Quantum information & computation

http://tph.tuwien.ac.at/~svozil/publ/2005-stpoelten-pres.pdf

Karl Svozil

Institut für Theoretische Physik, University of Technology Vienna,
Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria
svozil@tuwien.ac.at

Nov. 8, 2005

1. Quantum information
   - Basics & differences to classical information
   - Quantum state evolution: one-to-one
   - Mach-Zehnder interferometer
   - "Quantum mindbogglers"
   - Classical & quantum correlations and the Boole-Bell inequalities
2. Quantum computation
   - No-cloning (no-copy) theorem
   - Visions of parallelism & interference
   - Deutsch algorithm: parity of a function of one bit
   - Quantum cryptography & man-in-the-middle attacks
3. Resources
4. Conclusions

Basics & differences to classical information

- Elementary unit of classical information is the classical bit ("cbit") which is in one of the two classical states "0" or "no" or "false" and "1" or "yes" or "true," respectively.
- Elementary unit of quantum information is the quantum bit ("qubit") which can be in a *coherent superposition*

$$|\Psi\rangle = a_0|0\rangle + a_1|1\rangle, \qquad \text{with} \quad |a_0|^2 + |a_1|^2 = 1$$

  of the classical states "0" and "1."
- A single qubit "embodies" two classically contradictory states at once. This is the basis of "quantum parallelism."
- n single qubits "embody" 2^n classically contradictory states at once. A linear increase of quantum information is associated with an exponential increase of embodied classically states – "quantum parallelism."

Representations of cbits & qubits

- Representation of the two cbits as orthogonal vectors in a two-dimensional vector space:

$$0 \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \qquad 1 \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

- Representation of qubits as normalized vectors in a two-dimensional vector space:

$$|\Psi\rangle = a_0|0\rangle + a_1|1\rangle \equiv \begin{pmatrix} a_1 \\ a_0 \end{pmatrix}, \quad \text{with } |a_0|^2 + |a_1|^2 = 1.$$

Quantum state evolution: one-to-one

- Classical reversible computation associated with permutations of the classical states associated with permutation matrices (only a single entry "1" per row & column, else "0").
- Inbetween measurements, quantum states follow reversible deterministic, unitary state evolution:

$$|\Psi_{\rm later}\rangle = U|\Psi_{\rm former}\rangle.$$

- U is a unitary matrix: $UU^\dagger = U[(U^*)^T] = 1$; i.e., $U^\dagger = U^{-1}$. Here,
  - "$*$" stands for "complex conjugate,"
  - "T" stands for "transposition," and
  - "$\dagger$" stands for "hermitean conjugate" ("$= *\&T$"), respectively.

Quantum state evolution: Examples

- The identity defined by $|\mathbf{0}\rangle \rightarrow |\mathbf{0}\rangle$, $|\mathbf{1}\rangle \rightarrow |\mathbf{1}\rangle$: $\mathbb{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$,
- the "$\mathtt{not}$" defined by $|\mathbf{0}\rangle \rightarrow |\mathbf{1}\rangle$, $|\mathbf{1}\rangle \rightarrow |\mathbf{0}\rangle$:

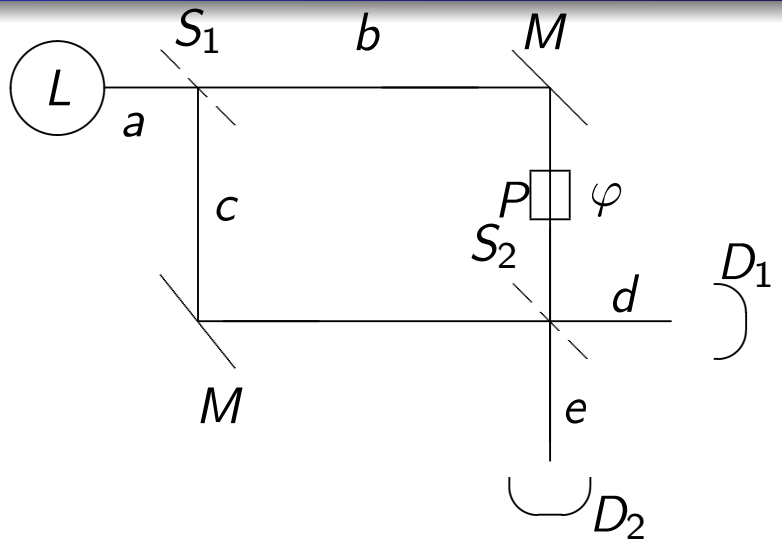
$$\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

- the Hadamard "$\mathbf{H} = \sqrt{\mathbb{I}_2}$," defined by $|\mathbf{0}\rangle \rightarrow (|\mathbf{0}\rangle + |\mathbf{1}\rangle)(1/\sqrt{2})$, $|\mathbf{1}\rangle \rightarrow (|\mathbf{0}\rangle - |\mathbf{1}\rangle)(1/\sqrt{2})$:

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

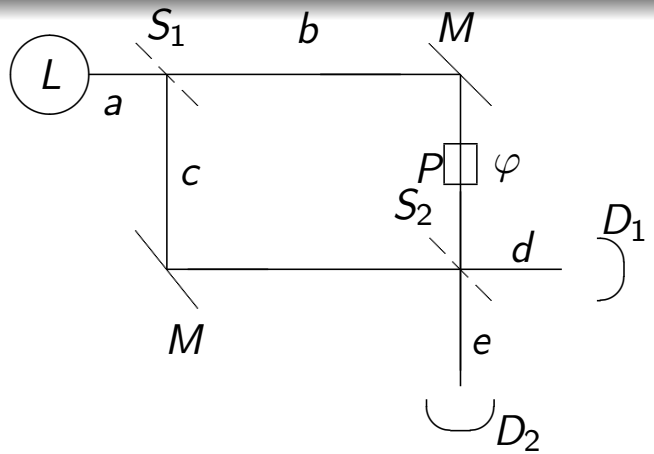
  with $\sqrt{\mathbb{I}_2} \cdot \sqrt{\mathbb{I}_2} = \mathbb{I}_2$,
- the $\sqrt{\mathtt{not}}$: $\frac{1}{2} \begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$ with $\sqrt{\mathtt{not}}\sqrt{\mathtt{not}} = \mathtt{not}$.

Mach-Zehnder interferometer



Mach-Zehnder interferometer. A single quantum (photon, neutron, electron *etc*) is emitted in L and meets a lossless beam splitter (half-silvered mirror) S_1, after which its wave function is in a coherent superposition of b and c. In beam path b a phase shifter shifts the phase of state b by φ. The two beams are then recombined at a second lossless beam splitter (half-silvered mirror) S_2. The quant is detected at either D_1 or D_2, corresponding to the states d and e, respectively.

Mach-Zehnder interferometer cntd.



$$\begin{aligned} S_1 &: a \rightarrow (b+ic)/\sqrt{2} \quad , \\ P &: b \rightarrow be^{i\varphi} \quad , \\ S_2 &: b \rightarrow (e+id)/\sqrt{2} \quad , \\ S_2 &: c \rightarrow (d+ie)/\sqrt{2} \quad . \end{aligned}$$

$$a \rightarrow \psi = i\left(\frac{e^{i\varphi}+1}{2}\right)d + \left(\frac{e^{i\varphi}-1}{2}\right)e.$$

$\varphi = 0$, i.e., there is no phase shift at all: $a \rightarrow id$, and the emitted quant is detected only by D_1.
$\varphi = \pi$: $a \rightarrow -e$, and the emitted quant is detected only by D_2.
For general phase shift φ:

$$P_{D_1}(\varphi) = |(d,\psi)|^2 = \cos^2(\frac{\varphi}{2}) \quad , \quad P_{D_2}(\varphi) = |(e,\psi)|^2 = \sin^2(\frac{\varphi}{2}) \quad .$$

Alternative representations

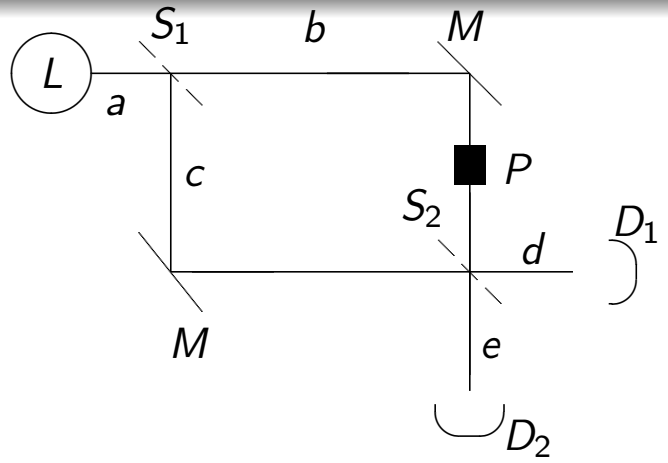
Alternatively, the action of a lossless beam splitter may be described by the unitary matrix

$$\begin{pmatrix} i\sqrt{R(\omega)} & \sqrt{T(\omega)} \\ \sqrt{T(\omega)} & i\sqrt{R(\omega)} \end{pmatrix} = \begin{pmatrix} i\sin\omega & \cos\omega \\ \cos\omega & i\sin\omega \end{pmatrix}.$$

A phase shifter in two-dimensional Hilbert space is represented by either the unitary matrix

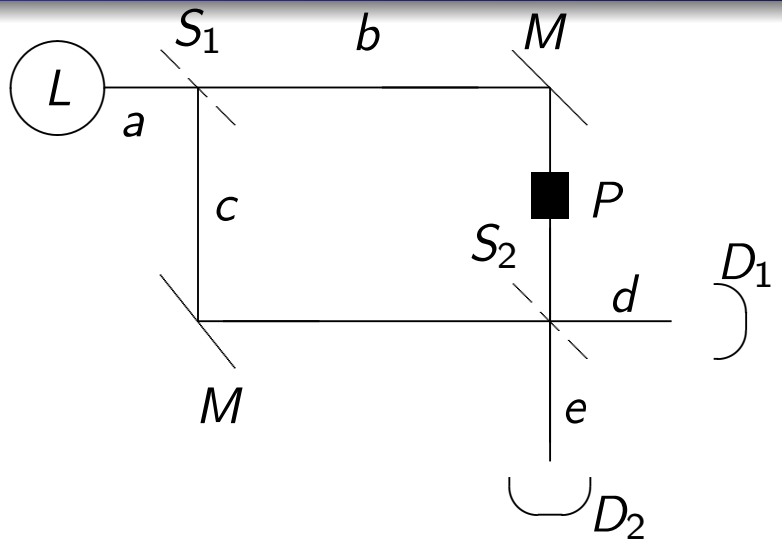
$$\mathrm{diag}\left(e^{i\varphi},1\right) \qquad \text{or} \qquad \mathrm{diag}\left(1,e^{i\varphi}\right).$$

"Interaction-free" measurement



Case #1: Suppose, P is not a beam splitter, but a perfect absorber. Then, the beam path b is blocked entirely, leaving open only beam path c, resulting in a 50:50 chance that detectors D_1 and D_2 fire.
Case #2: Suppose, P is a transparent medium (no absorber): since $\varphi \equiv 0$: only D_1 fires.
Hence: if we want to know whether or not an absorber is in beam path b, then whenever D_2 fires (in 1/4 of all cases), we know that the absorber is present although the quant "has not touched it." We als say that "no interachtion has taken place between the absorber & the quant." Has it not ;-)
SINGLE QUANT (QUBIT) EFFECT!!!!!

"Delayed choice" measurements



Suppose we block beam path b with an absorber at P only *after* the quant has "passed" the first 50:50 mirror at S_1 and is "somewhere inbetween S_1 and P."
Would this make any difference as compared to blocking the path b beforehand; i.e., before the quant has "passed" the first 50:50 mirror at S_1?
Guess what happens ;-)
SINGLE QUANT (QUBIT) EFFECT!!!!!

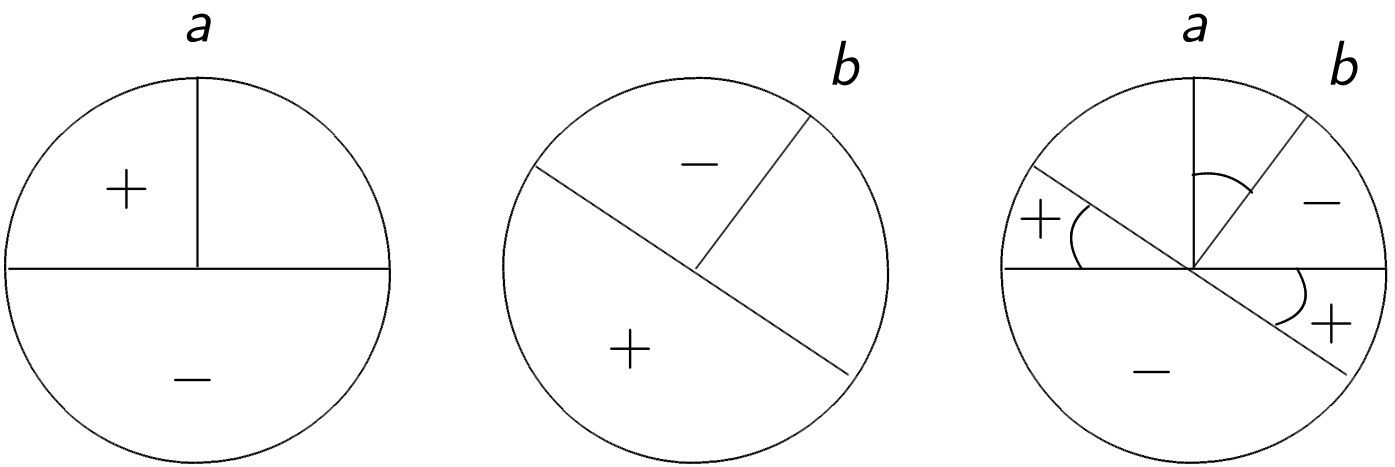
General setup

- Two measurement directions a and b of two dichotomic observables with values "-1" and "1" at two spatially separated locations.
- The measurement direction a at "Alice's location" is unknown to an observer "Bob" measuring b and *vice versa*.
- A two-particle correlation function $E(\theta)$ with $\theta = |a - b|$ is defined by averaging the product of the outcomes $O(a)_i, O(b)_i \in -1, 1$ in the ith experiment; i.e., $E(\theta) = (1/N) \sum_{i=1}^{N} O(a)_i O(b)_i$.

Classical correlations for two-particle "perfectly correlated" state

Assume uniform distribution of (opposite) "angular momentum" of the two particles; Alice measuring along angle a, Bob measuring along b:

$$E(a,b) = \frac{A_+(a,b) - A_-(a,b)}{2\pi} = \frac{2A_+(a,b) - 2\pi}{2\pi} = \\ = \frac{2}{\pi}|a-b| - 1 = \frac{2}{\pi}\theta - 1$$



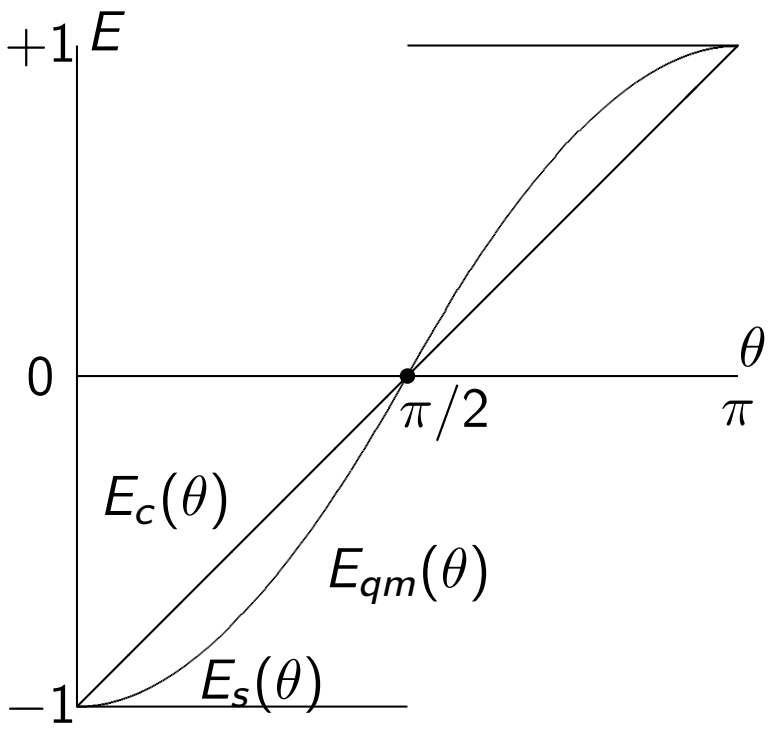
Quantum correlations for two-particle singlet state

$$E(\theta) = 3/[j(j+1)]C(\theta)$$

with non-normalized

$$\begin{aligned}
C(\theta) &= \langle J=0, M=0 \mid \alpha\cdot\hat{J}^A \otimes \beta\cdot\hat{J}^B \mid J=0, M=0\rangle \\
&= \sum_{m,m'} \langle 00 \mid jm, j-m\rangle\langle jm', j-m' \mid 00\rangle \times \\
&\qquad \times {}^A\langle jm \mid {}^B \langle j-m \mid \alpha\cdot\hat{J}^A \otimes \beta\cdot\hat{J}^B \mid jm'\rangle^A \mid j-m'\rangle^B \\
&= \sum_{m,m'} \langle 00 \mid jm, j-m\rangle\langle jm', j-m' \mid 00\rangle \times \\
&\qquad \times \langle jm \mid \alpha\cdot\hat{J}^A \mid jm'\rangle\langle j-m \mid \beta\cdot\hat{J}^B \mid j-m'\rangle \\
&= \sum_{m,m'} \frac{(-1)^{j-m}(-1)^{j-m'}}{2j+1} \langle jm \mid \hat{J}_z^A \mid jm'\rangle\langle j-m \mid \beta\cdot\hat{J}^B \mid j-m'\rangle \\
&= \sum_{m,m'} \frac{(-1)^{j-m}(-1)^{j-m'}}{2j+1} m\delta_{mm'}\langle j-m \mid \beta\cdot\hat{J}^B \mid j-m'\rangle \\
&= \sum_{m} m\frac{(-1)^{2j-2m}}{2j+1}\langle j-m \mid \beta\cdot\hat{J}^B \mid j-m\rangle = \frac{1}{2j+1}\sum_m -m^2\beta_z = -\frac{1}{2j+1}\cos\theta\sum_{m=-j}^{j} m^2 \qquad \text{for } 0\le\theta\le\pi \\
&= -\frac{j(j+1)}{3}\cos\theta \qquad \text{for } 0\le\theta\le\pi \quad .
\end{aligned}$$

Two-particle correlations cntd.



More anti-coincidences of detector clicks between $0 < \theta < \pi/2$;
more coincidences of detector clicks between $\pi/2 < \theta < \pi$;
same-as-classical and quantum for $\theta = 0, \pi/2, \pi$.

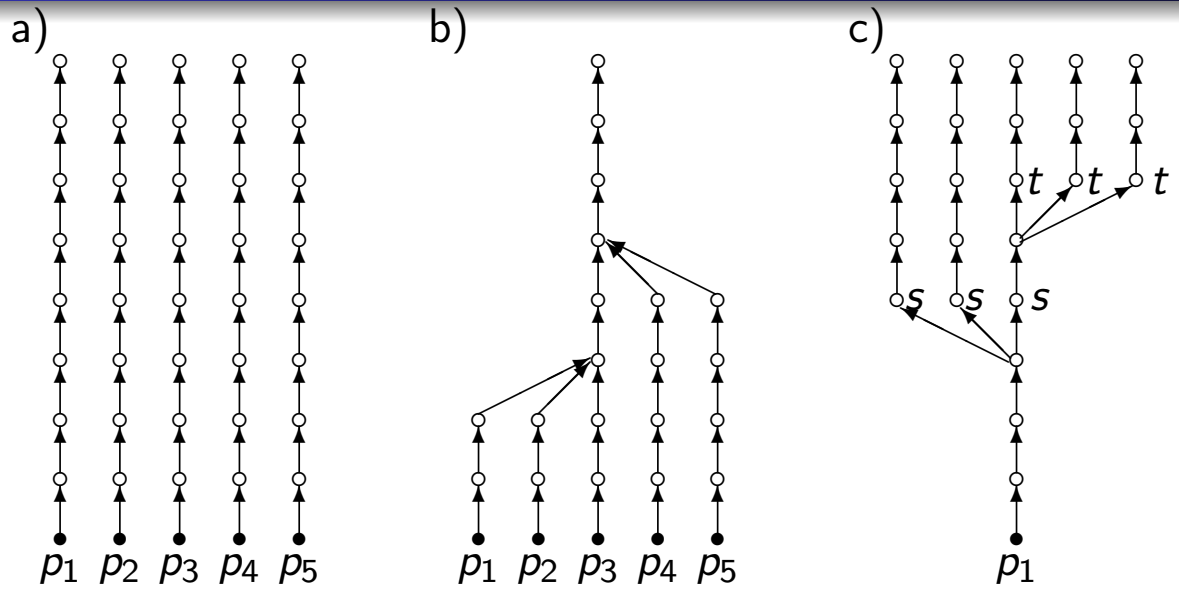
Boole-Bell-type inequalities

- Would you believe that (i) it rains in Vienna with probability 80%; (ii) it rains in Budapest with probability 80%; (i)&(ii) it rains in Vienna & jointly in Budapest with probability 0.1% ? Exactly when would you start believing me?
- Around 1860 Boole: "conditions of possible experience" (in "Laws of Thought")
- Around 1965 Bell: similar inequalities as classical bounds for probabilities of joint events.
- Pitowsky & others: geometric interpretation as "inside–outside" conditions with regards to faces of correlation polytopes: Take all possibilities of classical events. Take their joints. Interpret the entries in the truth tables as vectors in a vector space. These vectors form the vertices of a "correlation polytope" formed by the convex sum. The surface of this polytope represents all classical probability distributions. The faces of this polytope form the inside–outside relations. They are represented by Boole-Bell inequalities.

Kochen-Specker theorem & quantum "meaning"

- "It is impossible to consistently (re)construct an entire set of quantum properties from its parts. Therefore, a comprehensive list of 'elements of physical reality' cannot exist."
  Simon Kochen and Ernst P. Specker, "The Problem of Hidden Variables in Quantum Mechanics," Journal of Mathematics and Mechanics 17(1), pp.59-87 (1967)
  Review in Karl Svozil, "Quantum Logic," (Springer, Singapore,1998)
- Feynman: "Nobody understands quantum mechanics." (in "The Character of Physical Law")
- Is it useless to even think about possible interpretations of the formalism; even more so to go beyond the quantum? Will the human mine ever transcend the quantum world? Strong anti-rationalist tendencies (Bohr, Heisenberg,... versus Einstein, Schrödinger, De Broglie, ...).

Reversible, one-to-one computation



The lowest "root" represents the initial state interpretable as program. Forward computation represents upwards motion through a sequence of states represented by open circles. Different symbols p_i correspond to different initial states, that is, different programs. a) One-to-one computation. b) Many-to-one junction which is information discarding. Several computational paths, moving upwards, merge into one. c) One-to-many computation is allowed only if no information is created and discarded; e.g., in copy-type operations on blank memory.

No-cloning (no-copy) theorem

- Ideally, a perfect qcopy device A, acting upon an arbitrary state ψ and some arbitrary blank state b, would do this:

$$\psi \otimes |b\rangle \otimes |A_i\rangle \longrightarrow \psi \otimes \psi \otimes |A_f\rangle.$$

- Suppose it would copy the two "quasi-classical" state "$+$" and "$-$" accordingly:

$$|+, b, A_i\rangle \longrightarrow |+, +, A_f\rangle, \qquad |-, b, A_i\rangle \longrightarrow |-, -, A_f\rangle.$$

- By the linearity of quantum mechanics, the state $\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$ is copied according to

$$\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \otimes |b, A_i\rangle \longrightarrow \frac{1}{\sqrt{2}}(|+, +, A_f\rangle + |-, -, A_f\rangle)$$

$$\neq \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \otimes \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \otimes |A_i\rangle.$$

Visions of parallelism & interference

- A single qubit "embodies" two classically contradictory states at once. This is the basis of "quantum parallelism."
- n single qubits "embody" 2^n classically contradictory states at once. A linear increase of quantum information is associated with an exponential increase of embodied classically states – "quantum parallelism."
- The information in N qubits can be coded in a "distributed" ("entangled") manner, such that measurement of a single qubit "destroys" this information and makes a readout impossible.
- Encoding of a classical decision problem by
  - "folding" a quantum state as a coherent superposition of all (contradictory) classical cases
  - processing this coherent superposition; and finally
  - "unfolding" the processed state properly such that a readout of the unfolded state presents the solution to the decision problem (equivalent to a state identification).

Deutsch algorithm: parity of a function of one bit

f	0	1
f_0	0	0
f_1	0	1
f_2	1	0
f_3	1	1

Table: The binary functions of one bit considered in Deutsch's problem.

Interlude: definition of elementary unitary operations on single bits

- $\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is the *not*-operator
- $\mathbf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is the normalized Hadamard matrix

Three step strategy

- First step: unfold the quantum bit
- Second step: process the quantum bit
- Third step: read out the quantum bit

To preserve reversibility of information processing, start with two bits instead of one (undorgoing an irreversible functional transformation f):

$$\mathbf{U}_f(|x\rangle|y\rangle) = |x\rangle|y \oplus f(x)\rangle$$

Deutsch algorithm: parity of a function of one bit cntd.

- Start with $|0\rangle|0\rangle$ [or rather $(\mathbf{X}\otimes\mathbf{X})(|0\rangle|0\rangle)$ for convenience];
- then "unfold" with the two Hadamards $\mathbf{H}\otimes\mathbf{H}$;
- then apply $\mathbf{U}_f$

	$\frac{1}{2}[\|0\rangle\|0\oplus f(0)\rangle$	-	$\|0\rangle\|1\oplus f(0)\rangle$	-	$\|1\rangle\|0\oplus f(1)\rangle$	+	$\|1\rangle\|1\oplus f(1)\rangle]$
f_0: ψ_1	$\frac{1}{2}(\|0\rangle\|0\rangle$	-	$\|0\rangle\|1\rangle$	-	$\|1\rangle\|0\rangle$	+	$\|1\rangle\|1\rangle)$
f_1: ψ_2	$\frac{1}{2}(\|0\rangle\|0\rangle$	-	$\|0\rangle\|1\rangle$	-	$\|1\rangle\|1\rangle$	+	$\|1\rangle\|0\rangle)$
f_2: $-\psi_2$	$\frac{1}{2}(\|0\rangle\|1\rangle$	-	$\|0\rangle\|0\rangle$	-	$\|1\rangle\|0\rangle$	+	$\|1\rangle\|1\rangle)$
f_3: $-\psi_1$	$\frac{1}{2}(\|0\rangle\|1\rangle$	-	$\|0\rangle\|0\rangle$	-	$\|1\rangle\|1\rangle$	+	$\|1\rangle\|0\rangle)$

Table: State evolution of $\mathbf{U}_f(\mathbf{H}\otimes\mathbf{H})(\mathbf{X}\otimes\mathbf{X})(|0\rangle|0\rangle)$ for the four functions f_0, f_1, f_2, f_3. $\mathbf{X}$ and $\mathbf{H}$ stand for the not operator and the (normalized) Hadamard transformation.

Third step: Readout & state identification in Deutsch's case

- The encoding Ansatz $\mathbf{U}_f(\mathbf{H}\otimes\mathbf{H})(\mathbf{X}\otimes\mathbf{X})(|0\rangle|0\rangle)$, resulting in the two different states

$$|\psi_1\rangle = \pm\frac{1}{2}(|0\rangle-|1\rangle)(|0\rangle-|1\rangle) \equiv \pm\frac{1}{2}((1,-1)\otimes(1,-1))^T = \pm\frac{1}{2}(1,-1,-1,1)^T$$

for f_0 as well as f_3, and

$$|\psi_2\rangle = \pm\frac{1}{2}(|0\rangle+|1\rangle)(|0\rangle-|1\rangle) \equiv \pm\frac{1}{2}((1,1)\otimes(1,-1))^T = \pm\frac{1}{2}(1,-1,1,-1)^T$$

for f_1 as well as f_2.

- Finally, application of two additional Hadamard-transformations for each one of the two bits yields a representation in the standard computational basis; i.e.,

$$(\mathbf{H}\otimes\mathbf{H})\mathbf{U}_f(\mathbf{H}\otimes\mathbf{H})(\mathbf{X}\otimes\mathbf{X})(|0\rangle|0\rangle) = \begin{cases} |1\rangle|1\rangle \equiv (0,0,0,1)^T & \text{for } f(0)=f(1), \\ |0\rangle|1\rangle \equiv (0,1,0,0)^T & \text{for } f(0)\neq f(1). \end{cases}$$

Other speedups incl. factoring & database search

- Finding the period of a function, related to prime factorization, related to RSA encryption "Shor's" algorithm.
- Finding whether or not a function acquires "1" on an argument space or is "0" everywhere ("database search").
- General parity cannot be substantially sped up.

What may and may not be possible

- Speedup for all problems translatable into state identification problems.
- Speedup questionable for problems which are classically recursion theoretic hard, such as the Ackermann or the Busy Beaver function.
- Still no quantum speedup for NP-complete problems.

History

1970 Stephen Wiesner, *"Conjugate coding:"* noisy transmission of two or more "complementary messages" by using single photons in two or more complementary polarization directions/bases.

1984 BB84 Protocol: key growing via quantum channel & additional classical bidirectional communication channel

1989 First realization by Bennett et al. at 1989 IBM Yorktown Heights, 1993 by Gisin across Lake Geneva, 2003-present DARPA Network Boston (permanent real-time).

BB84 Protocol

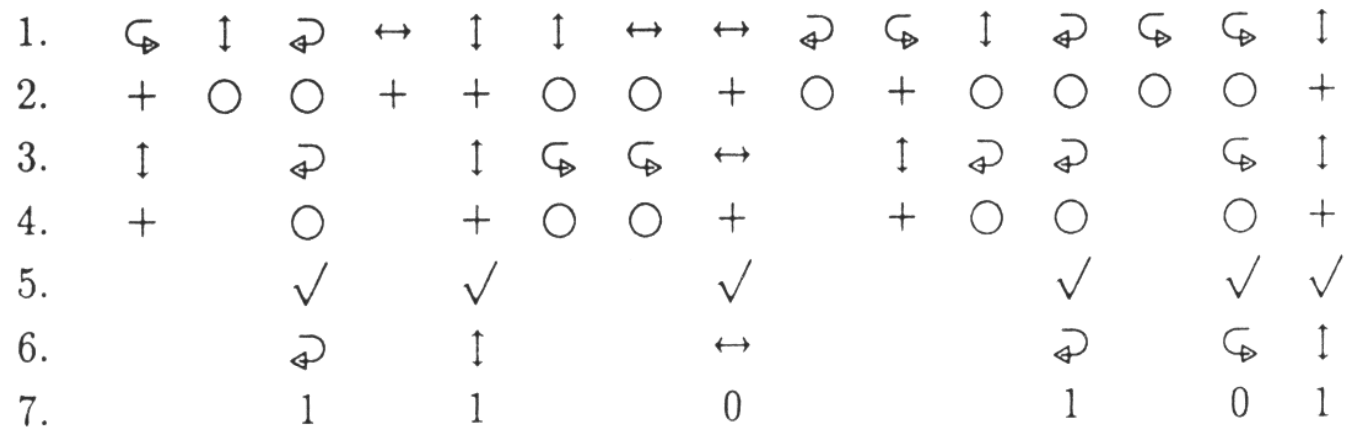
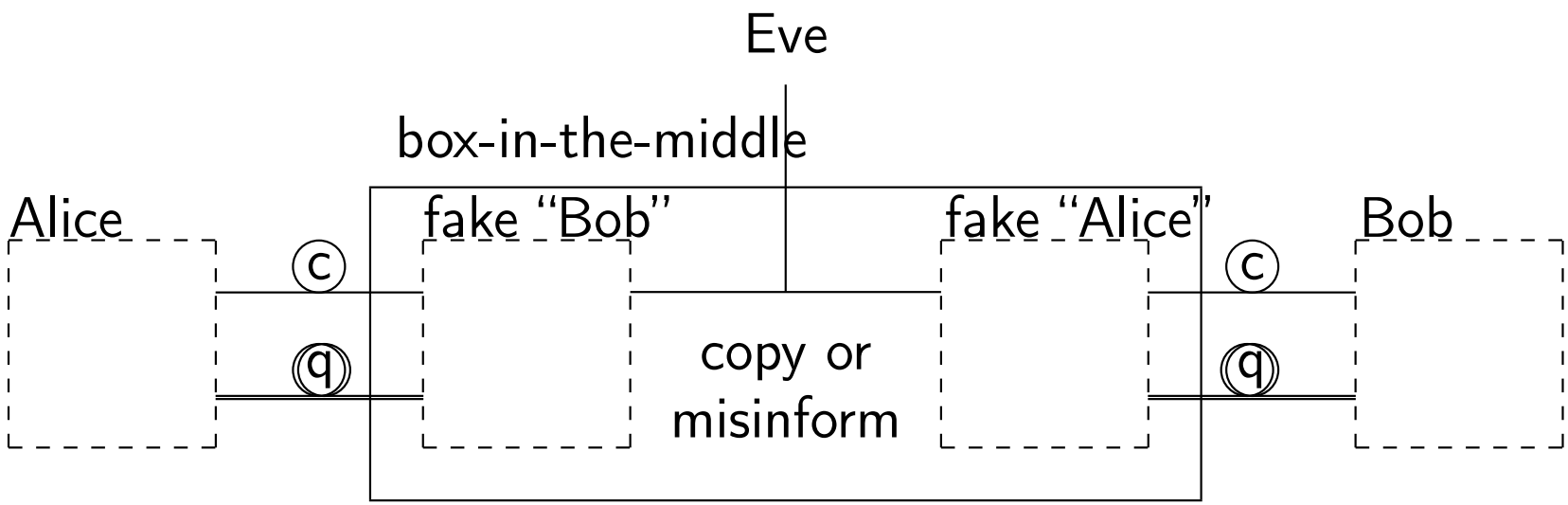


Fig. 1. Basic quantum key distribution protocol.

1. Alice sends a random sequence of photons polarized horizontal (↔), vertical (↕), right-circular (↻) and left-circular (↺);
2. Bob measures the photons' polarization in a random sequence of bases, rectilinear (+) and circular (○).
3. Results of Bob's measurements (some photons may not be received at all).
4. Bob tells Alice which basis he used for each photon he received;
5. Alice tells him which bases were correct;
6. Alice and Bob keep only the data from these correctly-measured photons, discarding all the rest.
7. This data is interpreted as a binary sequence according to the coding scheme ↔ = ↺ = 0 and

Man-in-the-middle attack: requiring classical authorization (merely "key growing")



from http://arxiv.org/abs/quant-ph/0501062

Techniques & gadgets

- Photon sources: faint laser pulses, photon pairs generated by parametric downconversion, photon guns, ...
- Quantum channels: single-mode fibers, free-space links, ...
- Single-photon detection: photon counters, ...
- (Quantum) Random number generators: calcite prism, ...

Resources

- David Mermin's qc lecture: very good, very popular:
  http://people.ccmr.cornell.edu/∼mermin/qcomp/CS483.html
- Up-to-May 2005 collection of findings & open questions:
  M. Arndt et al., "Quantum Physics from A to Z"
  http://www.arxiv.org/abs/quant-ph/0505187
- Older, very influential article by Schrödinger (the "cat" papers):
  E. Schrödinger, "Die gegenwärtige Situation in der Quantenmechanik", Naturwissenschaften 23, pp.807-812; 823-828; 844-849 (1935).
  http://wwwthep.physik.uni-mainz.de/∼matschul/rot/schroedinger.pdf
- Quantum "measurement" paradoxes:
  L. Vaidman, Z. Naturforsch. 56 a, 100-107 (2001)
  http://arxiv.org/abs/quant-ph/0102049
- Staging quantum cryptography with chocolate balls
  http://arxiv.org/abs/physics/0510050
- Up-to-date discussion on (subscribable abstracts):
  http://arxiv.org/archive/quant-ph

Conclusions

- Single quantum concepts and their experimental realization.
- Novel phenomena which go beyond the classical field.
- Possible application in quantum information processing.
- With growing integration & miniaturization, thechnology will "reach the quanta" soon.
- Many open questions, active & fascinating research field!

Thank you for your attention!