Emerging Technologies

http://tph.tuwien.ac.at/∼svozil/publ/2009-EmTech-pres.pdf

Karl Svozil

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

SS 2009

tu-logo

tu-logo

Part I: Foundations of Computer Science

tu-logo

What is an algorithm?

Informally, the concept of an algorithm is often illustrated by the example of a recipe for accomplishing some task; e.g., cooking. It involves “paper–&–pencil operations.”

`cooking-11697-large.pdf`

tu-logo

Church-Turing Thesis

The informal notion of “algorithm” can be formalized by the formalized notion of “recursive function.”

What is a “recursive function?”

Problem: As Deutsch puts it,

“The reason why we find it possible to construct, say, electronic calculators, and indeed why we can perform mental arithmetic, cannot be found in mathematics or logic. The reason is that the laws of physics ‘happen to’ permit the existence of physical models for the operations of arithmetic *such as addition, subtraction and multiplication. If they did not, these familiar operations would be noncomputable functions. We might still know* of *them and invoke them in mathematical proofs (which would presumably be called ‘nonconstructive’) but we could not perform them.”*

D. Deutsch, *Quantum theory, the Church-Turing principle and the universal quantum computer*, Proceedings of the Royal Society London **A 400**, 97–119 (1985).

algorithm cntd.

" . . . how can we ever exclude the possibility of our presented, some day (perhaps by some extraterrestrial visitors), with a (perhaps extremely complex) device or "oracle" that "computes" a noncomputable function?"
M. Davis, *Computability and Unsolvability* (McGraw-Hill, New York, 1958).

Turing computability

Alan Turing enshrined that part of mathematics, which can be "constructed" by paper and pencil operations, into a Turing machine which possesses a potentially unbounded one-dimensional tape divided into cells, some finite memory and some read-write head which transfers back and forth information from the tape to this memory. A table of transition rules figuring as the "program" steers the machine deterministically. The behaviour of a Turing machine may also be determined by its initial state.

Furthermore, a universal Turing machine is capable of simulating all other Turing machines (including itself).

A. M. Turing, *On computable numbers, with an application to the Entscheidungsproblem,* Proceedings of the London Mathematical Society, Series 2 **42 and 43**, 230–265 and 544–546 (1936-7 and 1937).

tu-logo

Universality and robustness

- Universality: a universal computer can simulate all other ones (including itself ;-)
- Robustness: any “robust” formalizations are essentially equivalent; i.e., any formalism can be somehow “translated” one-to-one into any other one of that “robust” class ;-)

tu-logo

Turing uncomputability and the halting problem

Consider a universal computer U and an arbitrary algorithm $B(X)$ whose input is a string of symbols X. Assume that there exists a "halting algorithm" $\texttt{HALT}$ which is able to decide whether B terminates on X or not. The domain of $\texttt{HALT}$ is the set of legal programs. The range of $\texttt{HALT}$ are classical bits.
Using $\texttt{HALT}(B(X))$ we shall construct another deterministic computing agent A, which has as input any effective program B and which proceeds as follows: Upon reading the program B as input, A makes a copy of it. This can be readily achieved, since the program B is presented to A in some encoded form $\ulcorner B \urcorner$, i.e., as a string of symbols. In the next step, the agent uses the code $\ulcorner B \urcorner$ as input string for B itself; i.e., A forms $B(\ulcorner B \urcorner)$, henceforth denoted by $B(B)$. The agent now hands $B(B)$ over to its subroutine $\texttt{HALT}$. Then, A proceeds as follows: if $\texttt{HALT}(B(B))$ decides that $B(B)$ halts, then the agent A does not halt; this can for instance be realized by an infinite DO-loop; if $\texttt{HALT}(B(B))$ decides that $B(B)$ does *not* halt, then A halts.

The agent A will now be confronted with the following paradoxical task: take the own code as input and proceed to determine whether or not it halts. Then, whenever $A(A)$ halts, $\texttt{HALT}(A(A))$, by the definition of A, would force $A(A)$ not to halt. Conversely, whenever $A(A)$ does not halt, then $\texttt{HALT}(A(A))$ would steer $A(A)$ into the halting mode. In both cases one arrives at a complete contradiction. Classically, this contradiction can only be consistently avoided by assuming the nonexistence of A and, since the only nontrivial feature of A is the use of the peculiar halting algorithm $\texttt{HALT}$, the impossibility of any such halting algorithm.

tu-logo

Undecidability of the rule inference (induction) problem

Induction in physics is the inference of general rules dominating and generating physical behaviors from these behaviors. For any deterministic system strong enough to support universal computation, the general induction problem is provable unsolvable. Induction is thereby reduced to the unsolvability of the rule inference problem,

Informally, the algorithmic idea of the proof is to take any sufficiently powerful rule or method of induction and, in using it, define some functional behavior which is not identified by it. This amounts to constructing an algorithm which (passively!) “fakes” the “guesser” by simulating some particular function φ until the guesser pretends to guess this function correctly. In a second, diagonalization step, the “faking” algorithm then switches to a different function $\varphi^* \neq \varphi$, such that the guesser's guesses become incorrect.

tu-logo

Busy Beaver Number

The busy beaver function addresses the following question: given a finite system; i.e., a system whose algorithmic description is of finite length. What is the biggest number producible by such a system before halting?

Let $\Sigma(n)$ denote the busy beaver function of n. Originally, T. Rado asked how many 1's a Turing machine with n possible states and an empty input tape could print on that tape before halting.

The first values of the Turing busy beaver function $\Sigma_T(x)$ are finite and are known:

$\Sigma_T(1) = 1$,
$\Sigma_T(2) = 4$,
$\Sigma_T(3) = 6$,
$\Sigma_T(4) = 13$,
$\Sigma_T(5) \geq 1915$,
$\Sigma_T(7) \geq 22961$,
$\Sigma_T(8) \geq 3 \cdot (7 \cdot 3^{92} - 1)/2$.

tu-logo

Omega Number

Omega Ω, the halting probability, is the sum

$$\sum_{U(p)\downarrow} 2^{-|p|}$$

of all halting, prefix-free programs of some universal computer U.

tu-logo

Continuum urn

With probability 1, a real initial value “taken from the continuum urn” is uncomputable (indeed, algorithmically incompressible = random). In the measure theoretic sense, “almost all” reals are uncomputable. This can be demonstrated by the following argument: Let $M = \{r_i\}$ be an infinite point set (i.e., M is a set of points r_i) which is denumerable and which is the subset of a dense set. Then, for instance, every $r_i \in M$ can be enclosed in the interval

$$I(i,\delta) = [r_i - 2^{-i-1}\delta, r_i + 2^{-i-1}\delta] \quad , \tag{1}$$

where δ may be arbitrary small (we choose δ to be small enough that all intervals are disjoint). Since M is denumerable, the measure μ of these intervals can be summed up, yielding

$$\sum_i \mu(I(i,\delta)) = \delta \sum_{i=1}^{\infty} 2^{-i} = \delta \quad . \tag{2}$$

From $\delta \to 0$ follows $\mu(M) = 0$.

NP complexity class

- In computational complexity theory, NP ("Non-deterministic Polynomial time") is the set of problems solvable
  - by non-deterministic "oracles" and
  - polynomial time verifiability
- NP completeness
  An NP-complete problem is one which is robust in the following sense: it is in NP and it is NP-hard, i.e. every other problem in NP is reducible to it.
  Example: "travelling salesman"
  Garey, M. and D. Johnson, Computers and Intractability; A Guide to the Theory of NP-Completeness, 1979
- Karp-Cook Thesis
  $NP \neq P$
  No proof so far.

tu-logo

Part II: Physical foundations of computation

tu-logo

Maxwell's Demon

MaxwellsDemon.pdf

tu-logo

Maxwell's Demon

MaxwellsDemonPicture.pdf

tu-logo

Maxwell's Demon

MaxwellsDemonPicture2.pdf

tu-logo

Maxwell's Demon

MaxwellsDemonPicture3.pdf

Maxwell's Demon

MaxwellsDemonPicture4.pdf

Information theoretic “solution” to Maxwell’s Demon

R. Landauer, Irreversibility and Heat Generation in the Computing Process, IBM Journal of Research and Development **3**, 183-191 (1961)

- logical irreversibility in connection with information-discarding processes — “cleared” memory can be from a variety of previous states
- Each logical step must somehow correspond to a physical state
- (“the bad news”) logical irreversibility is associated with physical “heat dissipation” and “entropy increase” ;-(
- (“the good news”) logically reversibile operations need not be associated with physical “heat dissipation” and “entropy increase” ;-)

tu-logo

Modern-day “solution” of Maxwell’s question cntd.

emtech-demon-op.pdf

Reversible computation from irreversible one

Charles H. Bennett, Logical Reversibility of Computation, IBM Journal of Research and Development **17**, 525-532 (1973).
Charles H. Bennett, The Thermodynamics of Computation—A Review, International Journal of Theoretical Physics **21**, 905-940 (1982).

- Every (irreversible) computer can be made logically reversible at every step
- saving of all intermediate results, avoiding erasure
- copy of computation "result;" outcome
- reverse computation to "get rid" of the intermediate results,
- one is left with the original "input" and one copy of the "output"
- splitting up the computation into many steps results in less memory requirements

tu-logo

Reversible computation from irreversible one

MaxwellsDemonBennett71.pdf

tu-logo

Reversible computation from irreversible one

MaxwellsDemonBennett71-2.pdf

Information theoretic “solution” to Maxwell’s Demon cntd.

- As Maxwell’s demon acquires information while performing its task, it “heats up.”
- Setting Maxwell’s demon into its initial configuration means erasure of informations, which in turn means energy dissipation.

tu-logo

Why all this?

- Consider this: “information is physical;” i.e., has a physical representation.
- Due to the (unitary) quantum evolution, quantum computation is reversible.

tu-logo

Cellular Automata

- John von Neumann, Theory of Self-Reproducing Automata, (A. W. Burks, editor), University of Illinois Press, Urbana, 1966
- Konrad Zuse, Rechnender Raum, Elektronische Datenverarbeitung, **8**, 336-344, (1967)
  URL: http://www.idsia.ch/˜juergen/digitalphysics.html

tu-logo

Cellular Automata

CellularAutomaton.pdf

tu-logo

Billiard Ball Cellular Automata

BBCellularAutomaton.pdf

tu-logo

Computational Complementarity and generalized urn model

Edward F. Moore, Gedanken-Experiments on Sequential Machines, in Automata Studies, ed. by C. E. Shannon and J. McCarthy, (Princeton University Press, Princeton 1956)

SubwayAutomaton.pdf

Part III: Quantum Mechanics

tu-logo

Hilbert space

All quantum mechanical entities are represented by objects of Hilbert spaces. A *Hilbert space* is a linear vector space $\mathcal{H}$ over the field Φ of complex numbers (with vector addition and scalar multiplication), together with a complex function $(\cdot,\cdot)$, the *scalar* or *inner product*, defined on $\mathcal{H} \times \mathcal{H}$ such that (i) $(x,x) = 0$ if and only if $x = 0$; (ii) $(x,x) \geq 0$ for all $x \in \mathcal{H}$; (iii) $(x+y,z) = (x,z) + (y,z)$ for all $x,y,z \in \mathcal{H}$; (iv) $(\alpha x, y) = \alpha(x,y)$ for all $x,y \in \mathcal{H}, \alpha \in \Phi$; (v) $(x,y) = \overline{(y,x)}$ for all $x,y \in \mathcal{H}$ ($\overline{\alpha}$ stands for the complex conjugate of α); (vi) If $x_n \in \mathcal{H}$, $n = 1,2,\ldots$, and if $\lim_{n,m\rightarrow\infty}(x_n - x_m, x_n - x_m) = 0$, then there exists an $x \in \mathcal{H}$ with $\lim_{n\rightarrow\infty}(x_n - x, x_n - x) = 0$.

State

A pure *physical state* is represented by a vector of the Hilbert space $\mathcal{H}$. Therefore, if two vectors $x, y \in \mathcal{H}$ represent physical states, their vector sum $z = x + y \in \mathcal{H}$ represent a physical state as well. This state z is called the *coherent superposition* of state x and y. Coherent state superpositions will become most important in quantum information theory.

tu-logo

Observables

Observables A are represented by self-adjoint operators A on the Hilbert space $\mathcal{H}$ such that $(Ax, y) = (x, Ay)$ for all $x, y \in \mathcal{H}$. (Observables and their corresponding operators are identified.)
In what follows, unless stated differently, only *finite* dimensional Hilbert spaces are considered. Then, the vectors corresponding to states can be written as usual vectors in complex Hilbert space. Furthermore, bounded self-adjoint operators are equivalent to bounded Hermitean operators. They can be represented by matrices, and the self-adjoint conjugation is just transposition and complex conjugation of the matrix elements.

tu-logo

Elements $b_i, b_j \in \mathcal{H}$ of the set of orthonormal base vectors satisfy $(b_i, b_j) = \delta_{ij}$, where δ_{ij} is the Kronecker delta function. Any state x can be written as a linear combination of the set of orthonormal base vectors $\{b_1, b_2, \cdots\}$, i.e., $x = \sum_{i=1}^{N} \beta_i b_i$, where N is the dimension of $\mathcal{H}$ and $\beta_i = (b_i, x) \in \Phi$. In the Dirac bra-ket notation, unity is given by $\mathbf{1} = \sum_{i=1}^{N} |b_i\rangle\langle b_i|$. Furthermore, any Hermitean operator has a spectral representation $A = \sum_{i=1}^{N} \alpha_i P_i$, where the P_i's are orthogonal projection operators onto the orthonormal eigenvectors a_i of A (nondegenerate case).

Complementarity

Observables are said to be *compatible* if they can be defined simultaneously with arbitrary accuracy; i.e., if they are "independent." A criterion for compatibility is the *commutator.* Two observables A, B are compatible, if their *commutator* vanishes; i.e., if $[A, B] = AB - BA = 0$. For example, position and momentum operators $[\mathfrak{x}, \mathfrak{p}_x] = \mathfrak{x}\mathfrak{p}_x - \mathfrak{p}_x\mathfrak{x} = x\frac{\hbar}{i}\frac{\partial}{\partial x} - \frac{\hbar}{i}\frac{\partial}{\partial x}x = i\,\hbar \neq 0$ and thus do not commute. Therefore, position and momentum of a state cannot be measured simultaneously with arbitrary accuracy. It can be shown that this property gives rise to the *Heisenberg uncertainty relations* $\Delta x \Delta p_x \geq \frac{\hbar}{2}$, where Δx and Δp_x is given by $\Delta x = \sqrt{\langle x^2 \rangle - \langle x \rangle^2}$ and $\Delta p_x = \sqrt{\langle p_x^2 \rangle - \langle p_x \rangle^2}$, respectively.

Outcome

The result of any single measurement of the observable A on a state $x \in \mathcal{H}$ can only be one of the real eigenvalues of the corresponding Hermitean operator A. If x is in a coherent superposition of eigenstates of A, the particular outcome of any such single measurement is indeterministic; i.e., it cannot be predicted with certainty. As a result of the measurement, the system is in the state which corresponds to the eigenvector a_n of A with the associated real-valued eigenvalue α_n; i.e., $Ax = \alpha_n a_n$ (no summation convention here).

tu-logo

Evolution

This “transition” $x \rightarrow a_n$ has given rise to speculations concerning the “collapse of the wave function (state).” But, as has been argued recently, it is possible to reconstruct coherence; i.e., to “reverse the collapse of the wave function (state)” if the process of measurement is reversible. After this reconstruction, no information about the measurement must be left, not even in principle.

How did Schrödinger, the creator of wave mechanics, perceive the ψ-function? In his 1935 paper "Die Gegenwärtige Situation in der Quantenmechanik" ("The present situation in quantum mechanics"), Schrödinger states,

> Die ψ-Funktion als Katalog der Erwartung: ... *Sie [[die ψ-Funktion]] ist jetzt das Instrument zur Voraussage der Wahrscheinlichkeit von Maßzahlen. In ihr ist die jeweils erreichte Summe theoretisch begründeter Zukunftserwartung verkörpert, gleichsam wie in einem* Katalog *niedergelegt. ... Bei jeder Messung ist man genötigt, der ψ-Funktion (=dem Voraussagenkatalog) eine eigenartige, etwas plötzliche Veränderung zuzuschreiben, die von der* gefundenen Maßzahl *abhängt und sich* nicht vorhersehen läßt; *woraus allein schon deutlich ist, daß diese zweite Art von Veränderung der ψ-Funktion mit ihrem regelmäßigen Abrollen* zwischen *zwei Messungen nicht das mindeste zu tun hat. Die abrupte Veränderung durch die Messung ... ist der interessanteste Punkt der ganzen Theorie. Es ist genau* der *Punkt, der den Bruch mit dem naiven Realismus verlangt. Aus* diesem *Grund kann man die ψ-Funktion* nicht *direkt an die Stelle des Modells oder des Realdings setzen. Und zwar nicht etwa weil man einem Realding oder einem Modell nicht abrupte unvorhergesehene Änderungen zumuten dürfte, sondern weil vom realistischen Standpunkt die Beobachtung ein Naturvorgang ist wie jeder andere und nicht per se eine Unterbrechung des regelmäßigen Naturlaufs hervorrufen darf.*

It therefore seems not unreasonable to state that, epistemologically, quantum mechanics is more a theory of knowledge of an (intrinsic) observer rather than the platonistic physics "God knows." The wave function, i.e., the state of the physical system in a particular representation (base), is a representation of the observer's knowledge; it is a representation or name or code or index of the information or knowledge the observer has access to.

Probability

The probability $P_y(x)$ to find a system represented by state x in some state y of an orthonormalized basis is given by $P_y(x) = |(x, y)|^2$.

tu-logo

Expectation value

The *average value* or *expectation value* of an observable A in the state x is given by $\langle A \rangle_x = \sum_{i=1}^N \alpha_i |(x, a_i)|^2$.

tu-logo

The dynamical law or equation of motion can be written in the form $x(t) = Ux(t_0)$, where $U^\dagger = U^{-1}$ ("$\dagger$ stands for transposition and complex conjugation) is a linear *unitary evolution operator*. The *Schrödinger equation* $i\hbar\frac{\partial}{\partial t}\psi(t) = H\psi(t)$ is obtained by identifying U with $U = e^{-iHt/\hbar}$, where H is a self-adjoint Hamiltonian ("energy") operator, by differentiating the equation of motion with respect to the time variable t; i.e., $\frac{\partial}{\partial t}\psi(t) = -\frac{iH}{\hbar}e^{-iHt/\hbar}\psi(t_0) = -\frac{iH}{\hbar}\psi(t)$.

tu-logo

In terms of the set of orthonormal base vectors $\{b_1, b_2, \ldots\}$, the Schrödinger equation can be written as $i\hbar\frac{\partial}{\partial t}(b_i, \psi(t)) = \sum_j H_{ij}(b_j, \psi(t))$. In the case of position base states $\psi(x,t) = (x, \psi(t))$, the Schrödinger equation takes on the form $i\hbar\frac{\partial}{\partial t}\psi(x,t) = H\psi(x,t) = \left[\frac{\mathfrak{p}\mathfrak{p}}{2m} + V(x)\right]\psi(x,t) = \left[-\frac{\hbar^2}{2m}\nabla^2 + V(x)\right]\psi(x,t)$.

tu-logo

For stationary $\psi_n(t) = e^{-(i/\hbar)E_n t}\psi_n$, the Schrödinger equation can be brought into its time-independent form $H\,\psi_n = E_n\,\psi_n$. Here, $i\hbar\frac{\partial}{\partial t}\psi_n(t) = E_n\,\psi_n(t)$ has been used; E_n and ψ_n stand for the n'th eigenvalue and eigenstate of H, respectively.

tu-logo

Usually, a physical problem is defined by the Hamiltonian H. The problem of finding the physically relevant states reduces to finding a complete set of eigenvalues and eigenstates of H. Most elegant solutions utilize the symmetries of the problem, i.e., of H. There exist two “canonical” examples, the $1/r$-potential and the harmonic oscillator potential, which can be solved wonderfully by these methods (and they are presented over and over again in standard courses of quantum mechanics), but not many more.

tu-logo

Part IV: Universal Quantum Computation

tu-logo

Concepts

Qubits are the fundamental units of quantum information. They refer to quantum states and observables which behave nonclassically; in particular they are capable of

- randomness of single events,
- complementarity (incompleteness),
- value indefiniteness (randomness),
- coherent superpositions (parallel co-representation of classically mutually excluding cases), and
- entanglement (information spread over a multitude of particles or observables),
- "interaction-free" counterfactual potentiality.

At the same time they are subject to *reversibility* in-between "irreversible" measurements.
All of these features can be used to efficiently and securely compute, distribute and transfer information.

tu-logo

Status

- Quantum cryptography is implemented [bbn.com/DARPA (US), idquantique.com (Switzerland), magiqtech.com (US/Australia), qinetiq.com (UK), NEC (Japan), Siemens (Austria/Germany), . . .];
- Quantum computer hardware not (yet?) existent; e.g., problems with maintaining coherence; still needed: a "quantum transistor;"
- Quantum algorithms:
  - Deutsch-type algorithm (counterexample: parity is qcomp-hard; gain only factor 2);
  - Factoring (Shor's algorithm): speedup may or may not be exponential;
  - Grover's search algorithm (quadratic speedup).

tu-logo

Universal Quantum Computation

- Quantum computation uses *arbitrary unitary transformations* $U^{-1} = U^{\dagger} = (U^{*})^{T}$ of quantum states in n–dimensional Hilbert space as the "universal" model of computation.
- Two-qbit operations are sufficient to guarantee "classical universality" in the sense of Church-Turing computability.
- By definition, unitary transformations are *"reversible."* If the functions f they code are irreversible, more auxiliary "tracking" bits are necessary:

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

  with $\oplus$ standing for the sum modulo two, for which $z \oplus z = 0$ for all $z \in \{0,1\}$ (this guarantees reversibility!).
- Thus, during a computation, all information is transformed one-to-one. There is no possibility to *copy* arbitrary qubits (one-to-many), or get rid of them (many-to-one). The classical analogy are *permutations*.

tu-logo

No-Cloning (no-copy) theorem

- Consider some state $|\psi\rangle$ which needs to be copied, and some blank state $|b\rangle$ which serves as "blank quantum paper", as well as some "quantum copier" represented by a unitary transformation U. Then, ideally, for arbitrary states $|\psi\rangle$,

$$U(|\psi\rangle|b\rangle) = |\psi\rangle|\psi\rangle.$$

- Unfortunately, for the coherent superposition $\alpha_\varphi|\varphi\rangle + \alpha_\psi|\psi\rangle$ of two arbitrary states $|\varphi\rangle$ and $|\psi\rangle$, with $U(|\varphi\rangle|b\rangle) = |\varphi\rangle|\varphi\rangle$, due to linearity,

$$U(\alpha_\psi|\psi\rangle + \alpha_\varphi|\varphi\rangle) = \alpha_\psi|\psi\rangle|\psi\rangle + \alpha_\varphi|\varphi\rangle|\varphi\rangle,$$

- whereas a "true copy" would be

$$\begin{aligned}(\alpha_\psi|\psi\rangle + \alpha_\varphi|\varphi\rangle)(\alpha_\psi|\psi\rangle + \alpha_\varphi|\varphi\rangle) =& \\ = \alpha_\psi^2|\psi\rangle|\psi\rangle + \alpha_\psi\alpha_\varphi(|\psi\rangle|\varphi\rangle + |\varphi\rangle|\psi\rangle) + \alpha_\varphi^2|\varphi\rangle|\varphi\rangle.&\end{aligned}$$

Due to linearity (unitarity), we *miss* all the *interference* terms.

tu-logo

No-Cloning (no-copy) theorem cntd.

Nevertheless, one could still attempt to copy quantum states

$$
\begin{aligned}
&U(|\psi\rangle|b\rangle) = |\psi\rangle|\psi\rangle \text{ and}\\
&[U(|\varphi\rangle|b\rangle)]^t = \langle\varphi|\langle b|U^{-1} = \langle\varphi|\langle\varphi|.
\end{aligned}
$$

Since $\langle b|b\rangle = 1$ and

$$
\begin{aligned}
&\langle\varphi|\langle\varphi|\psi\rangle|\psi\rangle = \langle\varphi|\psi\rangle^2 =\\
&\qquad = \langle\varphi|\langle b|U^{-1}U(|\psi\rangle|b\rangle) = \langle\varphi|\psi\rangle,
\end{aligned}
$$

is only satisfied by either $\langle\varphi|\psi\rangle = 0$ or 1, two nonidentical states ψ and φ can only be simultaneously copied if they are *orthogonal*; all other states cannot be copied. This is a generalization of the fact that classical bits can be copied.

tu-logo

Qbit versus Cbit

Let the *classical bit states* (cbit) be represented by 2-dim vectors:

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix} .$$

The *quantum bit (qbit) states* are the *coherent superposition* of cbits

$$\alpha_0|0\rangle + \alpha_1|1\rangle \equiv \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}, \quad \text{with} \quad |\alpha_0|^2 + |\alpha_1|^2 = 1.$$

Quantum mechanics allows the co-representation of two classically contradictory bit states in one qbit.

Quantum parallelism

In general, n qbits can co-represent 2^n cbits.

tu-logo

Quantum parallelism

Hadamard “spread”, “not” and $\sqrt{\text{“not”}}$ operators

$$\mathbf{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},\ \mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ \sqrt{\mathbf{X}} = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}.$$

Effect of **X** on cbits: negation; i.e.,

$$\mathbf{X}|0\rangle = |1\rangle, \quad \mathbf{H}|1\rangle = |0\rangle.$$

Effect of **H** on cbits: they become qbits; i.e.,

$$\mathbf{H}|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \quad \mathbf{H}|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right).$$

Part V:
Spread–Fold–Detect

tu-logo

Solving decision problems by “spreading” functional behaviour over multipartite states

(Classical) Information can be encoded by distributing it over different particles or quanta, such that:

- measurements of *single* quanta are irrelevant, yield “random” results, and even destroy the original information (by asking complementary questions);
- well defined correlations exist and can be defined among different particles or quanta — even to the extent that a state is solely defined by propositions ($\equiv$ projectors) about *collective* (or *relative*) properties of the particles or quanta involved;
- identifying a given state of a quantized system can yield information about *collective* (or *relative*) properties of the particles or quanta involved.

Related physical concepts

- Quantum entanglement (Schrödinger's "Verschränkung"): the state of two or more "entangled" particles or quanta cannot be constructed from or decomposed into (tensor) products of the states of the "single" particles or quanta involved. E.g., in *The essence of entanglement* [quant-ph/0106119], Brukner, Zukowski & Zeilinger write: *"the information in a composite system resides more in the correlations than in properties of individuals."*
- Zeilinger's foundational principle: *"An elementary system carries 1 bit of information."* ... more generally: n elementary d-state systems (like particles or quanta) carry exactly n dits of information.
- Example: the (singlet) Bell state $\frac{1}{\sqrt{2}}\left(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle\right)$ of two electrons is defined by the properties that the two particles have opposite spin when measured along two (or more) different (orthogonal) directions.

tu-logo

Quantum encoding decision problems about “collective” behaviours

Suppose one is interested in a decision problem which could be associated with some *“collective”* property or behaviour related to or involving, for instance,

- a function over a wide range of its arguments,
- which is of “comparative” nature; that is, only the relative functional values count;
- such that the single functional values are irrelevant; e.g., are of no interest, “annoying” or are otherwise unnecessary.

Then it is not completely unreasonable to speculate that one could use the kind of distributive information capacity encountered in the quantum physics of multipartite states for a more effective (encryption of the) solution.

tu-logo

Deutsch's problem: parity of a function of one bit

Find out whether or not an unknown function f that takes a single (classical) bit into a single (classical) bit is constant or not constant, which is equal to finding the parity of $f : \{0,1\} \rightarrow \{0,1\}$

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

tu-logo

Solution of Deutsch's problem

With

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

the solution of Deutsch's problem is

$$(\mathbf{H} \otimes \mathbf{1})\mathbf{U}_f(\mathbf{H} \otimes \mathbf{H})(\mathbf{X} \otimes \mathbf{X})(|0\rangle|0\rangle) =$$

$$= \begin{cases} |1\rangle \frac{1}{\sqrt{2}}\left(|f(0)\rangle - |1 \oplus f(0)\rangle\right) & \text{for } f(0) = f(1), \\ |0\rangle \frac{1}{\sqrt{2}}\left(|f(0)\rangle - |1 \oplus f(0)\rangle\right) & \text{for } f(0) \neq f(1). \end{cases}$$

Answer obtainable in a *single* cycle. This is impossible classically.

However, the parity of a function has been proven to be quantum computationally hard Farhi et al., 1998: It is only possible to go from 2^k classical queries down to $2^k/2$ quantum queries, thereby gaining a factor of 2.

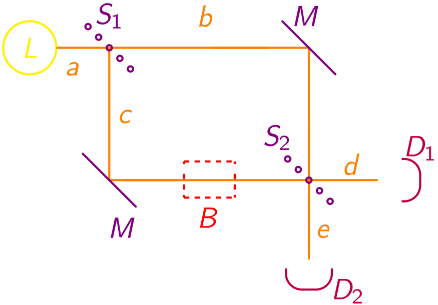
Other (possible) quantum speedups

- Shor's prime factoring algorism; prime factoring is *not* in NP-complete, may also be solvable by classical polynomial means;
- Grover's "database search" algorithm; speedup "only" quadratic and thus polynomial;
- ?!

tu-logo

Counterfactual computation (Elitzur and Vaidman, 1993)

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. 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.

tu-logo

Counterfactual computation cntd.

The computer is prepared to solve a decision problem, such that — *if* the particle takes pass c towards the computer — activates it and lets the photon pass through ("yes"), or blocks it ("no"); corresponding to the absence or presence of a bomb.

Case 1: Decision problem yields "yes" and thus path is free: The computation proceeds by successive substitution (transition) of states: let "i" stand for a phase factor from the beam reflection at 90 degrees, then

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

The resulting transition is (normalization factors omitted)

$$a \rightarrow b+ic \rightarrow id + 0 \cdot e = id \quad .$$

Thus, the emitted quant is always detected D_1, never in D_2.

Counterfactual computation cntd.

Case 2: Decision problem yields “no” and thus path is blocked: “Bomb” B presence is implemented by setting $c = 0$; i.e.,

$$\begin{aligned} S_1: \; a &\rightarrow (b + ic)/\sqrt{2} \quad , \\ B: \; c &\rightarrow 0, \\ S_2: \; b &\rightarrow (e + id)/\sqrt{2} \quad , \end{aligned}$$

The resulting transition is (normalization factors omitted)

$$a \rightarrow b \rightarrow e + id \quad .$$

The emitted quant — necessarily having taken path b *without* activating the computer (!) — is detected with 50:50 chance in D_1 or D_2. Thus, if D_2 clicks, we have certainty that the decision problem yields “no” without even having started the computation.

tu-logo

Part VI: Quantum cryptography

tu-logo

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

1991 EPR-Ekert protocol: maximally entangled state, three complementary polarization directions; additional security confirmation by violation of Bell-type inequality through data which cannot be directly used for coding

tu-logo

Man-in-the-middle attacks

- Not save against man–in–the–middle attacks.
- Due to complementarity and value indefiniteness save against eavesdropping on the (quantum) channel.
- Compare: “Standard quantum key distribution protocols are provably secure against eavesdropping attacks, if quantum theory is correct.” (from http://arxiv.org/abs/quant-ph/0405101).
- “The need for the public (non-quantum) channel in this scheme to be immune to active eavesdropping can be relaxed if the Alice and Bob have agreed beforehand on a small secret [[classical cryptographic]] key,.." (from BB84: C. H. Bennett and G. Brassard, 1984), pp. 175-179.)
- More realistic: “In accordance with our general philosophy that QKD forms a part of an overall cryptographic architecture, and not an entirely novel architecture of its own, the DARPA Quantum Network currently employs the standardized authentication mechanisms built into the Internet security architecture (IPsec), and in particular those provided by the Internet Key Exchange (IKE) protocol.” (from http://arxiv.org/abs/quant-ph/0503058)

BB84 Protocol

2005-qcrypt-pres-BBBSS92.pdf

Literature

- Introductory: N. David Mermin, *"Quantum Computer Science"* (Cambridge University Press, 2007) http://people.ccmr.cornell.edu/ mermin/qcomp/CS483.html
- Extended: M. A. Nielsen and I. L. Chuang, *"Quantum Computation and Quantum Information"* (Cambridge University Press, 2000)
- John Preskill's Caltech lecture notes, available at URL http://www.theory.caltech.edu/people/preskill/ph229/

tu-logo

Thank you for your attention!