathrm{s}^{-1}$

Photocounters (photon count detectors)

- **Si APD = Si avalanche photodiode** (working in Geiger mode)

$\eta \sim 70 - 80\%$

$F_{\text{noise}} \geq 2$ $\Rightarrow$ relatively high noise $\Rightarrow$ useless for QC

- **PMT = photomultiplier tube**

$\eta < 25\%$ for detection of single photon

$\eta \sim 6\%$ for detection of two photons

- **SSPM = solid state photomultiplier**

$\eta \sim 70 - 80\%$

$F_{\text{noise}} = 1$ $\Rightarrow$ basically noise free

- **VLPC = visible light photon counters**

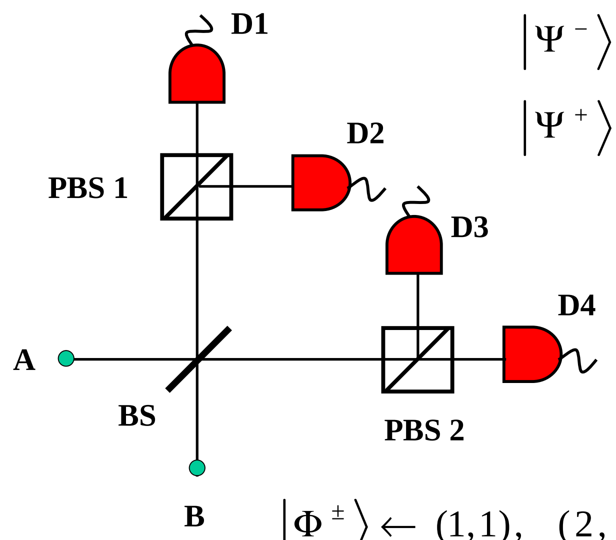
with noise free avalanche photomultiplication

$\eta \sim 88\%$ for detection of single photon

$\eta \sim 47\%$ for detection of two photons

$\tau \sim 2ns$ $\Rightarrow$ small resolution time (for detection of two photons)

Bell-state analyzer (1)



$|\Psi^-\rangle \leftarrow (1,4)$ or $(2,3)$

$|\Psi^+\rangle \leftarrow (1,3)$ or $(2,4)$

$|\Phi^\pm\rangle \leftarrow (1,1),\ (2,2),\ (3,3)$, or $(4,4)$

Bell-state and GHZ-state analyzers

- How to discriminate between the optical Bell states?

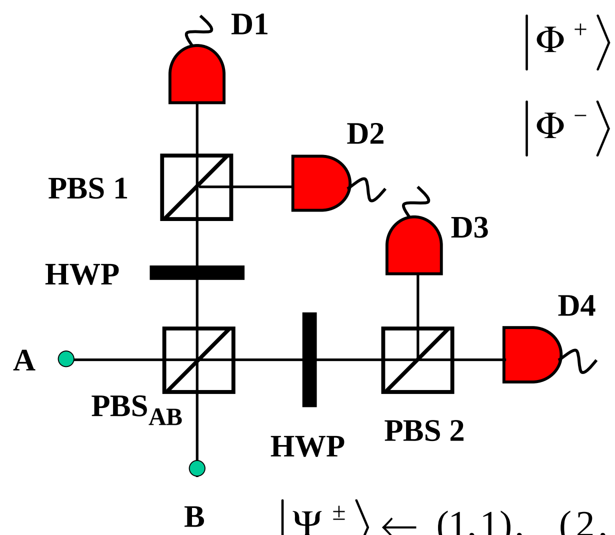
$$|\Psi^\pm\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}$$
$$|\Phi^\pm\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}$$

- Do they exist perfect linear Bell-state analyzers?

  Is it possible to unambiguously discriminate between all the Bell states using only linear optics?

- How to distinguish experimentally the GHZ states?

Bell-state analyzer (2)



$|\Phi^+\rangle \leftarrow (1,4)$ or $(2,3)$

$|\Phi^-\rangle \leftarrow (1,3)$ or $(2,4)$

$|\Psi^\pm\rangle \leftarrow (1,1),\ (2,2),\ (3,3)$, or $(4,4)$

What Bell states can uniquely be distinguished in the (Pan-Zeilinger) analyzer?

notation: particles A,B; modes 1,2

1. general input state

$$|\psi_{in}\rangle = \alpha|H_A\rangle|H_B\rangle + \beta|H_A\rangle|V_B\rangle + \gamma|V_A\rangle|H_B\rangle + \delta|V_A\rangle|V_B\rangle$$

2. state after PBS$_{AB}$

if horizontal (vertical) polarization component is transmitted (reflected) then

$$|\psi\rangle = \alpha|H_{A2}\rangle|H_{B1}\rangle + \beta|H_{A2}\rangle|V_{B2}\rangle + \gamma|V_{A1}\rangle|H_{B1}\rangle + \delta|V_{A1}\rangle|V_{B2}\rangle$$

3. indistinguishability of photons

implies that we can omit subscripts A, B:

$$\begin{aligned}|\psi\rangle &= \alpha|H_1\rangle|H_2\rangle + \beta|H_2\rangle|V_2\rangle + \gamma|V_1\rangle|H_1\rangle + \delta|V_1\rangle|V_2\rangle \\ &= \frac{1}{\sqrt{2}}(\alpha+\delta)|\Phi^+_{\text{two}}\rangle + \frac{1}{\sqrt{2}}(\alpha-\delta)|\Phi^-_{\text{two}}\rangle + \frac{1}{\sqrt{2}}(\beta+\gamma)|\Psi^+_{\text{one}}\rangle + \frac{1}{\sqrt{2}}(\beta-\gamma)|\Psi^-_{\text{one}}\rangle\end{aligned}$$

where

$$|\Phi^\pm_{\text{two}}\rangle = \frac{1}{\sqrt{2}}\Big(|H_1\rangle|H_2\rangle \pm |V_1\rangle|V_2\rangle\Big), \quad |\Psi^\pm_{\text{one}}\rangle = \frac{1}{\sqrt{2}}\Big(|H_1\rangle|V_1\rangle \pm |V_2\rangle|H_2\rangle\Big)$$

4. state after quarter-wave plates and detection

- **quarter-wave plates** change polarizations as follows

$$|H_i\rangle \to \frac{1}{\sqrt{2}}(|H_i\rangle + |V_i\rangle), \quad |V_i\rangle \to \frac{1}{\sqrt{2}}(|H_i\rangle - |V_i\rangle)$$

- **notation**: $D_1 \equiv D_{H1}, \quad D_2 \equiv D_{V1}, \quad D_3 \equiv D_{V2}, \quad D_4 \equiv D_{H2}$
- **case 1:**

$$|\Phi^+_{\text{two}}\rangle \to |\Phi^+_{\text{two}}\rangle = \frac{1}{\sqrt{2}}\Big(|H_1\rangle|H_2\rangle + |V_1\rangle|V_2\rangle\Big)$$

then photons are detected in D1 and D4 or D2 and D3

- **case 2:**

$$|\Phi^-_{\text{two}}\rangle \to |\Psi^+_{\text{two}}\rangle = \frac{1}{\sqrt{2}}\Big(|H_1\rangle|V_2\rangle + |V_1\rangle|H_2\rangle\Big)$$

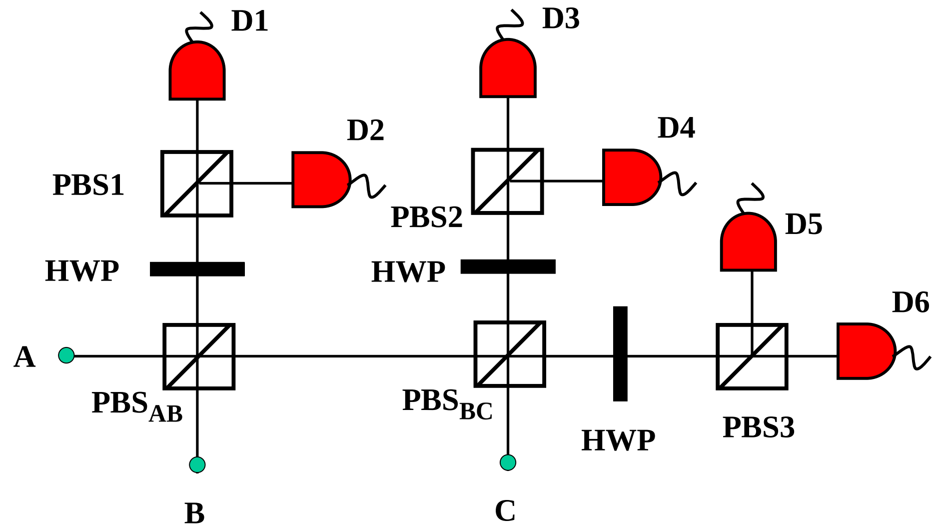
then photons are detected in D1 and D3 or D2 and D4

- **cases 3,4:**

$$|\Psi^+_{\text{one}}\rangle \to \frac{1}{2}\Big(|H_1\rangle|H_1\rangle \pm |H_2\rangle|H_2\rangle - |V_1\rangle|V_1\rangle \mp |V_2\rangle|V_2\rangle\Big)$$

then both photons are detected in either D1, or D2, or D3, or D4

GHZ-state analyzer



polarization GHZ states

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}\Big(|H\rangle|H\rangle|H\rangle + |V\rangle|V\rangle|V\rangle\Big)$$

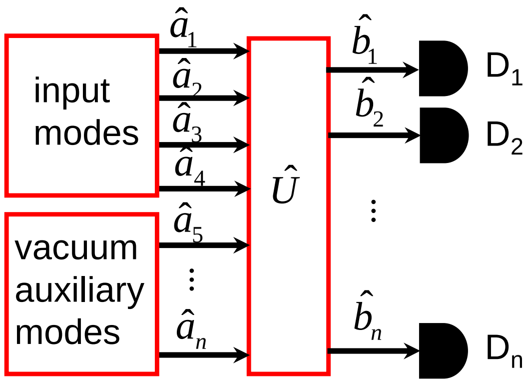
$$|\Psi^\pm_1\rangle = \frac{1}{\sqrt{2}}\Big(|V\rangle|H\rangle|H\rangle + |H\rangle|V\rangle|V\rangle\Big)$$

$$|\Psi^\pm_2\rangle = \frac{1}{\sqrt{2}}\Big(|H\rangle|V\rangle|H\rangle + |V\rangle|H\rangle|V\rangle\Big)$$

$$|\Psi^\pm_3\rangle = \frac{1}{\sqrt{2}}\Big(|H\rangle|H\rangle|V\rangle + |V\rangle|V\rangle|H\rangle\Big)$$

- **the Pan-Zeilinger analyzer discriminates between only two ($|\Phi^\pm\rangle$) among 2^N GHZ states**

Not complete linear Bell-state analyzer



probability to discriminate unambiguously between all the Bell states is

$$P_{\text{success}} \leq \frac{1}{2}$$

[Calsamiglia i Lütkenhaus, 2000]

Do they exist perfect Bell-state linear analyzers?

No-go theorem:

There is no perfect Bell state linear analyzer on two qubits in polarization entanglement without conditional measurements.

Calsamiglia-Lütkenhaus theorem:

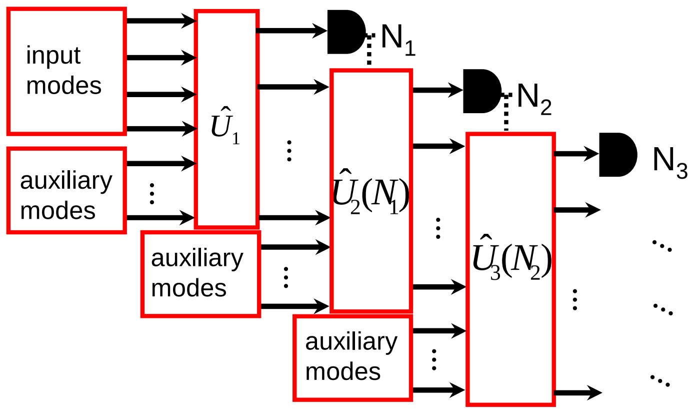
Within this subclass it is not possible to discriminate unambiguously four equiprobable Bell states with a probability higher than 50%.

Why no-go?

Linear optical elements can provide any arbitrary unitary mapping only over creation operators, not over a general input state.

Complete linear Bell-state analyzer

- based on conditional measurements



$$P_{\text{success}} = 1 - \frac{1}{1 + f(N_{\text{ph}}, N_{\text{cm}})} \to 1$$

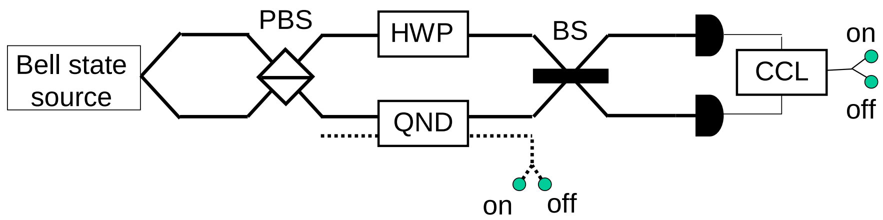
where N_{cm} – number of conditional measurements
N_{ph} – number of entangled photons in auxiliary modes

Complete nonlinear Bell-state analyzer

[Paris et al. (2000)]

based on

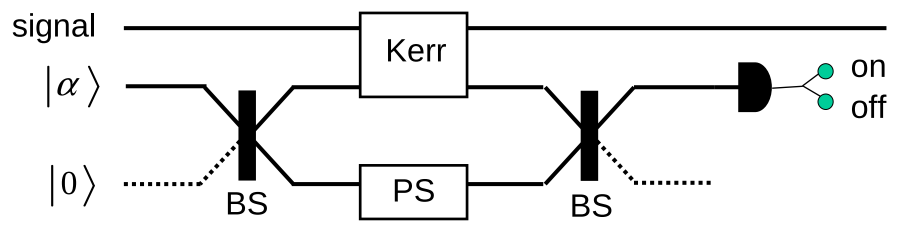
nonlinear Mach-Zehnder interferometer



Key: QND – quantum non-demolition detector,
CCL – classical coincidence & logic,
HWP – half-wave plate,
(P)BS – (polarization) beam splitter.

Bell state	QND	CCL
$\vert\Psi^+\rangle$	off	off
$\vert\Psi^-\rangle$	off	on
$\vert\Phi^+\rangle$	on	off
$\vert\Phi^-\rangle$	on	on

QND – Fock filter



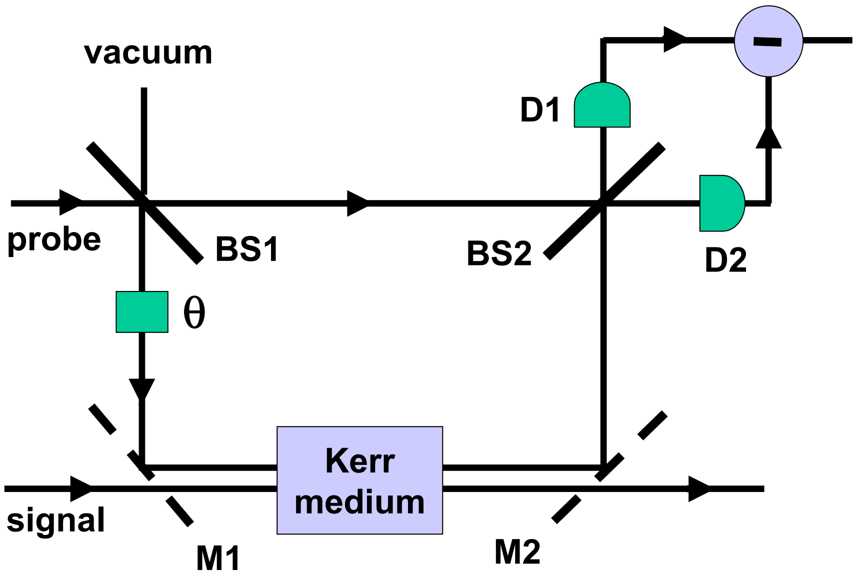
Key: Kerr nonlinear medium described by 3rd order susceptibility $\chi^{(3)}$

$|\alpha\rangle$ – strong coherent field

PS – phase shifter

QND measurement does not destroy coherence of the signal state, but only adds extra phase, which can easily be corrected.

Kerr effect and QND



Measures of quality of the state generation

1. Fidelity

= Uhlmann's transition probability for mixed states

$$F(\hat{\rho}_{\rm exp}, \hat{\rho}_{\rm th}) = \left\{ \mathrm{Tr} \left[\sqrt{\sqrt{\hat{\rho}_{\rm th}} \hat{\rho}_{\rm exp} \sqrt{\hat{\rho}_{\rm th}}} \right] \right\}^2$$

$\hat{\rho}_{\rm exp}$ – density matrix for the experimentally generated state

$\hat{\rho}_{\rm th}$ – theoretically predicted density matrix

2. Bures distance

a measure of discrepancy between $\hat{\rho}_{\rm exp}$ and $\hat{\rho}_{\rm th}$:

$$D_B(\hat{\rho}_{\rm exp}||\hat{\rho}_{\rm th}) = 2 - 2\sqrt{F(\hat{\rho}_{\rm exp}, \hat{\rho}_{\rm th})}$$

- it satisfies the usual metric properties including symmetry

$$D_B(\hat{\rho}_{\rm exp}||\hat{\rho}_{\rm th}) = D_B(\hat{\rho}_{\rm th}||\hat{\rho}_{\rm exp})$$

3. Quantum relative entropy = Kullback-Leibler 'distance'

$$S(\sigma||\rho) = \mathrm{Tr}\,(\sigma \lg \sigma - \sigma \lg \rho)$$

it is not a true metric since

$$S(\sigma||\rho) \neq S(\rho||\sigma)$$

4. MaxLik parameters

- used by us in the tomographic reconstruction of physical density matrices

5. Relative entropy of entanglement

minimum of the quantum relative entropy

over set $\mathcal{D}$ of all separable states ρ:

$$E(\sigma) = \min_{\rho \in \mathcal{D}} S(\sigma||\rho) = S(\sigma||\bar{\rho})$$

$\bar{\rho}$ is the separable state closest to σ.

Criteria for a good entanglement measure

ρ – the density matrix of a given state

C1. $E(\rho) \geq 0$

$E(\rho) = 0$ for an **unentangled state**

$E(\rho) = 1$ for a **Bell state**

C2. local unitary transformations $U_A \otimes U_B$ do not change $E(\rho)$

C3. LOCC operations cannot increase $E(\rho)$

C4. Entanglement is **convex** under discarding information:

$\sum_i p_i E(\rho_i) \geq E(\sum_i p_i \rho_i)$

i.e., mixing cannot increase $E(\rho)$

C5.* $E(\rho)$ should reduce to the entropy of entanglement for a **pure state**

Measures of entanglement

- entanglement of formation E_F
- entanglement cost $E_C = \lim_{n\to\infty} \frac{E_F(\rho^{\otimes n})}{n}$
- relative entropy of entanglement E_R
- entanglement of distillation E_D
- $\cdots$

for pure states

$$\boxed{E_F = E_C = E_R = E_D}$$

for mixed states

$$\boxed{E_F \geq E_C \geq E_R \geq E_D}$$

Entanglement of formation

[Bennett, DiVincenzo, Smolin, and Wootters, PRA'96]

It is the minimized average entanglement of any ensemble of pure states $|\psi_i\rangle$ realizing $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$:

$$E_F(\rho) = \min_{p_i,\psi_i} \sum_i p_i E(|\psi_i\rangle\langle\psi_i|)$$

Special case

For two qubits [Wootters, PRL'98]

$$E_F(\rho) = H\left(\tfrac{1}{2}[1 + \sqrt{1 - C^2(\rho)}]\right)$$

in terms of the **concurrence**

$$C(\rho) = \max\{0, \sqrt{\lambda_1} - \sqrt{\lambda_2} - \sqrt{\lambda_3} - \sqrt{\lambda_4}\}$$

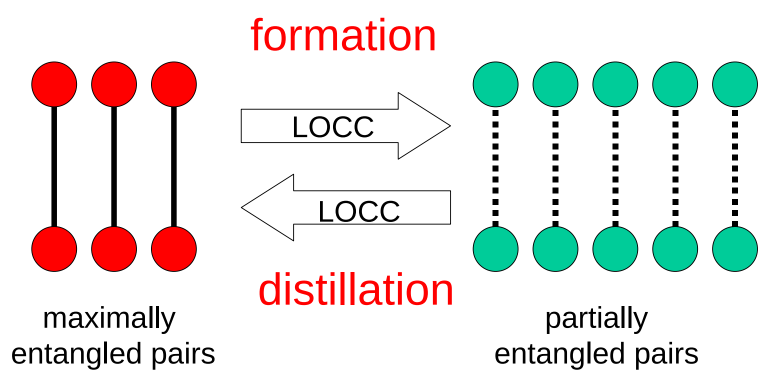
where λ_i's are in nonincreasing order the eigenvalues of

$$\rho(\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y)$$

"$C(\rho)$ is a measure of the entanglement of formation in its own right." [Wootters]

entanglement of formation and distillation

asymptotic conversion ratios for



Negativity

[Życzkowski et al. PRA'98, Eisert, Plenio JMO'99, Vidal, Werner, PRA'02]

a quantitative version of the Peres-Horodecki entanglement criterion [Peres, PRL'96, Horodecki et al., PLA'96]

$N(\rho) = \max\{0, -2\min_i \mu_i\}$

$N(\rho) = \max\{0, -2\sum \mu_i\}$

where μ_i eigenvalues of the partial transpose of ρ

Logarithmic negativity

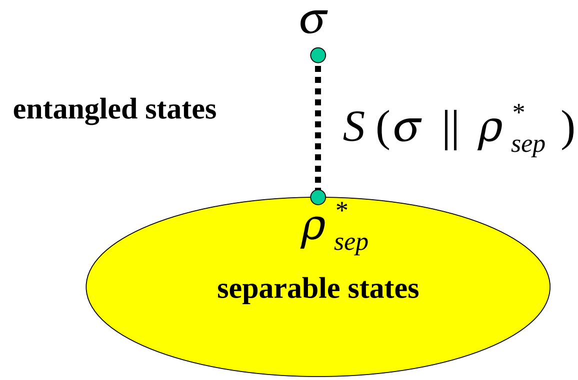
$E_N(\rho) = \log_2[N(\rho) + 1]$

a measure of the PPT entanglement cost

[Audenaert et al. PRL'03, Ishizaka PRA'04]

E_N **gives upper bounds on the teleportation capacity and the entanglement of distillation** E_D [Vidal, Werner PRA'02]

geometric measure of entanglement



Relative entropy of entanglement (REE)

[Vedral, Plenio, Jacobs, Knight, PRA'1997]

$E(\sigma) = \inf_{\rho\in\mathcal{D}} S(\sigma||\rho) = S(\sigma||\rho^*)$

ρ^* **– the closest separable state to σ**

quantum relative entropy

or a quantum Kullback-Leibler distance

$S(\sigma||\rho) = \mathrm{Tr}\,(\sigma\log\sigma - \sigma\log\rho)$

NOTE:

$S(\sigma||\rho)$ **is a "distance" between σ and ρ**

- but it is not a true metric:

  it is neither symmetric nor satisfies the triangle inequality

- it is not a unique measure of the distance:

  see also Bures measure with the Uhlmann transition probability (or fidelity)

  $S'(\sigma||\rho) = 2 - 2\sqrt{F(\sigma,\rho)}$ with $F(\sigma,\rho) = [Tr(\sqrt{\rho}\sigma\sqrt{\rho})^{1/2}]^2$

Bell-inequality violation

For two qubits the Bell inequality due to Clauser, Horne, Shimony and Holt (CHSH) [PRL'69]:

$|\mathrm{Tr}\,(\rho\,\mathcal{B}_{\mathrm{CHSH}})| \le 2$

where Bell operator is

$\mathcal{B}_{\mathrm{CHSH}} = \mathbf{a}\cdot\boldsymbol{\sigma}\otimes(\mathbf{b}+\mathbf{b}')\cdot\boldsymbol{\sigma} + \mathbf{a}'\cdot\boldsymbol{\sigma}\otimes(\mathbf{b}-\mathbf{b}')\cdot\boldsymbol{\sigma}$

and arbitrary ρ in Hilbert-Schmidt basis is

$$\rho = \frac{1}{4}\left(I\otimes I + \mathbf{r}\cdot\boldsymbol{\sigma}\otimes I + I\otimes\mathbf{s}\cdot\boldsymbol{\sigma} + \sum_{n,m=1}^{3} t_{nm}\,\sigma_n\otimes\sigma_m\right)$$

with $t_{nm} = \mathrm{Tr}\,(\rho\,\sigma_n\otimes\sigma_m)$

Horodecki et al. [PLA'95] showed that

$\max_{\mathcal{B}_{\mathrm{CHSH}}} \mathrm{Tr}\,(\rho\,\mathcal{B}_{\mathrm{CHSH}}) = 2\sqrt{M(\rho)}$

where $M(\rho) = \max_{j<k}\{u_j + u_k\}$;

u_j are eigenvalues of $U_\rho = T_\rho^T T_\rho$; $T_\rho = [t_{nm}]_{3\times3}$

Degree of the Bell-inequality violation (BIV)

Horodecki theorem: the Bell inequality is violated iff $M(\rho) > 1$

- useful parameter

$$B(\rho) \equiv \sqrt{\max\{0,\ M(\rho) - 1\}}$$

then

$B(\rho) = 1 \quad \Rightarrow \quad$ **the maximal violation of Bell inequality**

$B(\rho) = 0 \quad \Rightarrow \quad$ **state ρ admits local hidden variable model**

Entanglement measures for two-qubit pure states

$$|\Psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$$

$$\boxed{C(\Psi) = N(\Psi) = B(\Psi) = 2|c_{00}c_{11} - c_{01}c_{10}|}$$

Two-qubit Werner states

1. **Definition**

   Mixture of the maximally entangled state (singlet) $|\Psi^-\rangle$ and the (separable) maximally mixed state [Werner, PRA'89]:

   $$\boxed{\rho_W = p|\Psi^-\rangle\langle\Psi^-| + \tfrac{1-p}{4} I \otimes I \quad \textbf{for} \quad 0 \le p \le 1}$$

2. **Degree of Bell-inequality violation**

   $$\boxed{B(\rho_W) = \max\{0, 2p^2 - 1\}^{1/2}}$$

   thus the Werner state violates the Bell inequality iff $1/\sqrt{2} < p \le 1$

3. **Concurrence & negativity**

   $$\boxed{C(\rho_W) = N(\rho_W) = \max\left\{0, \tfrac{1}{2}(3p - 1)\right\}}$$

   states are entangled iff $1/3 < p \le 1$.

   $\Rightarrow$ Entanglement without Bell inequality violation for $p \in \left(\frac{1}{3}, \frac{1}{\sqrt{2}}\right\rangle$

CONJECTURE

Entanglement measures should impose the same ordering of states

$$\boxed{E'(\rho_1) < E'(\rho_2) \Leftrightarrow E''(\rho_1) < E''(\rho_2)}$$

QUESTIONS:

Can this condition be violated?

Yes.

Eisert and Plenio [J. Mod. Opt. 1999] - numerical example

Is it a necessary condition for consistency of entanglement measures?

Strange, but no.

Eisert-Plenio conclusion from Monte Carlo simulations:

ordering of states can depend on the applied measures of entanglement

Virmani-Plenio theorem:

all good asymptotic entanglement measures,
which reduce to the entropy of entanglement for pure states,
are either equivalent or do not impose the same state ordering

Why is it so?

It is implied by the requirements of equivalence and continuity of the measures on pure states

Is it physically reasonable?

Yes, as these incomparable states cannot be
transformed to each other with unit efficiency by LOCC.

Can we avoid the state-ordering ambiguity?

No, if we want to define entanglement measures for
examining the problems of how to prepare and use the entanglement.

509

Questions

1. Can we find analytical examples of two-qubit states for which entanglement measures impose different orderings ?

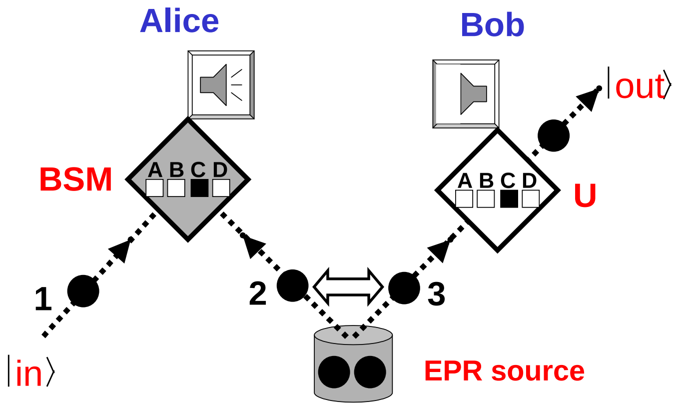
2. Are there mixed states more entangled than pure states ???

3. Can we find a physical process manifesting the different orderings ?

510

ideal teleportation

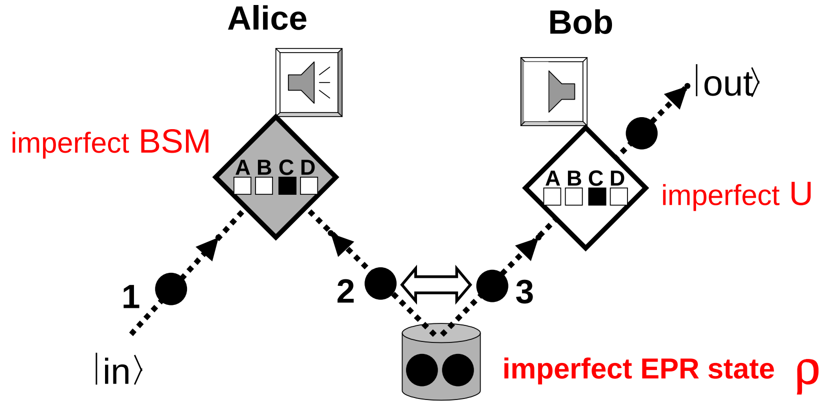
Bennett, Brassard, Crepeau, Jozsa, Peres, Wootters (1993)



teleportation fidelity $F = \langle in \mid \rho_{out} \mid in \rangle = 1$

511

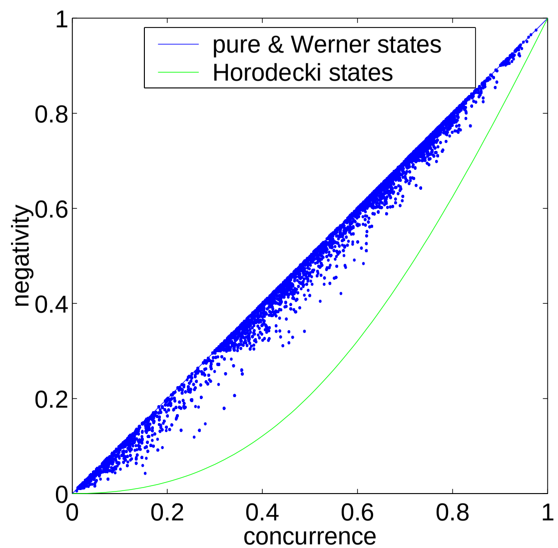
real teleportation



$$E(\rho') > E(\rho'') \overset{?}{\Rightarrow} F(\rho') > F(\rho'')$$

512

Upper & lower bounds for negativity vs concurrence



Numerical simulations of 5×10^4 states.

Upper & lower bounds for negativity vs concurrence

[Verstraete et al. JPA'01]

$$\boxed{C(\rho) \geq N(\rho) \geq \sqrt{[1-C(\rho)]^2 + C^2(\rho)} + C(\rho) - 1 \equiv f_C(\rho)}$$

Structure of the extremal states:

1. $N(\rho) = C(\rho) \iff$

the eigenvector corresponds to the negative eigenvalue of ρ^{T_A} is a Bell state

$\Rightarrow$ states have the maximum negativity for a given concurrence

2. $N(\rho) = f_C(\rho) \iff$

two eigenvalues are vanishing and the other two correspond to eigenvectors, which are a Bell state and separable state orthogonal to it

$\Rightarrow$ states have the minimum negativity for a given concurrence

• Examples of the minimum-negativity states

1. **Horodecki state** $\rho_H(p) = p|\psi_-\rangle\langle\psi_-| + (1-p)|00\rangle\langle 00|$
2. **Horodecki-like state** $\rho'_H(p) = p|\psi_-\rangle\langle\psi_-| + (1-p)|\psi'\rangle\langle\psi'|$

where $|\psi'\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

$\Rightarrow$ **concurrence** $C(\rho_H) = p$

negativity $N(\rho_H) = \sqrt{(1-p)^2 + p^2} - (1-p)$

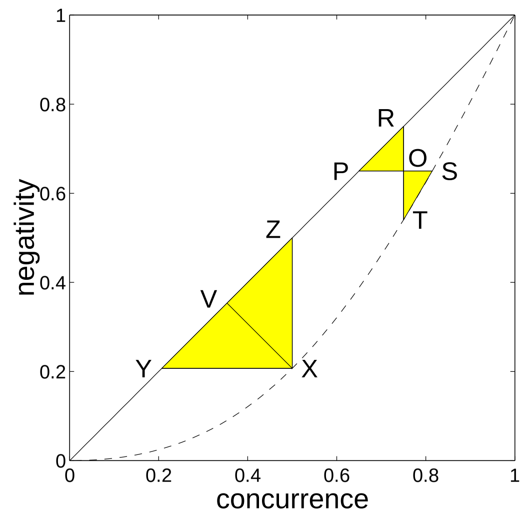
• Examples of the maximum-negativity states

1. **pure states**
2. **Bell diagonal states**

2(a) **Werner state** $\rho_W(p) = p|\psi_-\rangle\langle\psi_-| + \frac{1-p}{4} I \otimes I$

$$\Rightarrow \quad N(\rho_W) = C(\rho_W) = \max\{0, \tfrac{3p-1}{2}\}$$

Regions of different state orderings for negativity N and concurrence C



Two states, when one corresponds to a point O (or X) and the other to any other point in yellow regions, exhibit different state orderings for N and C.

Explicit examples of states extremely violating the ordering condition

Let us choose the Horodecki state:

$\rho_X = \rho_H(1/2)$

and the Werner states:

$\rho_Y = \rho_W(\sqrt{2}/3)$**,**

$\rho_Z = \rho_W(2/3)$**,**

$\rho_V = \rho_W(1/3 + \sqrt{2}/6)$

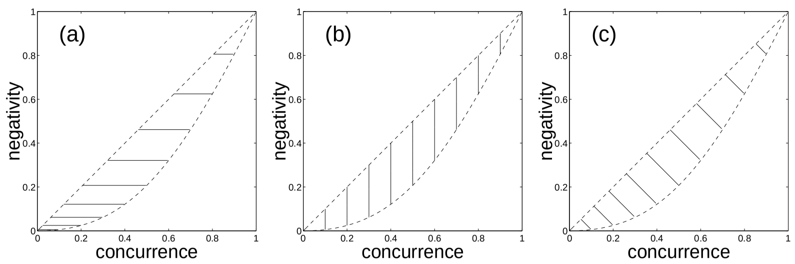
or pure state $|\Psi(p)\rangle = \sqrt{p}\,|01\rangle + \sqrt{1-p}\,|10\rangle$**:**

$\rho_Y = |\Psi(p)\rangle\langle\Psi(p)|$ **for** $p = 1/2 \pm \sqrt{1+2\sqrt{2}}/4$**,**

ρ_Z **for** $p = 1/2 \pm \sqrt{3}/4$**,**

ρ_V **for** $p = 1/2 \pm \sqrt{14}/8$

States specifically violating the ordering condition



(a) states with constant negativity

(b) states with constant concurrence

(c) states for which $C(\rho_1) - C(\rho_2) = -[N(\rho_1) - N(\rho_2)]$

States specifically violating the ordering condition

$\bar{\rho}(p,q) = p|\psi_-\rangle\langle\psi_-| + (1-p)|\psi_q\rangle\langle\psi_q|$

with $|\psi_q\rangle = \sqrt{1-q}|00\rangle + \sqrt{q}|01\rangle$

then

$N(\bar{\rho}(p,q)) = \sqrt{1-2p(1-p)(1-q)} - (1-p)$
$C(\bar{\rho}(p,q)) = p$

- **Three classes of states**:

1. states with the same negativity N_0:

$\rho' = \bar{\rho}(p,q')$ for $q' = \frac{N_0[N_0+2(1-p)]-p^2}{2p(1-p)}$

2. states with the same concurrence C_0:

$\rho'' = \bar{\rho}(C_0,q)$

3. states giving exactly opposite predictions:

$\rho''' = \bar{\rho}(p,q''')$ for $q''' = 1 + \frac{[N(\rho)+C(\rho)+1-2p]^2-1}{2p(1-p)}$

REE vs concurrence and negativity

REE for Bell diagonal (including Werner) states

$E_W(C) = E_W(N) = \frac{1}{2}\left[(1+C)\log(1+C) + (1-C)\log(1-C)\ \right]$

REE for pure states

$E_P(C) = E_P(N) = H\left(\frac{1}{2}[1+\sqrt{1-C^2}]\right)$

REE for Horodecki states

$\sigma_H = C|\psi_-\rangle\langle\psi_-| + (1-C)|00\rangle\langle 00|$

$E_H(C) = (C-2)\log(1-C/2) + (1-C)\log(1-C)$

$E_H(C = \sqrt{2N(1+N)} - 1)$

Numerics for two-qubit REE:

[Vedral and Plenio, PRA'1998]

Caratheodory's theorem:

Any state in $\mathcal{D}$ can be decomposed into a sum of at most $(\dim(H_A) \times \dim(H_B))^2$ products of pure states.

Thus, any disentangled 2 qubit state can be given by

$$\rho = \sum_{i=1}^{16} p_i |\psi_{Ai}\rangle\langle\psi_{Ai}| \otimes |\psi_{Bi}\rangle\langle\psi_{Bi}|$$

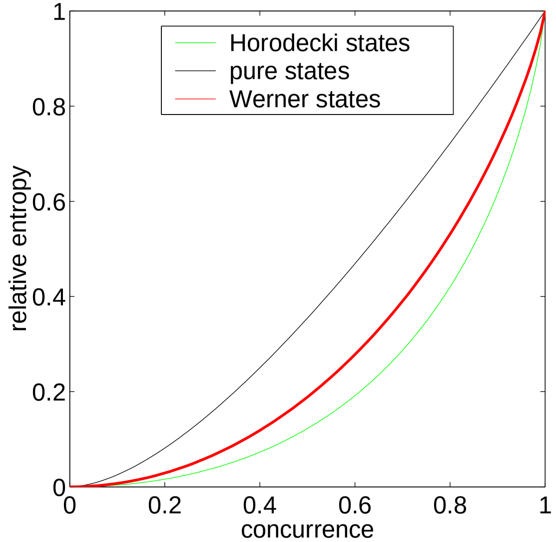
$\Rightarrow$ **there are at most** $15 + 16 \times 4 = 79$ **real parameters**

How to minimize $S(\sigma||\rho)$ over 79 parameters?

$S(\sigma||\rho)$ is a convex function

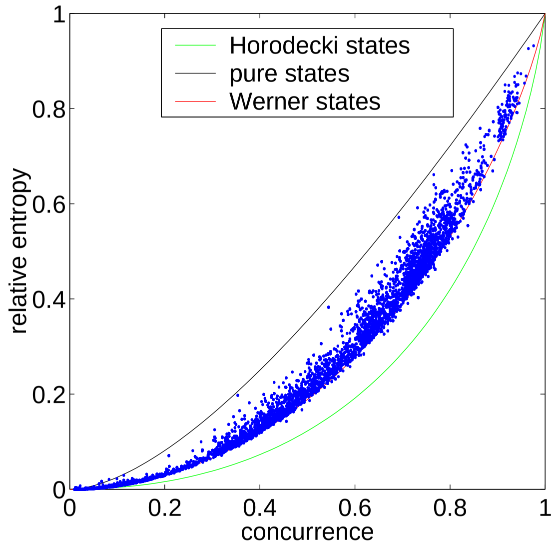
$\mathcal{D}$ is a convex set (convex hull) of its pure states

a convex function over a convex set can only have a global minimum

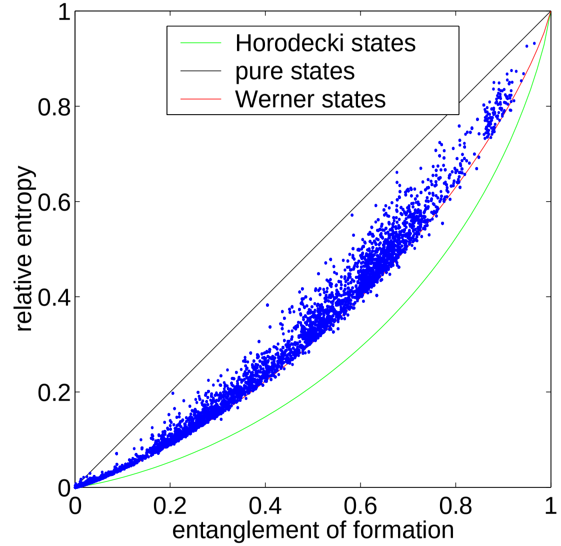


Relative entropy vs concurrence:

$E_{\rm pure}(C) > E_{\rm W}(C) > E_{\rm H}(C)$ **for** $C \in (0,1)$

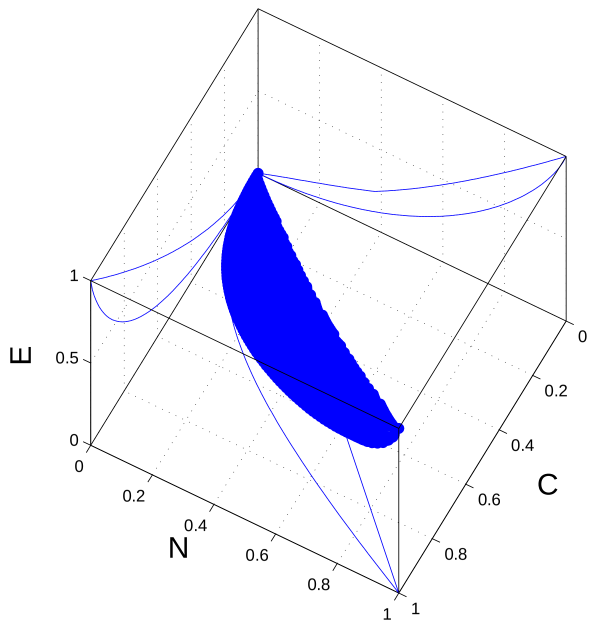


Relative entropy vs concurrence:
Numerical simulations of 5×10^4 states



Relative entropy vs entropy of formation:
Numerical simulations of 5×10^4 states

How to find different state orderings imposed by E, C & N



All cases of different state orderings

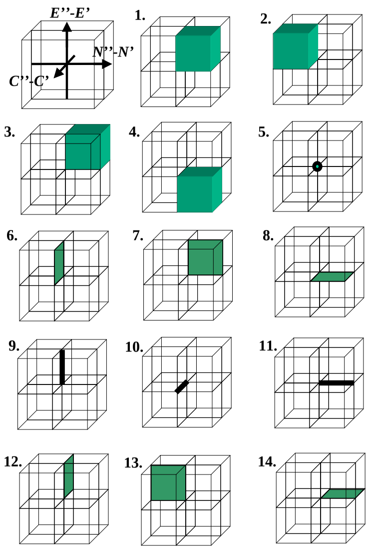


Table 1: All cases of different state orderings by E, C & N.

Class	Concurrences	Negativities	REEs
1	$C(\sigma') < C(\sigma'')$	$N(\sigma') < N(\sigma'')$	$E(\sigma') < E(\sigma'')$
2	$C(\sigma') < C(\sigma'')$	$N(\sigma') > N(\sigma'')$	$E(\sigma') < E(\sigma'')$
3	$C(\sigma') > C(\sigma'')$	$N(\sigma') < N(\sigma'')$	$E(\sigma') < E(\sigma'')$
4	$C(\sigma') < C(\sigma'')$	$N(\sigma') < N(\sigma'')$	$E(\sigma') > E(\sigma'')$
5	$C(\sigma') = C(\sigma'')$	$N(\sigma') = N(\sigma'')$	$E(\sigma') = E(\sigma'')$
6	$C(\sigma') < C(\sigma'')$	$N(\sigma') = N(\sigma'')$	$E(\sigma') < E(\sigma'')$
7	$C(\sigma') = C(\sigma'')$	$N(\sigma') < N(\sigma'')$	$E(\sigma') < E(\sigma'')$
8	$C(\sigma') < C(\sigma'')$	$N(\sigma') < N(\sigma'')$	$E(\sigma') = E(\sigma'')$
9	$C(\sigma') = C(\sigma'')$	$N(\sigma') = N(\sigma'')$	$E(\sigma') < E(\sigma'')$
10	$C(\sigma') < C(\sigma'')$	$N(\sigma') = N(\sigma'')$	$E(\sigma') = E(\sigma'')$
11	$C(\sigma') = C(\sigma'')$	$N(\sigma') < N(\sigma'')$	$E(\sigma') = E(\sigma'')$
12	$C(\sigma') > C(\sigma'')$	$N(\sigma') = N(\sigma'')$	$E(\sigma') < E(\sigma'')$
13	$C(\sigma') = C(\sigma'')$	$N(\sigma') > N(\sigma'')$	$E(\sigma') < E(\sigma'')$
14	$C(\sigma') < C(\sigma'')$	$N(\sigma') > N(\sigma'')$	$E(\sigma') = E(\sigma'')$

Quantum information processing with quantum dots

1. based on electron spins of quantum dots
   using optical methods

2. based on nuclear spins of quantum dots
   using NMR methods

What are the quantum dots?

Quantum dots (q-dots or artificial atoms) are small metal or semiconductor boxes that hold a well-defined number of electrons

useful property

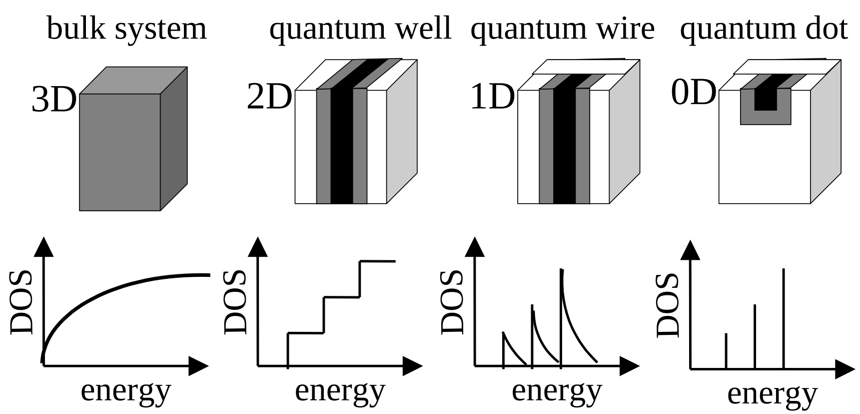
number of electrons in a q-dot can be adjusted by changing the dot electrostatic environment

parameters

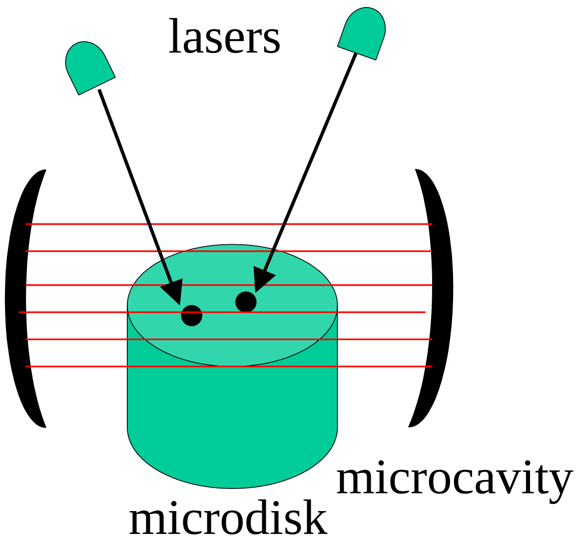
number of electrons: from 0 to hundreds

size of q-dots: from 30 nm to 1 micron

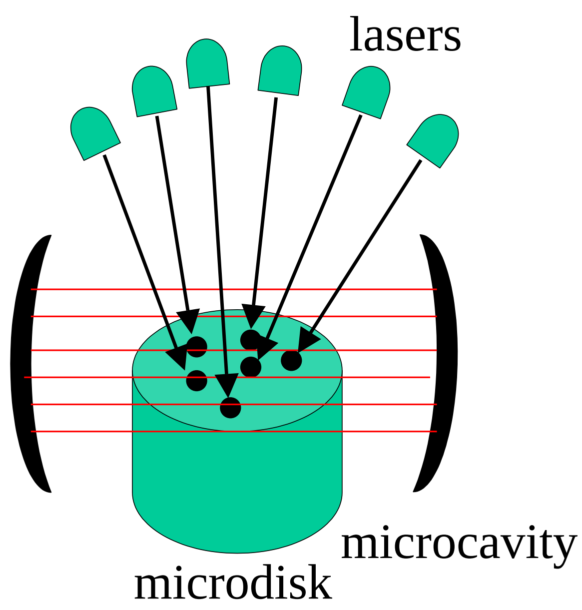
Energy spectra of q-dots vs other nano-structures



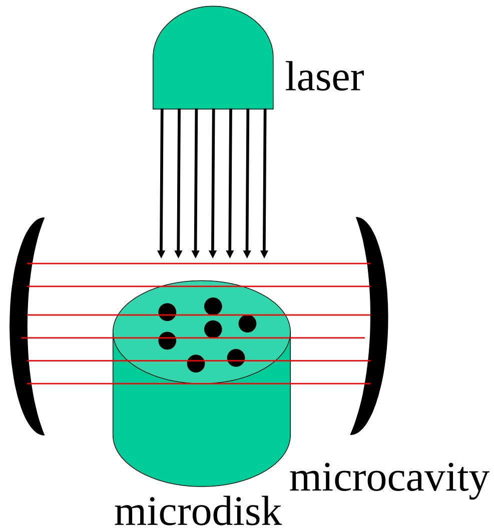
Quantum-information processing based on q-dots and cavity QED [Imamoğlu et al., PRL'99]

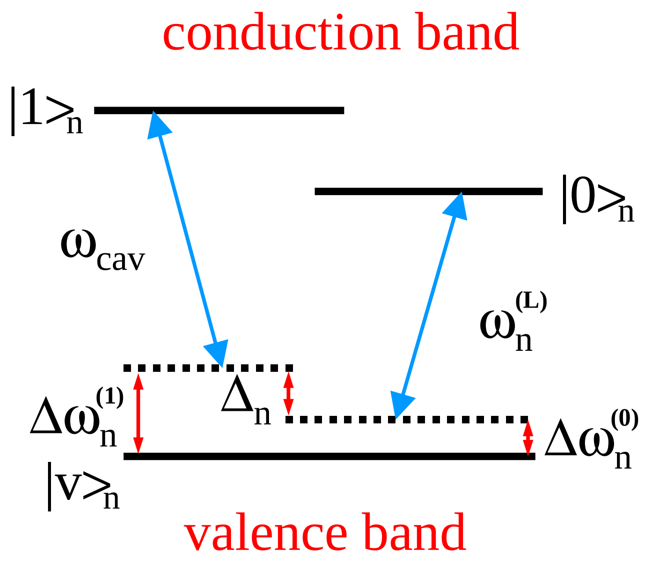


Scalable system of quantum dot interactions and cavity QED



Identical quantum dots in microcavity





Level structure of quantum dots in V configuration

Hamiltonian for N three-level q-dots interacting with $N+1$ fields

$$\begin{aligned}
\hat{H} &= \hat{H}_{QD} + \hat{H}_F + \hat{H}_{\text{int}}, \\
\hat{H}_{QD} &= \sum_n \left(\mathcal{E}_n^{(0)}\hat{\sigma}_n^{00} + \mathcal{E}_n^{(1)}\hat{\sigma}_n^{11} + \mathcal{E}_n^{(v)}\hat{\sigma}_n^{vv}\right), \\
\hat{H}_F &= \hbar\omega_{\text{cav}}\hat{a}_{\text{cav}}^\dagger\hat{a}_{\text{cav}} + \sum_n \hbar\omega_n^{(L)}(\hat{a}_n^{(L)})^\dagger\hat{a}_n^{(L)}, \\
\hat{H}_{\text{int}} &= \sum_n \hbar g_n^{v0}[\hat{a}_n^{(L)}\hat{\sigma}_n^{0v} + (\hat{a}_n^{(L)})^\dagger\hat{\sigma}_n^{v0}] \\
&\quad + \sum_n \hbar g_n^{v1}(\hat{a}_{\text{cav}}\hat{\sigma}_n^{1v} + \hat{a}_{\text{cav}}^\dagger\hat{\sigma}_n^{v1}),
\end{aligned}$$

where the nth dot operator is $\hat{\sigma}_n^{xy} = |x\rangle_{nn}\langle y|$

Note: Q-dots are coupled only indirectly via the cavity and laser fields

Derivation of q-dot interaction Hamiltonian

3-level Hamiltonian for $|g_n>$, $|e_n>$, $|v_n>$, $a_n^{(\mathrm{L})}$, a_{cav}

⇓

effective 2-level Hamiltonian for $|g_n>$, $|e_n>$, $a_n^{(\mathrm{L})}$, a_{cav}

⇓

effective spin-spin interaction Hamiltonian for $|g_n>$, $|e_n>$

⇓

equivalent-neighbor (SVW) Hamiltonian

Hamiltonian after adiabatic elimination

$$\hat{H}_{\text{eff}} = \frac{\hbar}{2}\sum_{n\neq m}\kappa_{nm}(t)[\hat{\sigma}_n^+\hat{\sigma}_m^- e^{i(\Delta_n-\Delta_m)t} + \hat{\sigma}_n^-\hat{\sigma}_m^+ e^{-i(\Delta_n-\Delta_m)t}]$$

where

$$\kappa_{nm}(t) = \frac{g_n(t)g_m(t)}{\Delta_n}$$

$$g_n(t) = g_n^{v0}g_n^{v1}|E_n^{(L)}(t)|\left(\frac{1}{\Delta\omega_n^{(1)}} + \frac{1}{\Delta\omega_n^{(0)}}\right)$$

$$\Delta\omega_k^{(n)} = \omega_k^{(n)} - \omega_{VB}^{(n)} - \omega_{cav} \quad (k = e, g)$$

$$\Delta_n = \omega_e^{(n)} - \omega_g^{(n)} + \omega_L^{(n)} - \omega_{cav} = \Delta\omega_e^{(n)} - \Delta\omega_g^{(n)}$$

Adiabatic elimination requires

1. coupling strength, cavity decay rate, and thermal fluctuations $\ll \hbar\Delta_n, \hbar\Delta\omega_n^{(x)}, \mathcal{E}_n^{(1)} - \mathcal{E}_n^{(0)}$
2. valence-band levels $|v\rangle_n$ are far off resonance.

Models

Frenkel-type model or Heisenberg model

$$\hat{H}_{\rm int} = \hbar \sum_{n\neq m} T_{nm}\left[\hat{\sigma}_n^+\hat{\sigma}_m^- + \hat{\sigma}_n^-\hat{\sigma}_m^+ + \gamma(\hat{\sigma}_n^+\hat{\sigma}_m^+ + \hat{\sigma}_n^-\hat{\sigma}_m^-)\right]$$

Spin van der Waals (SVW) model

Frenkel model for T_{nm}=const

$$\hat{H}_{\rm int} = \kappa \sum_{n\neq m}[\hat{\sigma}_n^+\hat{\sigma}_m^- + \hat{\sigma}_n^-\hat{\sigma}_m^+ + \gamma(\hat{\sigma}_n^+\hat{\sigma}_m^+ + \hat{\sigma}_n^-\hat{\sigma}_m^-)]$$

Conservative SVW model (CE model)

SVW model for $\gamma = 0$

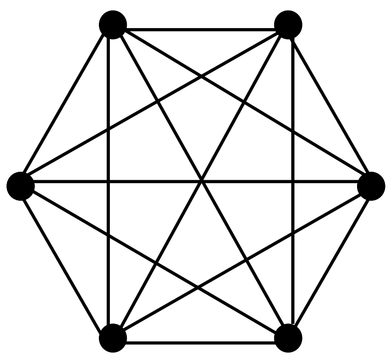
$$\hat{H}_{\rm int} = \kappa \sum_{n\neq m} \hat{\sigma}_n^+\hat{\sigma}_m^- + \hat{\sigma}_n^-\hat{\sigma}_m^+$$

Non-conservative SVW model (NCE model)

SVW model for $\gamma = 1$

$$\hat{H}_{\rm int} = 4\kappa \sum_{n\neq m} \hat{\sigma}_n^x\hat{\sigma}_m^x$$

Entangled webs in spin van der Waals (SVW) model

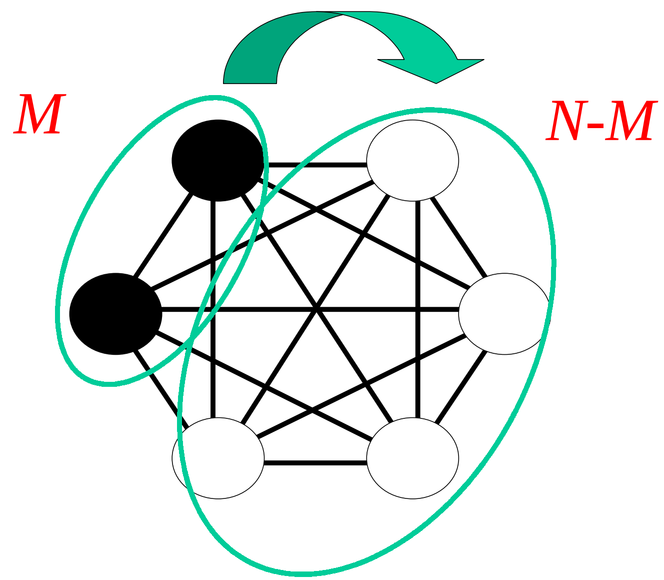


Tight bound for symmetric sharing of entanglement

$C_{ij} \leq 2/N$

[Koashi,Bužek,Imoto, PRA'00]

Q-dot bipartite entanglement in SVW model



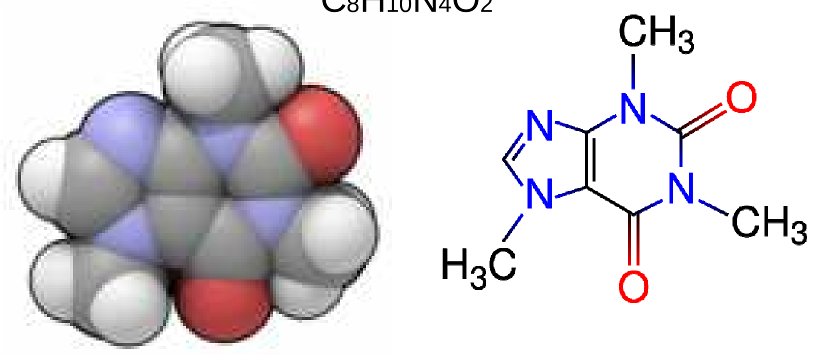
Quantum Computing Based on Nuclear Magnetic Resonance (NMR)

1. nuclear qubits and qudits
2. control of nuclear spins
3. pseudo-pure states
4. quantum gates
5. quantum algorithms
6. tomography of nuclear spins

Quantum computer in a cup of coffee?

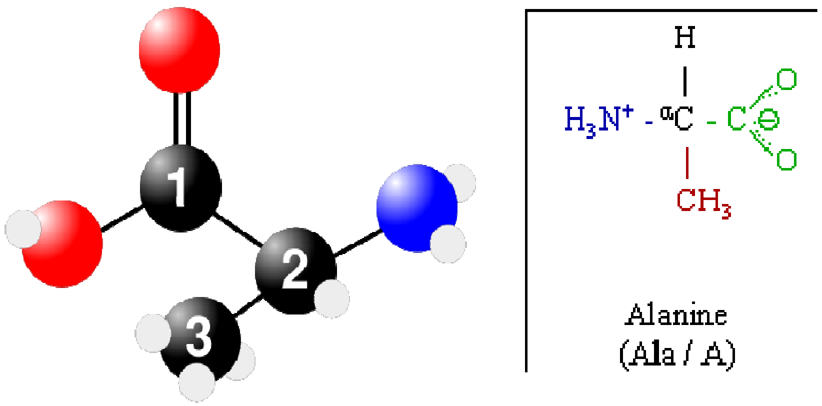
caffeine molecule
- qubits encoded in nonequivalent C-nuclei

$C_8H_{10}N_4O_2$



CHEMICAL NAME : 3,7-Dihydro-1,3,7-trimethyl-1H-purine-2,6-dione

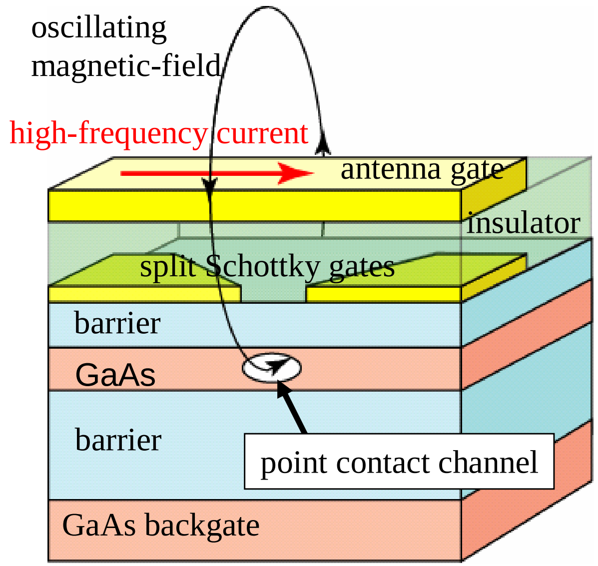
three qubits encoded in ^{13}C-labeled alanine molecule



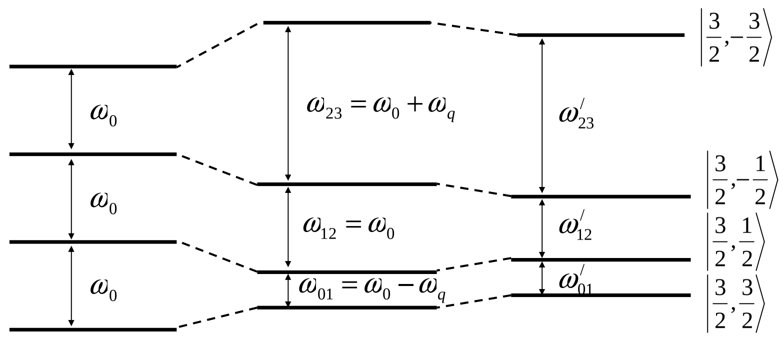
J-coupling Hamiltonian for carbon-13 nuclei

$$\hat{H}_{int} = \nu_1 \hat{\sigma}_z^{(1)} + \nu_2 \hat{\sigma}_z^{(2)} + \nu_3 \hat{\sigma}_z^{(3)} + \tfrac{1}{2}(J_{12}\hat{\sigma}_z^{(1)}\hat{\sigma}_z^{(2)} + J_{23}\hat{\sigma}_z^{(2)}\hat{\sigma}_z^{(3)} + J_{13}\hat{\sigma}_z^{(1)}\hat{\sigma}_z^{(3)})$$

NMR quantum computing in nanostructures



energy levels of spin I=3/2

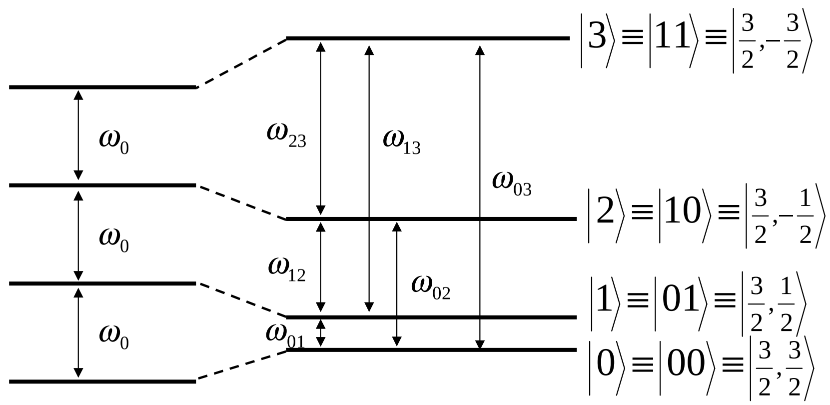


Zeeman interaction

quadrupole interaction

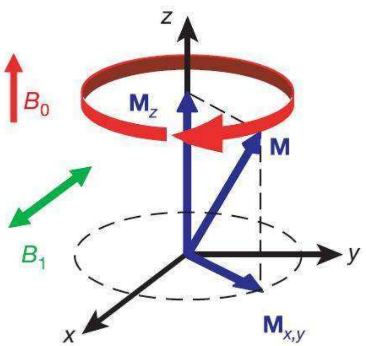
2nd order shifts (usually neglected)

quartit is equivalent to 2 virtual qubits



quartit = ququart = 4-level qudit

Larmor precession



M – magnetization vector of an ensemble of nuclear spins

B_0 – static magnetic field

B_1 – magnetic field component of the r.f. field

M_{xy} – transverse component of M precessing in the x–y plane (Larmor precession)

M_z – longitudinal component of M static along B_0

rotations via NMR techniques

Z-rotation

corresponds to free evolution of a spin-1/2 system without r.f. fields

- **Hamiltonian**

$$\hat{\mathcal{H}}_0 = \tfrac{1}{2}\hbar\omega_0\hat{\sigma}_z$$

- **solution of Schödinger equation**

$$|\psi(t_p)\rangle = \hat{R}_z(\omega_0 t_p)|\psi(0)\rangle$$

in terms of the propagator

$$\hat{R}_z(\omega_0 t_p) \;=\; \exp\left[\frac{1}{i\hbar}\hat{\mathcal{H}}_0 t_p\right] = \begin{bmatrix} e^{-i\omega_0 t_p/2} & 0 \\ 0 & e^{i\omega_0 t_p/2} \end{bmatrix},$$

which is equal to $\hat{Z}(\theta)$ for $\theta = \omega_0 t_p$.

X- and Y-rotations

- **assumptions**

coil is along x-axis generating an r.f. pulse field

$$\mathbf{B}_{\rm rf}(t) = B_{\rm rf}\cos(\omega_{\rm ref} + \phi_p)\mathbf{e}_x$$

– ϕ_p is the phase of the pulse

– $B_{\rm rf}$ is the amplitude of the oscillating r.f. field

– $\omega_{\rm ref}$ is the spectrometer reference frequency

spin Hamiltonian during the r.f. pulse set on resonance

$$\omega_{\rm Larmor} = \omega_{\rm ref}$$

- **Hamiltonian** in the rotating frame

$$\hat{\mathcal{H}}'_{\rm rf,rot} = \frac{\hbar\omega_{\rm nut}}{2}(\hat{\sigma}_x\cos\phi_p + \hat{\sigma}_y\sin\phi_p)$$

where $\omega_{\rm nut} = \gamma B_{\rm rf}$ is the nutation frequency

- **solution of Schödinger equation**

for a pulse at resonant frequency ω of duration t_p, which corresponds to the nutation angle $\theta_p = \omega_{\mathrm{nut}} t_p$, and general phase ϕ_p can be given as

$$|\psi(t_p)\rangle = \hat{\chi}(\phi_p, \theta_p)|\psi(0)\rangle$$

where the **propagator** is

$$\begin{aligned}\hat{\chi}(\phi_p,\theta_p) &= \exp\left[\frac{1}{i\hbar}\hat{\mathcal{H}}'_{\mathrm{rf,rot}} t_p\right] \\ &= \exp\left[-\frac{i}{2}\theta_p(\hat{\sigma}_x\cos\phi_p + \hat{\sigma}_y \sin\phi_p)\right] \\ &= \begin{bmatrix} \cos\frac{\theta_p}{2} & -i\exp(-i\phi_p)\sin\frac{\theta_p}{2} \\ -i\exp(i\phi_p)\sin\frac{\theta_p}{2} & \cos\frac{\theta_p}{2}\end{bmatrix} \\ &= \hat{Z}(\phi_p)\hat{X}(\theta_p)\hat{Z}(-\phi_p)\end{aligned}$$

- **special cases**

$$\hat{X}(\theta) = \hat{\chi}(0,\theta)$$
$$\hat{Y}(\theta) = \hat{\chi}(\pi/2,\theta)$$

selective rotations in a quartit

$$\hat{X}_{01}(\tfrac{\pi}{2}) = \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{i}{\sqrt{2}} & 0 & 0 \\ -\frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1\end{pmatrix}, \quad \hat{X}_{12}(\tfrac{\pi}{2}) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{i}{\sqrt{2}} & 0 \\ 0 & -\frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1\end{pmatrix},$$

$$\hat{X}_{02}(\tfrac{\pi}{2}) = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & -\frac{i}{\sqrt{2}} & 0 \\ 0 & 1 & 0 & 0 \\ -\frac{i}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1\end{pmatrix}, \quad \hat{Y}_{01}(\tfrac{\pi}{2}) = \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1\end{pmatrix},$$

$$\hat{X}_{01}(\pi) = \begin{pmatrix} 0 & -i & 0 & 0 \\ -i & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1\end{pmatrix}, \quad \hat{Y}_{01}(\pi) = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1\end{pmatrix}, \quad \ldots$$

Who has introduced NMR quantum computing?

the method has been developed independently by:

1. **Cory, Fahmy, Havel** in the article on "NMR spectroscopy: an experimentally accessible paradigm for quantum computing" (1996)
2. **Gershenfeld and Chuang** in "Bulk quantum computation" (1996).

How to generate pseudo-pure states?

pseudo-pure states (PPS) or effective pure states

can be obtained via

1. spatial averaging
2. temporal averaging
3. logical labeling

Here, we describe only a version of spatial averaging.

How to obtain pseudo-pure states?

population of the spin energy level $|k\rangle$

$$N_k = A + (4-k)\Delta$$

where

$$A = \frac{N}{4} - \frac{5N\hbar\omega_0}{8k_BT}, \quad \Delta = \frac{N\hbar\omega_0}{4k_BT},$$

N – total umber of spins

ω_0 – Larmor frequency

Note: A does not contribute to the observed NMR signal

Assumption: quadrupole interaction $\ll$ Zeeman interaction

●●$\leftrightarrow \Delta$ – relative occupation of the corresponding quantum level

$|3\rangle$ ●●

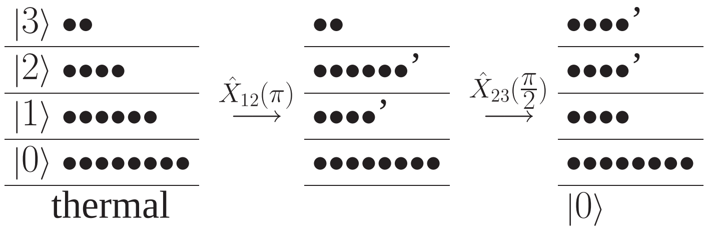
$|2\rangle$ ●●●●

$|1\rangle$ ●●●●●●

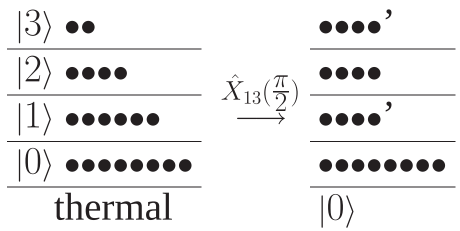
$|0\rangle$ ●●●●●●●●

thermal

How to obtain pseudo-pure state $|0\rangle$ in a quartit

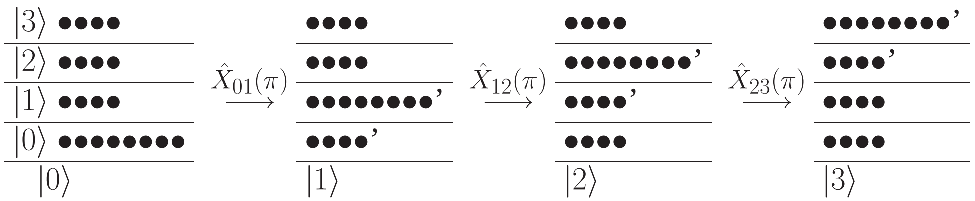


or equivalently

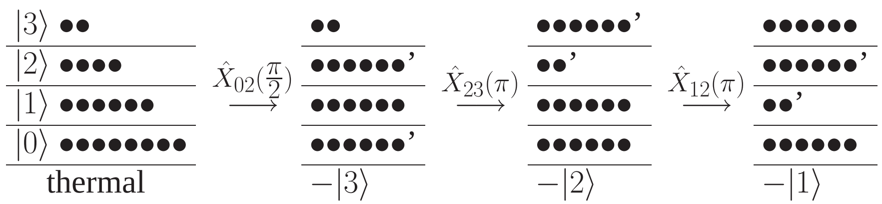


How to obtain pseudo-pure states in a quartit

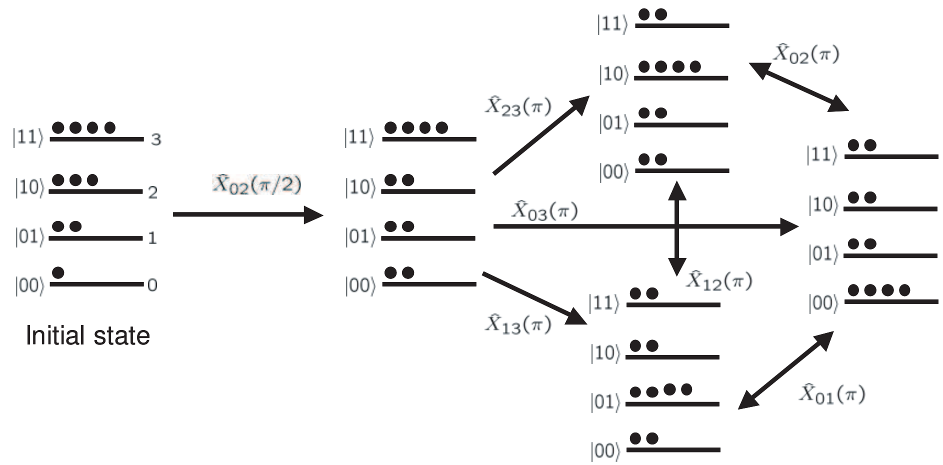
- states $|k\rangle$ ($k = 1, 2, 3$):



- states $(-|k\rangle)$



Interchanging pseudo-pure states in a quartit



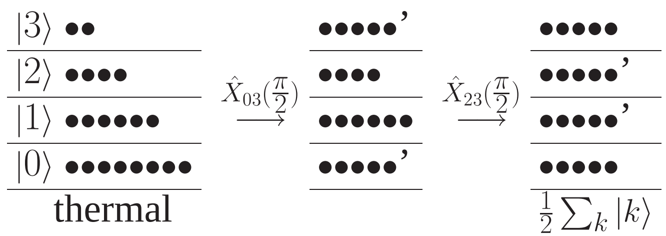
Note: here $|11\rangle$ – is the most populated state in equilibrium.

Whether $|11\rangle$ or $|00\rangle$ is the most populated depends on our labeling and direction of external magnetic field.

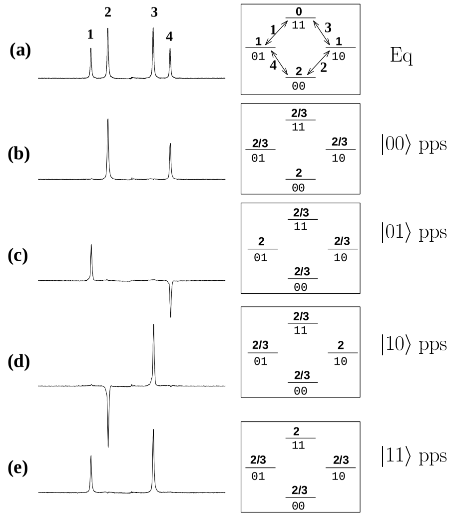
How to prepare equally-weighted superposition of pseudo-pure states in a quartit?

Apply gate equivalent to two-qubit Hadamard gate.

$$\hat{H}^A \otimes \hat{H}^B|0\rangle = \frac{1}{2}\sum_k |k\rangle$$

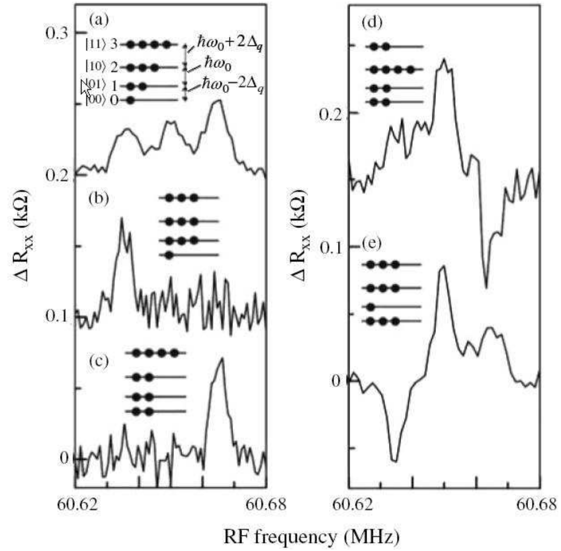


NMR spectra for pseudo-pure states of two spin-1/2 systems



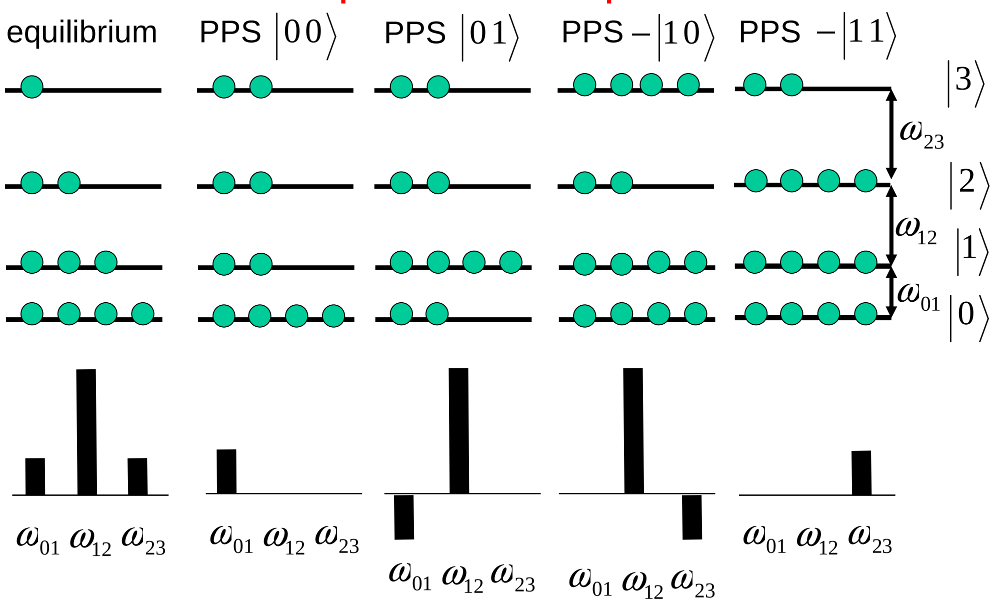
Key: $\frac{\text{population}}{\text{energy level}}$, PPS - pseudo-pure states, Eq - equilibrium [Mahesh *et al.*'03]

experimental generation of pseudo-pure states in solid-state systems of ^{69}Ga nuclei

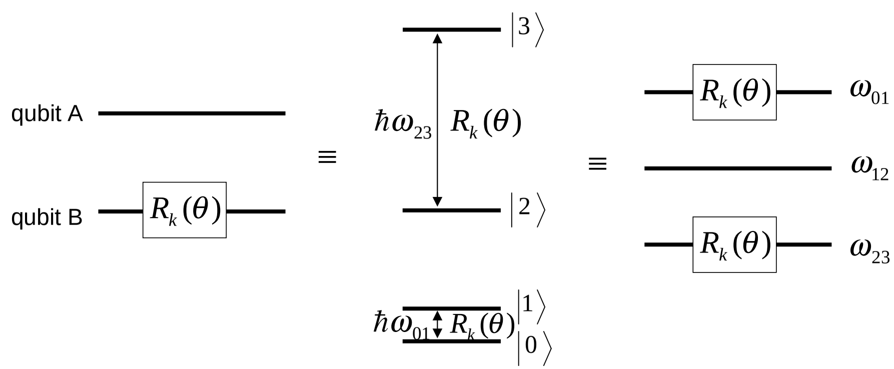


[Hirayama *et al.*'06]

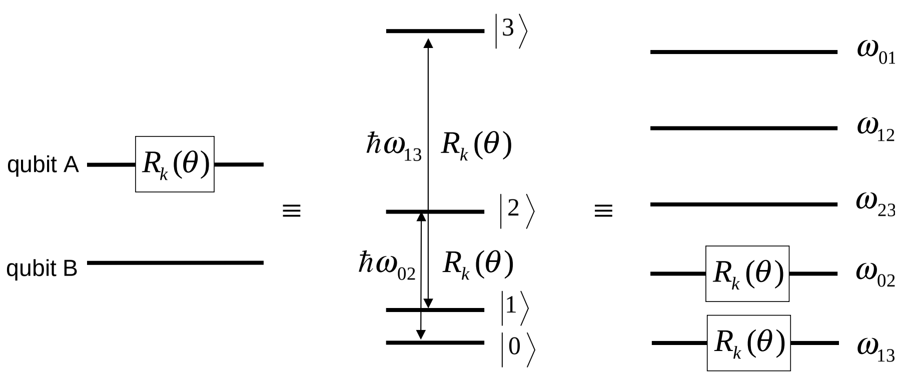
NMR spectra for a quartit



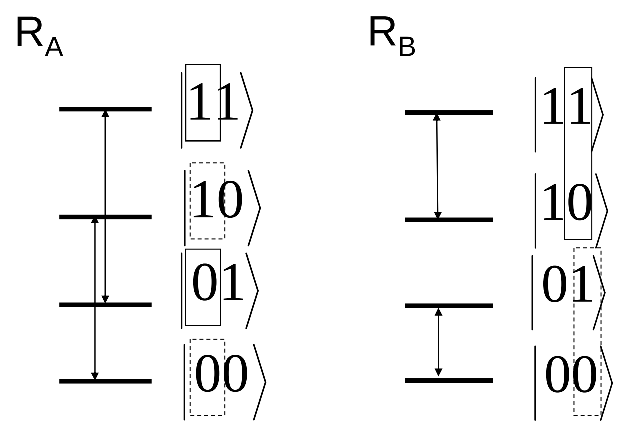
How to rotate "qubit" B in a quartit?



How to rotate “qubit” A in a quartit?

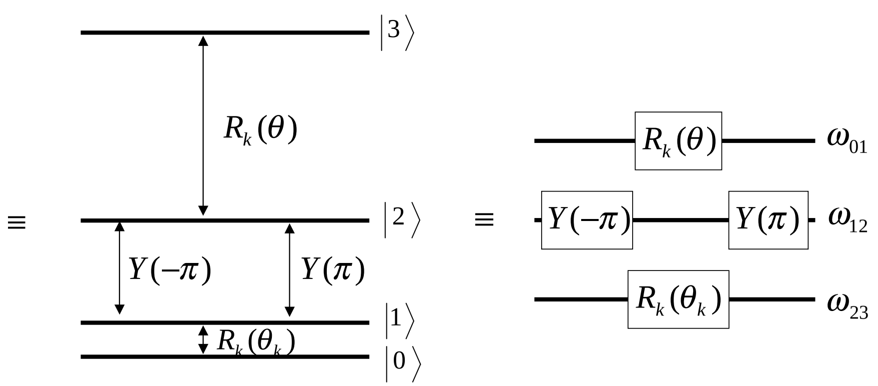


rotations of virtual qubit in quartit

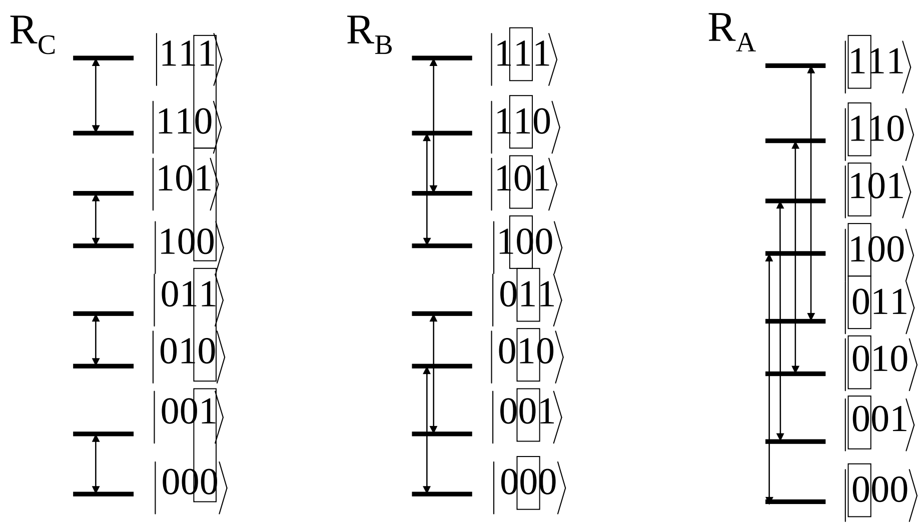


pulses are applied simultaneously

Another method to rotate “qubit” A in a quartit



rotations of a virtual qubit in 8D qudit



simultaneous application of pulses

NOT gates via rotations

- **NOT gate for a qubit**

$$\hat{U}_{\mathrm{NOT}} = \hat{\sigma}_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = i\hat{X}(\pi)$$

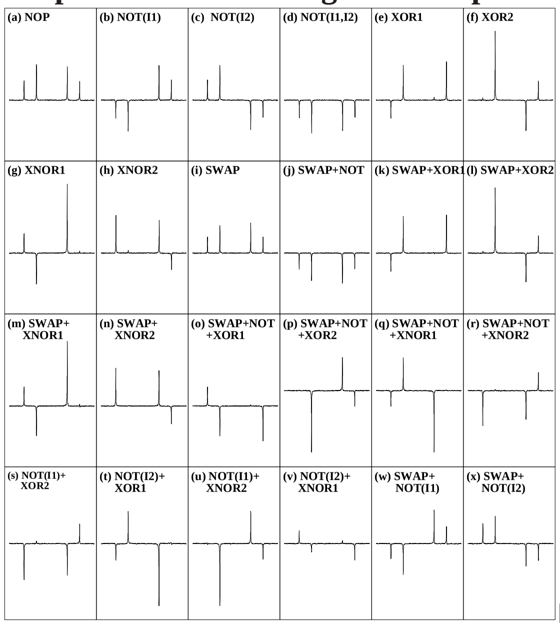
- **NOT gate for qubit A in a quartit**

$$\hat{U}^A_{\mathrm{NOT}} = \hat{U}_{\mathrm{NOT}} \otimes \hat{I} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} = \hat{U}^A_{\mathrm{NOT}} = \underline{i\hat{X}_{02}(\pi)\hat{X}_{13}(\pi)}$$

- **NOT gate for qubit B in a quartit**

$$\hat{U}^B_{\mathrm{NOT}} = \hat{I} \otimes \hat{U}_{\mathrm{NOT}} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \hat{U}^B_{\mathrm{NOT}} = \underline{i\hat{X}_{01}(\pi)\hat{X}_{23}(\pi)}$$

NMR spectra for classical gates in a spin-1/2 system



[Mahesh *et al.*'03]

Hadamard gates via rotations

- **Hadamard gate for a qubit**

$$\hat{H} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = i\hat{X}(\pi)\hat{Y}(\tfrac{\pi}{2}) = i\hat{Y}(\tfrac{\pi}{2})\hat{Z}(\pi)$$

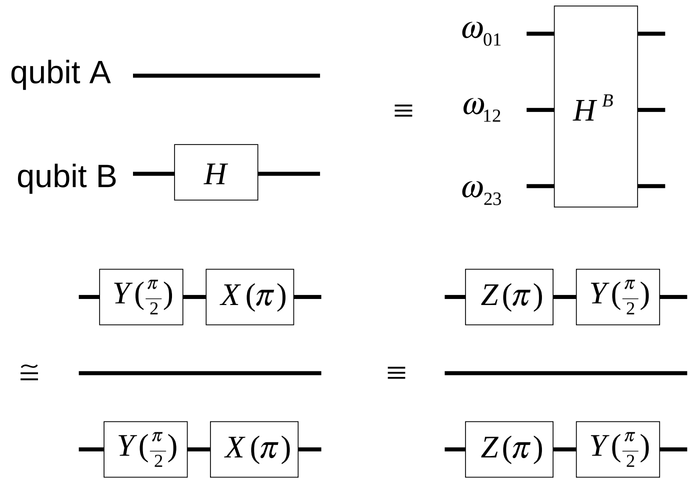
- **Hadamard gate for qubit A in a quartit**

$$\hat{H}^A = \hat{H}\otimes\hat{I} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} = i\hat{Y}_{12}(\pi)\hat{X}_{01}(\pi)\hat{Y}_{01}(\tfrac{\pi}{2})\hat{X}_{23}(-\pi)\hat{Y}_{23}(-\tfrac{\pi}{2})\hat{Y}_{12}(-\pi)$$

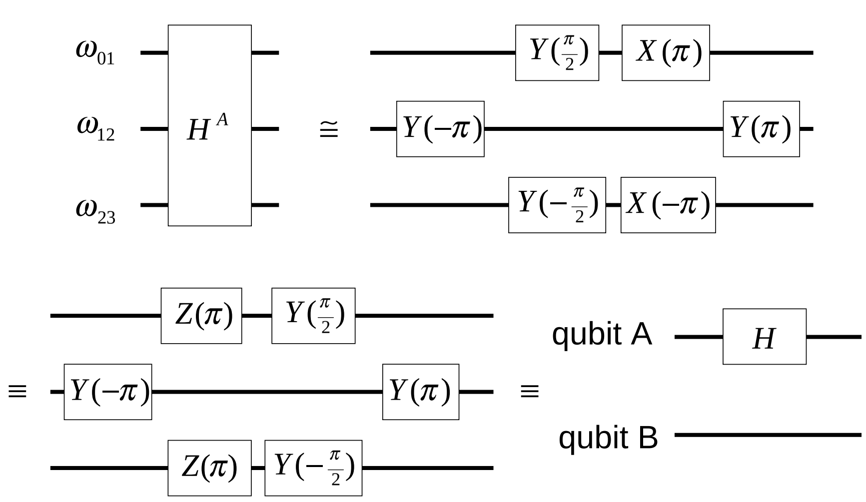
- **Hadamard gate for qubit B in a quartit**

$$\hat{H}^B = \hat{I} \otimes \hat{H} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} = i\hat{X}_{01}(\pi)\hat{Y}_{01}(\tfrac{\pi}{2})\hat{X}_{23}(\pi)\hat{Y}_{23}(\tfrac{\pi}{2})$$

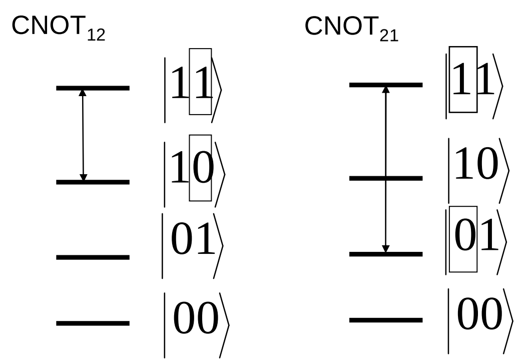
Equivalent realizations of Hadamard gate H^B (up to factor i)



Equivalent realizations of Hadamard gate H^A (up to factor i)



CNOT gates of 2 virtual qubits



CNOT gates via rotations

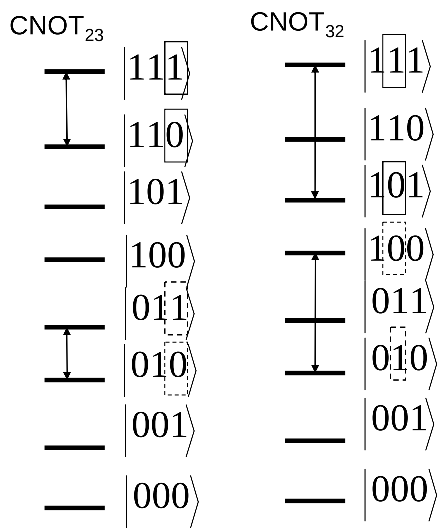
$$\hat{U}_{\mathrm{CNOT1}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \mathrm{diag}([1,1,-1,1]) \cdot \hat{Y}_{23}(\pi),$$

$$\hat{U}_{\mathrm{CNOT2}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} = \mathrm{diag}([1,1,1,-1]) \cdot Y_{12}(\pi)\hat{Y}_{23}(\pi)\hat{Y}_{12}(-\pi)$$

truth tables

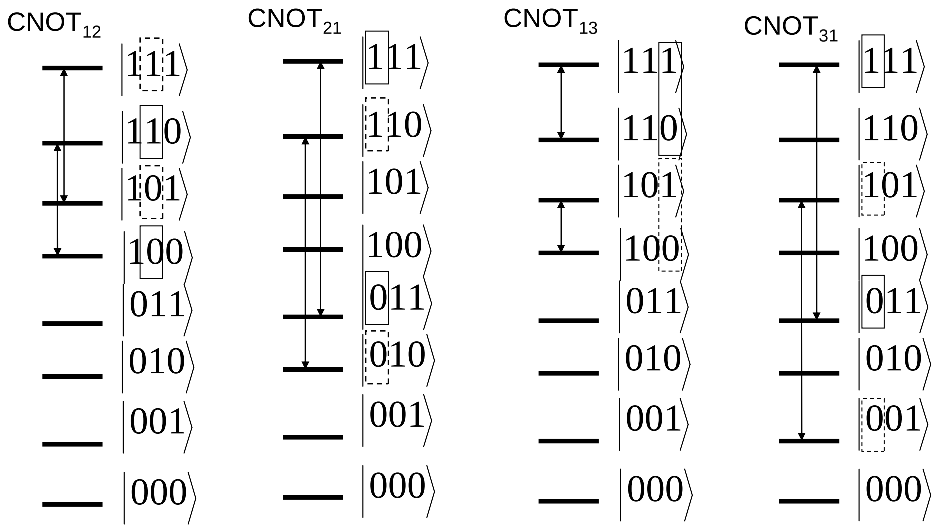
```
CNOT1       CNOT2       SWAP
in | out    in | out    in | out
--------    --------    --------
00 | 00     00 | 00     00 | 00
01 | 01     01 | 11     01 | 10
10 | 11     10 | 10     10 | 01
11 | 10     11 | 01     11 | 11
```

CNOT gates of 3 virtual qubits #1



pulses are applied simultaneously

CNOT gates of 3 virtual qubits #2



pulses are applied simultaneously

SWAP gates via rotations

$$\hat{U}_{\mathrm{SWAP}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \hat{U}_{\mathrm{CNOT1}}\hat{U}_{\mathrm{CNOT2}}\hat{U}_{\mathrm{CNOT1}}$$

which acts as follows

$$\hat{U}_{\mathrm{SWAP}}\Big(c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle\Big) \;=\; c_0|00\rangle + c_2|01\rangle + c_1|10\rangle + c_3|11\rangle$$

similar gates

$$\hat{U}'_{\mathrm{SWAP}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \hat{Y}_{12}(\pi), \qquad \hat{U}''_{\mathrm{SWAP}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -i & 0 \\ 0 & -i & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \hat{X}_{12}(\pi)$$

relation between them

$$\begin{aligned} \hat{U}_{\mathrm{SWAP}} &= \hat{U}'_{\mathrm{SWAP}} \cdot \mathrm{diag}([1,1,-1,1]) = \mathrm{diag}([1,-1,1,1]) \cdot \hat{U}'_{\mathrm{SWAP}} \\ &= \hat{U}''_{\mathrm{SWAP}} \cdot \mathrm{diag}([1,i,i,1]) = \mathrm{diag}([1,i,i,1]) \cdot \hat{U}''_{\mathrm{SWAP}} \end{aligned}$$

NMR implementations of two-qubit algorithms

1. Deutsch-Jozsa algorithm [Chuang *et al.*'98, Jones *et al.*'98]
2. Grover search algorithm [Jones *et al.*'98]
3. quantum Fourier transform [Fu *et al.*'99]
4. quantum error detection [Leung *et al.*'99]
5. quantum simulations [Somaroo *et al.*'99]
6. dense coding [Fang *et al.*'99]
7. Hogg algorithm [Zhu *et al.*'01]
8. quantum erasers [Teklemarian *et al.*'02]

Hogg algorithm – a highly structured search algorithm

What can be done with two-virtual qubits?

NMR implementations of two-qubit algorithms on spin-3/2 nuclei:

1. **demonstration of classical gates**
   [Khitrin *et al.*'00, Sinha *et al.*'01, Kumar *et al.*'02]
2. **demonstration of quantum gates**
   [Sarthour *et al.*'03, Kampermann *et al.*'02, Steffen'03,
3. **generation of Bell states**
   [Sarthour *et al.*'03, Kampermann *et al.*'02]
4. **quantum tomography**
   [Bonk *et al.*'04, Steffen'03, Kampermann *et al.*'05]

5. **Grover search algorithm**

   [Ermakov *et al.*'02, Steffen'03, Kampermann *et al.*'05]

6. **Deutsch-Jozsa algorithm**

   [Das *et al.*'03, Kampermann *et al.*'05]

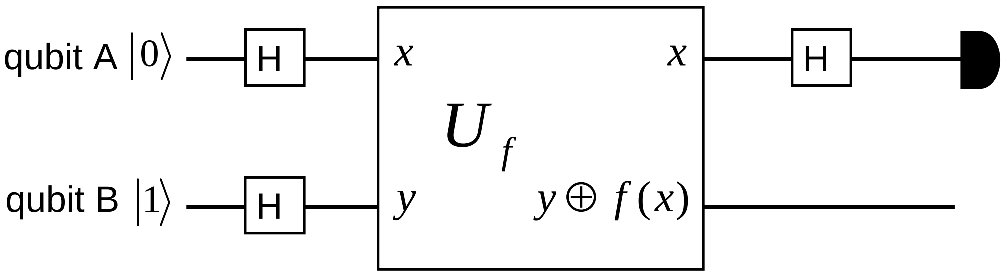
7. **quantum Fourier transform**

   [Kampermann *et al.*'05]

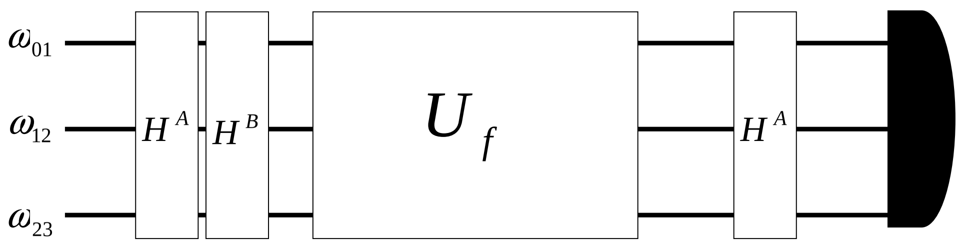
8. * quantum error detection
9. * quantum simulations
10. * dense coding
11. * Hogg algorithm
12. * quantum erasers

(∗) - not implemented yet

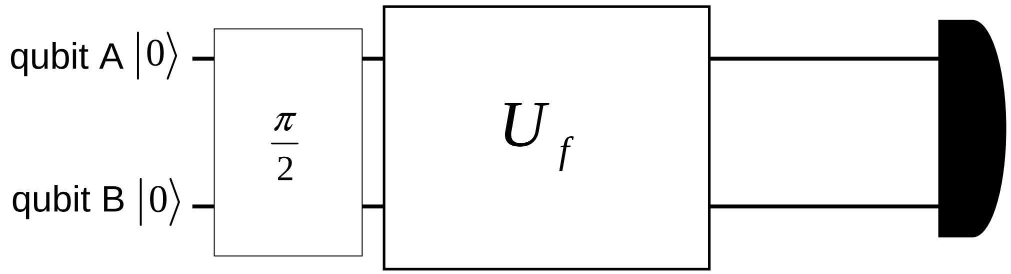
Deutsch's algorithm for two qubits



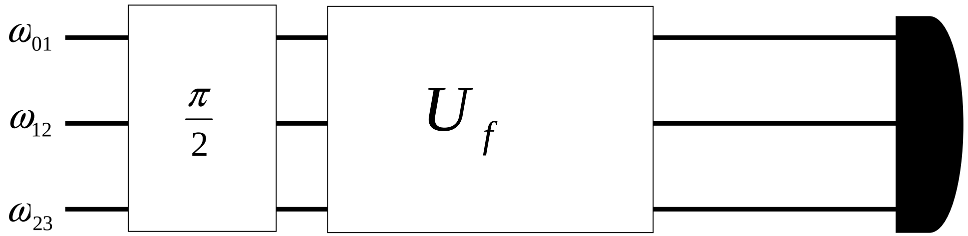
Deutsch's algorithm for a quartit



experimental Deutsch's algorithm for two qubits

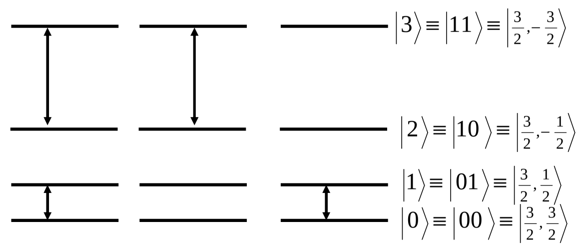


experimental Deutsch's algorithm for a quartit

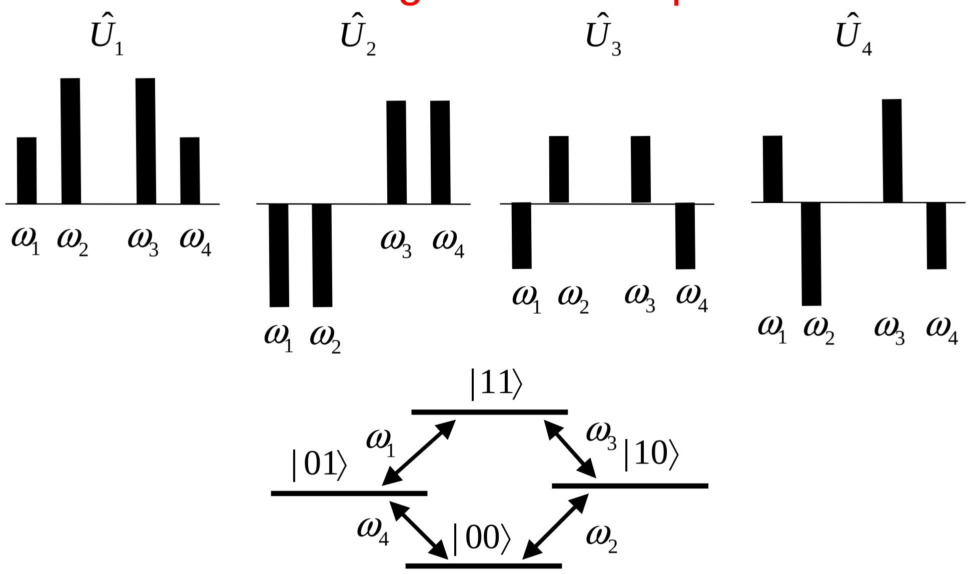


NMR pulses for the oracle in Deutsch's algorithm

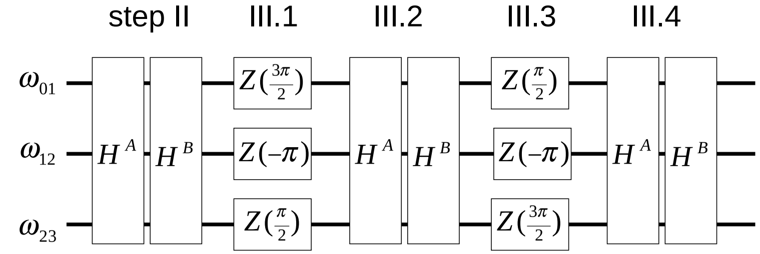
	Constant		Balanced	
	f_1	f_2	f_3	f_4
0	0	1	0	1
1	0	1	1	0
U_f	$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$	$\begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$	$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$	$\begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$
Pulse	no pulse	$\hat{X}_{01}(\pi)\hat{X}_{23}(\pi)$	$\hat{X}_{23}(\pi)$	$\hat{X}_{01}(\pi)$



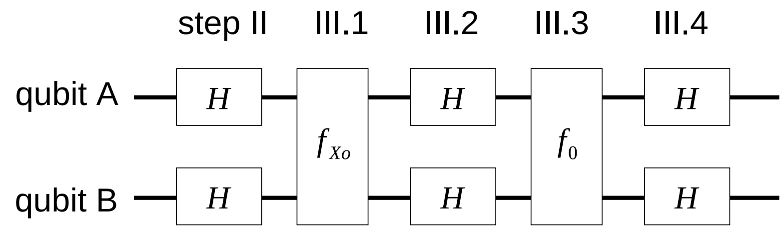
exemplary NMR spectra for Deutsch algorithm in 2 qubits



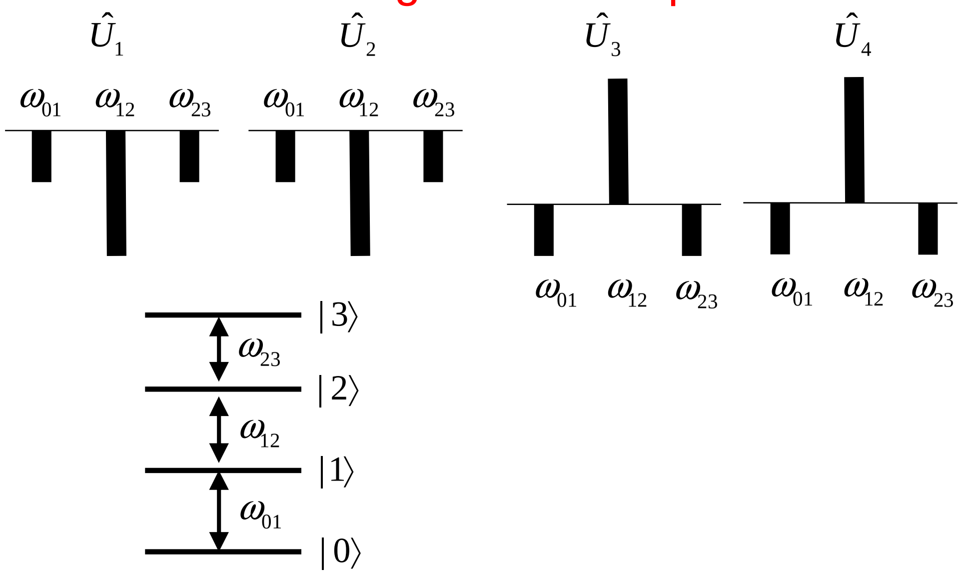
a circuit for Grover's search in a quartit



a circuit for Grover search in two qubits



exemplary NMR spectra for Deutsch algorithm in a quartit



NMR detections of magnetization of a spin-3/2

- M_{xy}-detection of a two spin-1/2 system enables determination of the off-diagonal elements marked in boxes:

$$\hat{\rho} = \begin{bmatrix} \rho_{00} & \boxed{\rho_{01}} & \boxed{\rho_{02}} & \rho_{03} \\ \boxed{\rho_{10}} & \rho_{11} & \rho_{12} & \boxed{\rho_{13}} \\ \boxed{\rho_{20}} & \rho_{21} & \rho_{22} & \boxed{\rho_{23}} \\ \rho_{30} & \boxed{\rho_{31}} & \boxed{\rho_{32}} & \rho_{33} \end{bmatrix}$$

- M_{xy}-detection of a spin-3/2 system gives the other off-diagonal elements:

$$\hat{\rho} = \begin{bmatrix} \rho_{00} & \boxed{\rho_{01}} & \rho_{02} & \rho_{03} \\ \boxed{\rho_{10}} & \rho_{11} & \boxed{\rho_{12}} & \rho_{13} \\ \rho_{20} & \boxed{\rho_{21}} & \rho_{22} & \boxed{\rho_{23}} \\ \rho_{30} & \rho_{31} & \boxed{\rho_{32}} & \rho_{33} \end{bmatrix}$$

- M_z-detection of a spin-3/2 system gives:

$$\hat{\rho} = \begin{bmatrix} \boxed{\rho_{00}} & \rho_{01} & \rho_{02} & \rho_{03} \\ \rho_{10} & \boxed{\rho_{11}} & \rho_{12} & \rho_{13} \\ \rho_{20} & \rho_{21} & \boxed{\rho_{22}} & \rho_{23} \\ \rho_{30} & \rho_{31} & \rho_{32} & \boxed{\rho_{33}} \end{bmatrix}$$

NMR quantum state tomography

is a method for complete reconstruction of a given density matrix $\hat{\rho}$ in a serious of NMR measurements.

Principle ideas

- M_{xy} and M_z detections give only some elements of $\hat{\rho}$
- The remaining matrix elements can be obtained by rotating the original density matrix $\hat{\rho}$ through properly chosen rotational operations $\hat{R}_k$:

$$\hat{\rho}^{(k)} \;=\; \hat{R}_k \hat{\rho} \hat{R}_k^{\dagger}$$

1. Chuang's set of rotations for M_{xy} tomography of 2 qubits

$$\begin{aligned}
\hat{R}_1 &= \hat{I}\otimes\hat{I}, & \hat{R}_2 &= \hat{I}\otimes\hat{X}, & \hat{R}_3 &= \hat{I}\otimes\hat{Y},\\
\hat{R}_4 &= \hat{X}\otimes\hat{I}, & \hat{R}_5 &= \hat{X}\otimes\hat{X}, & \hat{R}_6 &= \hat{X}\otimes\hat{Y},\\
\hat{R}_7 &= \hat{Y}\otimes\hat{I}, & \hat{R}_8 &= \hat{Y}\otimes\hat{X}, & \hat{R}_9 &= \hat{Y}\otimes\hat{Y}
\end{aligned}$$

where $\hat{X} \equiv \hat{X}(\frac{\pi}{2}), \hat{Y} \equiv \hat{Y}(\frac{\pi}{2})$

2. other sets of rotations for tomography of n-qubits

n=1 $\Rightarrow$ X, I **n=2** $\Rightarrow$ XX, II, IX, IY;

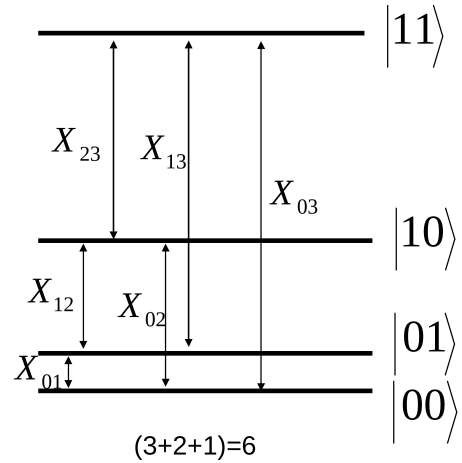
n=3 $\Rightarrow$ XXX, III, IIY, XYX, YII, XXY, IYY

n=4 $\Rightarrow$ XXXX, IIII, IIYY, YYXX, IIIY, XYXX, YXYI, IXYI, IIIX, XIYY, YXII, YYXY, XYXI, IIYX, IXIY, IIXI, IYIY

n=5 $\Rightarrow$ XXXXX, IIIII, YYYYY, IIIXX, XXYYY, YYXII, IIXIY, XYXXI, YXIYY, XXYIX, IYIXX, IIXYI, YIYXI, XXIYY, YXYXI, YYXIX, IYYYY, XIXIY, IIIYI, IXYIX, XIYYX, IXXXY, XYIXI, YXIIY, XIYIX, XYYXI, YIIXX, YYXYX, IIXXY, IXXYI, XYIII, IYYIY, YYXYY, IXIXX, XIXXY, XXXIX, XYIYI, YXYXX, IIYIY, IYIXY

n=6 $\Rightarrow$ XXXXXX, IIIIII, YYYYYY, IIXXYY, XXYYII, YYIIXX, IXIYXY, XYXIYI, YIYXIX, IIXYYX, XXYIIY, YYIXXI, IIYIXI, XXIXYX, YYXYIY, IYYXIX, XIIYXY, YXXIYI, IXIIIY, IYYXXI, XIIYYX, YIXXIY, YXXIXX, XYXYII, XYYIYY, YXYYYI, IIIXYI, IYIYXX, XIYXXX, XYXIIY, IIXIXI, IXXYYX, XXIXIX, YIIYXY, YXYIYY, IYYIIX, YYIXXY, IXYYXY, YXYYII, YYIIYX, IIIXII, XIXXXX, IYXXYY, XXXXXI, XYYYYY, IIXYIX, YIYXIY, IXIIXY, XIIIII, IXXXYY, IYIYXI, XYYIYI, YXXYXX, XXXIIY, YIIIII, YIYXYX, XYIIXX, YYXYII, YYYXXI, IXXYIX, YXIXIX, YXIYYI, IIIXYY, XIXYXY, XYXXXX, IIYIXY, IXYIYX, XIYYII, XXIXYY, XYYYYX, YIXIYI, YYYIIX, IXIYIY, IYIIYX, XXYXXX, XYIXIY, YIXIYY, IXIIXI, IXXXII, IXYXII, IYIYYI, IYXIXI, XIIIYX, XIIXYI, YIYYXX, YXYIXY, YYXXYX, IIIXXX, IIXIIX, IIYYII, XXIIXI, XXXYYX, XYYXIY, IIXYXI, IIYXYY, IYIYIX, IYXIXY, XIXXXI, YIIYXX, YXXXYY, IIIIXX, IIXYYI, IIYIIX, IIYIYX, IIYYIY, IXIYXX, IXYXYI, IYIIIY, IYXXYX, IYYYXI

tomography of 4-level system



(3+2+1)=6
so 12 readouts (including Y-rotations)

a natural set of rotations for tomography of a quartit state

- single-photon transitions

$$\begin{aligned}
\hat{R}_1 &= \hat{X}_{01}(\tfrac{\pi}{2}), & \hat{R}_2 &= \hat{Y}_{01}(\tfrac{\pi}{2})\\
\hat{R}_3 &= \hat{X}_{12}(\tfrac{\pi}{2}), & \hat{R}_4 &= \hat{Y}_{12}(\tfrac{\pi}{2})\\
\hat{R}_5 &= \hat{X}_{23}(\tfrac{\pi}{2}), & \hat{R}_6 &= \hat{Y}_{23}(\tfrac{\pi}{2})
\end{aligned}$$

- two-photon transitions

$$\begin{aligned}
\hat{R}_7 &= \hat{X}_{02}(\tfrac{\pi}{2}), & \hat{R}_8 &= \hat{Y}_{02}(\tfrac{\pi}{2})\\
\hat{R}_9 &= \hat{X}_{13}(\tfrac{\pi}{2}), & \hat{R}_{10} &= \hat{Y}_{13}(\tfrac{\pi}{2})
\end{aligned}$$

- three-photon transitions

$$\hat{R}_{11} = \hat{X}_{03}(\tfrac{\pi}{2}), \quad \hat{R}_{12} = \hat{Y}_{03}(\tfrac{\pi}{2})$$

rotations in M_z-based tomography

e.g.

$\hat{\rho}$ after $\hat{R}_1 = \hat{X}_{01}(\frac{\pi}{2})$

$$\hat{\rho}' = \begin{bmatrix} \frac{1}{2}(\rho_{00}-\rho_{01}-\rho_{10}+\rho_{11}) & \cdots & \cdots & \cdots \\ \cdots & \frac{1}{2}(\rho_{00}+\rho_{01}+\rho_{10}+\rho_{11}) & \cdots & \cdots \\ \cdots & \cdots & \rho_{22} & \cdots \\ \cdots & \cdots & \cdots & \rho_{33} \end{bmatrix}$$

$\hat{\rho}$ after $\hat{R}_5 = \hat{X}_{23}(\frac{\pi}{2})$

$$\hat{\rho}'' = \begin{bmatrix} \rho_{00} & \cdots & \cdots & \cdots \\ \cdots & \rho_{11} & \cdots & \cdots \\ \cdots & \cdots & \frac{1}{2}(\rho_{22}-\rho_{23}-\rho_{32}+\rho_{33}) & \cdots \\ \cdots & \cdots & \cdots & \frac{1}{2}(\rho_{22}+\rho_{23}+\rho_{32}+\rho_{33}) \end{bmatrix}$$

so let us apply both rotation before read-outs

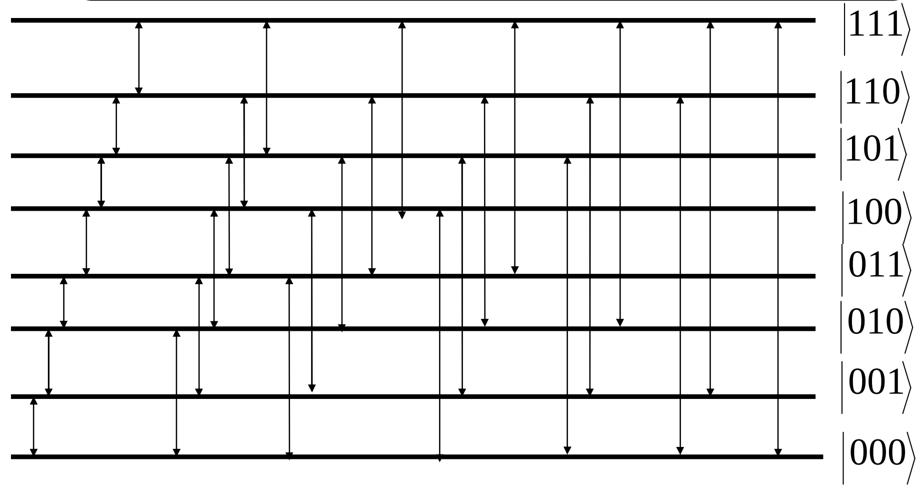
tomography without three-photon rotations

$$\begin{aligned} \hat{X}_{03}(\theta) &= \hat{Y}_{13}(\pi)\hat{X}_{01}(\theta)\hat{Y}_{13}(-\pi) \\ &= \hat{Y}_{02}(\pi)\hat{X}_{23}(-\theta)\hat{Y}_{02}(-\pi) \\ &= \hat{Y}_{01}(\pi)\hat{X}_{13}(-\theta)\hat{Y}_{01}(-\pi) \\ &= \hat{Y}_{23}(\pi)\hat{X}_{02}(\theta)\hat{Y}_{23}(-\pi) \\ &= \hat{Y}_{01}(\pi)\hat{Y}_{23}(\pi)\hat{X}_{12}(-\theta)\hat{Y}_{23}(-\pi)\hat{Y}_{01}(-\pi) \\ &= \cdots \end{aligned}$$

tomography without two-photon rotations

$$\begin{aligned} \hat{X}_{13}(\theta) &= \hat{Y}_{23}(\pi)\hat{X}_{12}(\theta)\hat{Y}_{23}(-\pi) \\ &= \hat{Y}_{12}(\pi)\hat{X}_{23}(-\theta)\hat{Y}_{12}(-\pi), \\ \hat{Y}_{13}(\theta) &= \hat{Y}_{23}(\pi)\hat{Y}_{12}(\theta)\hat{Y}_{23}(-\pi) \\ &= \hat{Y}_{12}(\pi)\hat{Y}_{23}(-\theta)\hat{Y}_{12}(-\pi), \\ \hat{X}_{02}(\theta) &= \hat{Y}_{12}(\pi)\hat{X}_{01}(\theta)\hat{Y}_{12}(-\pi) \\ &= \hat{Y}_{01}(\pi)\hat{X}_{12}(-\theta)\hat{Y}_{01}(-\pi), \\ \hat{Y}_{02}(\theta) &= \hat{Y}_{12}(\pi)\hat{Y}_{01}(\theta)\hat{Y}_{12}(-\pi) \\ &= \hat{Y}_{01}(\pi)\hat{Y}_{12}(-\theta)\hat{Y}_{01}(-\pi). \end{aligned}$$

tomography of 8-level system



7 +6 +5 +4 +3 +2 +1 = 28

so 56 readouts (including X and Y-rotations)

NMR implementations of 3-qubit algorithms on spin-1/2 nuclei

1. generation of GHZ states [Laflamme *et al.*'97]
2. quantum error correction [Cory *et al.*'98]
3. quantum teleportation [Nielsen *et al.*'98]
4. Deutsch-Jozsa algorithm [Linden *et al.*'98]
5. refined Deutsch-Jozsa algorithm for entangled qubits [Kim *et al.*'00] (a meaningful test of quantum parallelism)
6. Grover algorithm (with cancellation of systematic errors) [Vandersypen *et al.*'00]
7. quantum simulation [Tseng *et al.*'00]
8. Schulman-Vazirani algorithm (a cooling scheme) [Chang *et al.*'01]
9. noiseless subsystems [Viola *et al.*'01]
10. quantum Fourier transform [Weinstein *et al.*'01]

11. quantum erasers [Teklemarian *et al.*'01]
12. quantum chaotic map (baker's map) [Weinstein *et al.*'02]
13. phase estimation algorithm [Lee *et al.*'02]
14. Hogg algorithm [Peng *et al.*'02]
15. half-adder and subtractor operations [Murali *et al.*'02, Kumar *et al.*'02]
16. adiabatic quantum optimization algorithm [Steffen *et al.*'03]
17. quantum state and process tomography [Vandersypen *et al.*'04]
18. test of phase coherence in electromagnetically induced transparency (EIT) [Murali *et al.*'04]

NMR implementation of a seven-qubit algorithm

Shor's factorization algorithm [Vandersypen *et al.*'01]

What can be done with three virtual qubits?

possible QIP applications of spin-7/2 nuclei

- **implemented (in liquid NMR systems)**

1. quantum simulation [Khitrin *et al.*'01]
2. half-adder and subtractor operations [Murali *et al.*'02, Kumar *et al.*'02]
3. test of phase coherence in EIT [Murali *et al.*'04]

- **not implemented yet**

6. quantum tomography
7. generation of GHZ states
8. quantum error correction
9. quantum teleportation
10. logical labeling

11. Deutsch-Jozsa algorithm
12. refined Deutsch-Jozsa algorithm for entangled qubits (a meaningful test of quantum parallelism)
13. Grover algorithm (with cancellation of systematic errors)
14. Schulman-Vazirani algorithm (a cooling scheme)
15. noiseless subsystems
16. quantum Fourier transform
17. quantum erasers
18. quantum baker's map
19. phase estimation algorithm
20. Hogg algorithm
21. adiabatic quantum optimization algorithm

empirical Moore's law

Gordon E. Moore - a co-founder of Intel.

- **original Moore's law (1965)**

  The number of transistors and resistors on a chip doubles every 18 months.

- **modified Moore's law (1975)**

  The number doubles every 24 months.

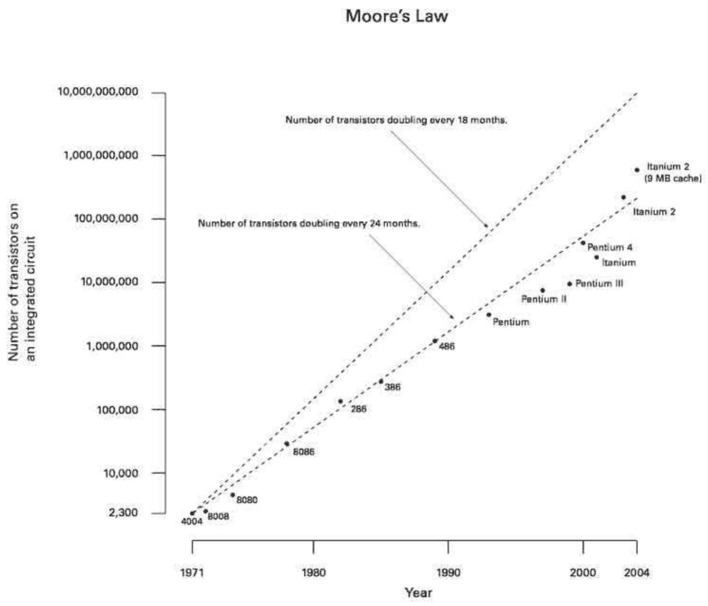
  1965 - approximately 60 devices on a chip.

  2007 - Dual-Core Intel Itanium 2 chip contains 1.7 billion transistors

- **the end of Moore's law?**

  2018 - estimated year for reaching the fundamental limits

Moore's Law



[source: Wikipedia]

end of Moore's Law?

- how to provide energy to a chip?
- how to cool down a chip?

  As power-driven heat can cause major malfunctions.

  "Chip with 3nm-length gates would overheat itself." [Gargini]
- when the gate length < 5 nm quantum effects become important

gate lengths

37 nm in 2007

$\sim$5 nm in 2015-2018

quantum tunneling

source & drain are so close that the electrons will tunnel

even if voltage is not applied to the gate

$\Rightarrow$ **Heisenberg uncertainty** becomes important

$\Rightarrow$ transistor becomes unreliable

Physical principles of quantum computing

1. Superposition
2. Interference
3. Entanglement
4. Non-cloning
5. Uncertainty

purely quantum applications of QC

1. Quantum cryptography
2. Quantum teleportation

advantages of QC

- superfast (Shor) and fast (Grover) algorithms
- understanding new aspects of measurement theory
- improvement of precision spectroscopy
- understanding dissipation in mesoscopic system
- partial control of decoherence
- quantum state engineering
- quantum simulations

Quantum Computing is the frontier of

- Information Science
- Cryptography
- Quantum physics
  including
- Quantum Optics
- Nanotechnology

"Quantum computers must be a component of any world view that seeks to be fundamental"
David Deutsch