Journal of Universal Computer Science, vol. 2, no. 5 (1996), 311-346
submitted: 13/5/96, accepted: 13/5/96, appeared: 28/5/96 © Springer Pub. Co.

QUANTUM ALGORITHMIC INFORMATION THEORY [1]

K. Svozil
Institut für Theoretische Physik, University of Technology Vienna, Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria, email: svozil@tph.tuwien.ac.at, www: http://tph.tuwien.ac.at/esvozil.

Abstract: *The agenda of quantum algorithmic information theory, ordered 'top-down,' is the quantum halting amplitude, followed by the quantum algorithmic information content, which in turn requires the theory of quantum computation. The fundamental atoms processed by quantum computation are the quantum bits which are dealt with in quantum information theory. The theory of quantum computation will be based upon a model of universal quantum computer whose elementary unit is a two-port interferometer capable of arbitrary $U(2)$ transformations. Basic to all these considerations is quantum theory, which is most conveniently expressible in Hilbert space.*

1 Information is physical, so is computation

The reasoning in constructive mathematics [16, 19, 20] and recursion theory, at least insofar as their applicability to worldly things is concerned, makes implicit assumptions about the operationalizability of the entities of discourse. It is this postulated correspondence between practical and theoretical objects, subsumed by the Church-Turing thesis, which confers power to the formal methods. Therefore, any finding in physics concerns the formal sciences; at least insofar as they claim to be applicable in the physical universe. In this sense one might quite justifiably say that the Church-Turing thesis is under permanent physical attack.[2]

[1] C. Calude (ed.). *The Finite, the Unbounded and the Infinite, Proceedings of the Summer School "Chaitin Complexity and Applications"*, Mangalia, Romania, 27 June – 6 July, 1995.

[2] For an early discussion of this topic, see Davis [31, p. 11]:

> *"... 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 non computable function?"*

A main theme of Landauer's work has been the connections between physics and computation; see, for example, his 1967 article [62] *"Wanted: a physically possible theory of physics,"* or his more recent survey [64] *"Information is physical."* See also Rosen [84]. As Deutsch puts it more recently [34, p. 101],

> *"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 non-computable functions. We might still know* of *them and invoke them in mathematical proofs (which would presumably be called 'non constructive') but we could not perform them."*

Conversely, any feature of the (constructive or non-constructive [16, 19, 96]) formalism should correspond to some physically operationalizable [21] property.

Hence, any theory of information, if applicable, has to deal with entities which are operational [21, 64, 62, 60, 65]. In Bridgman's words [22, p. V],

> *"the meaning of one's terms are to be found by an analysis of the operations which one performs in applying the term in concrete situations or in verifying the truth of statements or in finding the answers to questions."*

In particular, the fundamental atom of information, the bit, must be represented by whatever physical theories are available and must be experimentally producible and manipulable by whatever physical operations are available.

The classical digital computer, at least up to finite resources, seems to be a canonical example for physical information representation and processing. Classical digital computers, however, are designed to behave classically. That is, if functioning correctly, certain of their physical states can be mapped one-to-one onto the set of classical bit states. (This is achieved by appropriately filtering out noise.) The set of instructions implement the classical propositional calculus and so on.

In miniaturizing components, however, one encounters limits to the quasi-classical domain. The alternative is either to stop miniaturization before quantum effects become dominant, or to take the quantum domain seriously. The latter alternative (at least to the author) seems the only progressive one, but it results in a head-on collision with long-held classical properties. Several long-held assumptions about the character of information have to be adapted. Furthermore, the formal computational techniques in manipulating information have to be revised.

This can be rather negatively perceived as a failure of the old models; but I think that we are justified to think of it in very positive terms: Physics, in particular quantum physics, stimulates us to re-consider our conceptions. We could hope that the outcome will be new tools and technologies in computing.

Indeed, right now, we are experiencing an attack on the "Cook-Karp thesis," putting into question the robustness of the notion of tractability or polynomial time complexity class with respect to variations of "reasonable" models of computation. In particular, factoring may require polynomial time on quantum computers within "reasonable statistics" [87]. I would suspect that it is wise of mathematicians and computer scientists to keep an eye on new developments in physics, just as we physicists are required to be open for the great advances in the formal sciences.

2 Hilbert space quantum mechanics

"Quantization" has been introduced by Max Planck in 1900 [79]. Planck assumed a *discretization* of the total energy U_N of N linear oscillators ("Resonatoren"), $U_N = P\epsilon \in \{0, \epsilon, 2\epsilon, 3\epsilon, 4\epsilon, \ldots\}$, where $P \in \mathrm{N}_0$ is zero or a positive integer and ϵ stands for the *smallest quantum of energy*. ϵ is a linear function of frequency ν and proportional to Planck's fundamental constant h; i.e., $\epsilon = h\nu$. That was a bold step in a time of the predominant continuum models of classical mechanics.

In extension of Planck's discretized resonator energy model, Einstein [40] proposed a quantization of the electromagnetic field. Every field mode of frequency ν could carry a discrete number of light quanta of energy $h\nu$ per quantum.

The present quantum theory is still a continuum theory in many respects: for infinite systems, there is a continuity of field modes of frequency ω. Also the quantum theoretical coefficients characterizing the mixture between orthogonal states, as well as space and time and other coordinates remain continuous — all but one: action. Thus, in the old days, discretization of phase space appeared to be a promising starting point for quantization. In a 1916 article on the structure of physical phase space, Planck emphasized that the quantum hypothesis should not be interpreted at the level of energy quanta but at the level of action quanta, according to the fact that the volume of $2f$-dimensional phase space (f degrees of freedom) is a positive integer of h^f [80, p. 387],[3]

> Es bestätigt sich auch hier wieder, daß die Quantenhypothese nicht auf Energieelemente, sondern auf Wirkungselemente zu gründen ist, entsprechend dem Umstand, daß das Volumen des Phasenraumes die Dimension von h^f besitzt.

The following is a very brief introduction to quantum mechanics for logicians and computer scientists.[4] To avoid a shock from a too early exposure to 'exotic' nomenclature prevalent in physics–the Dirac bra-ket notation–the notation of Dunford-Schwartz [39] is adopted.[5]

All quantum mechanical entities are represented by objects of Hilbert spaces [99]. A *Hilbert space* is a linear vector space 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 H $\times$ H such that (i) $(x,x)=0$ if and only if $x=0$; (ii) $(x,x)\geq 0$ for all $x\in$ H; (iii) $(x+y,z)=(x,z)+\overline{(y,z)}$ for all $x,y,z\in$ H; (iv) $(\alpha x,y)=\alpha(x,y)$ for all $x,y\in \mathrm{H},\alpha\in\Phi$; (v) $(x,y)=\overline{(y,x)}$ for all $x,y\in$ H ($\overline{\alpha}$ stands for the complex conjugate of α); (vi) If $x_n\in$ 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 $x\in$ H with $\lim_{n\rightarrow\infty}(x_n-x,x_n-x)=0$.

The following identifications between physical and theoretical objects are made (a *caveat:* this is an incomplete list):

(I) A *physical state* is represented by a vector of the Hilbert space H. Therefore, if two vectors $x,y\in$ H represent physical states, their vector sum $z=x+y\in$ 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.

---

[3] Again it is confirmed that the quantum hypothesis is not based on energy elements but on action elements, according to the fact that the volume of phase space has the dimension h^f.

[4] Introductions to quantum mechanics can be found in Feynman, Leighton & M. Sands [44], Harris [52], Lipkin [69], Ballentine [3], Messiah [74], Dirac [38], Peres [78], von Neumann [99], and Bell [5], among many other expositions. The history of quantum mechanics is reviewed by Jammer [55]. Wheeler & Zurek [100] published a helpful resource book.

[5] The bra-ket notation introduced by Dirac is widely used in physics. To translate expressions into the bra-ket notation, the following identifications work for most practical purposes: for the scalar product, "$\langle\equiv$ (", "$\rangle\equiv$)", ", $\equiv |$". States are written as $\mid\psi\rangle\equiv\psi$, operators as $\langle i\mid A\mid j\rangle\equiv A_{ij}$.

(II) *Observables* A are represented by self-adjoint operators A on the Hilbert space H such that $(Ax, y) = (x, Ay)$ for all $x, y \in$ H. (Observables and their corresponding operators are identified.)
In what follows, unless stated differently, only *finite* dimensional Hilbert spaces are considered.[6] 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.
Elements $b_i, b_j \in$ 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 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).
As infinite dimensional examples, take the position operator $\mathrm{x} = \mathbf{x} = (x_1, x_2, x_3)$, and the momentum operator $\mathrm{p}_x = \frac{\hbar}{i}\nabla = \frac{\hbar}{i}\left(\frac{\partial}{\partial x_1}, \frac{\partial}{\partial x_2}, \frac{\partial}{\partial x_3}\right)$, where $\hbar = \frac{h}{2\pi}$. The scalar product is given by $(\mathbf{x}, \mathbf{y}) = \delta^3(\mathbf{x}-\mathbf{y}) = \delta(x_1-y_1)\delta(x_2-y_2)\delta(x_3-y_3)$. The non-relativistic energy operator (Hamiltonian) is $H = \frac{\mathrm{p}\mathrm{p}}{2m} + V(x) = -\frac{\hbar^2}{2m}\nabla^2 + V(x)$.
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[7] $[\mathrm{x}, \mathrm{p}_x] = \mathrm{x}\mathrm{p}_x - \mathrm{p}_x\mathrm{x} = x\frac{\hbar}{i}\frac{\partial}{\partial x} - \frac{\hbar}{i}\frac{\partial}{\partial x}x = i\hbar \neq 0$ 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. The expectation value or average value $\langle\cdot\rangle$ is defined in **(V)** below.
It has recently been demonstrated that (by an analog embodiment using particle beams) every self-adjoint operator in a finite dimensional Hilbert space can be experimentally realized [82].

(III) The result of any single measurement of the observable A on a state $x \in$ 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

[6] Infinite dimensional cases and continuous spectra are nontrivial extensions of the finite dimensional Hilbert space treatment. As a heuristic rule, it could be stated that the sums become integrals, and the Kronecker delta function δ_{ij} becomes the Dirac delta function $\delta(i-j)$, which is a generalized function in the continuous variables i, j. In the Dirac bra-ket notation, unity is given by $\mathbf{1} = \int_{-\infty}^{+\infty} |i\rangle\langle i|\, di$.

[7] the expressions should be interpreted in the sense of operator equations; the operators themselves act on states.

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). This "transition" $x \to a_n$ has given rise to speculations concerning the "collapse of the wave function (state)." But, as has been argued recently [50], 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" [85, p. 53]), Schrödinger states,[8]

> *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.

8 *The ψ-function as expectation-catalog:* ... In it [[the ψ-function]] is embodied the momentarily-attained sum of theoretically based future expectation, somewhat as laid down in a *catalog*. ... For each measurement one is required to ascribe to the ψ-function (=the prediction catalog) a characteristic, quite sudden change, which *depends on the measurement result obtained,* and so *cannot be foreseen;* from which alone it is already quite clear that this second kind of change of the ψ-function has nothing whatever in common with its orderly development *between* two measurements. The abrupt change [[of the ψ-function (=the prediction catalog)]] by measurement ... is the most interesting point of the entire theory. It is precisely *the* point that demands the break with naive realism. For *this* reason one cannot put the ψ-function directly in place of the model or of the physical thing. And indeed not because one might never dare impute abrupt unforeseen changes to a physical thing or to a model, but because in the realism point of view observation is a natural process like any other and cannot *per se* bring about an interruption of the orderly flow of natural events.

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

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

(VI) 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., $\frac{\partial}{\partial t}\psi(t) = -\frac{iH}{\hbar}e^{-iHt/\hbar}\psi(t_0) = -\frac{iH}{\hbar}\psi(t)$. 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 $i\hbar\frac{\partial}{\partial t}\psi(x,t) = H\psi(x,t) = \left[\frac{\mathrm{pp}}{2m} + V(x)\right]\psi(x,t) = \left[-\frac{\hbar^2}{2m}\nabla^2 + V(x)\right]\psi(x,t)$.
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.
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. (See, for instance, [33] for a detailed treatment of various Hamiltonians H.)

For a quantum mechanical treatment of a two-state system, see appendix A. For a review of the quantum theory of multiple particles, see appendix B.

3 Quantum information theory

The fundamental atom of information is the quantum bit, henceforth abbreviated by the term 'qbit'. As we shall see, qbits feature quantum mechanics 'in a nutshell.'

Classical information theory (e.g., [51]) is based on the classical bit as fundamental atom. This classical bit, henceforth called *cbit,* is in one of two classical states t (often interpreted as "true") and f (often interpreted as "false"). It is customary to code the classical logical states by $\ulcorner t\urcorner = 1$ and $\ulcorner f\urcorner = 0$ ($\ulcorner s\urcorner$ stands for the code of s). The states can, for instance, be realized by some condenser who is discharged ($\equiv$ cbit state 0) or charged ($\equiv$ cbit state 1).

In quantum information theory [1, 34, 43, 6, 7, 35, 36], the most elementary unit of information is the *quantum bit,* henceforth called *qbit.* Qbits can be physically represented by a coherent superposition of the two orthonormal[9] states t

[9] $(t,t) = (f,f) = 1$ and $(t,f) = 0$.

and f. The qbit states

$$x_{\alpha,\beta} = \alpha t + \beta f \tag{1}$$

form a continuum, with $|\alpha|^2 + |\beta|^2 = 1$, $\alpha, \beta \in \mathrm{C}$.

3.1 Coding

Cbits can then be coded by

$$\ulcorner x_{\alpha,\beta} \urcorner = (\alpha, \beta) = e^{i\varphi}(\sin\omega, e^{i\delta}\cos\omega) \quad , \tag{2}$$

with $\omega, \varphi, \delta \in \mathrm{R}$. Qbits can be identified with cbits as follows

$$(a, 0) \equiv 1 \text{ and } (0, b) \equiv 0 \quad , \qquad |a|, |b| = 1 \quad , \tag{3}$$

where the complex numbers a and b are of modulus one. The quantum mechanical states associated with the classical states 0 and 1 are mutually orthogonal.

Notice that, provided that $\alpha, \beta \neq 0$, a qbit is not in a pure classical state. Therefore, any practical determination of the qbit $x_{\alpha,\beta}$ amounts to a measurement of the state amplitude of t or f. Any such *single* measurement will be indeterministic (provided again that $\alpha, \beta \neq 0$). That is, the outcome of a single measurement occurs unpredictably. Yet, according to the rules of quantum mechanics, the probabilities that the qbit $x_{\alpha,\beta}$ is measured in states t and f is $P_t(x_{\alpha,\beta}) = |(x_{\alpha,\beta}, t)|^2$ and $P_f(x_{\alpha,\beta}) = |(x_{\alpha,\beta}, f)|^2 = 1 - P_t(_{\alpha,\beta})$, respectively.

The classical and the quantum mechanical concept of information differ from each other in several aspects. Intuitively and classically, a unit of information is context-free. That is, it is independent of what other information is or might be present. A classical bit remains unchanged, no matter by what methods it is inferred. It obeys classical logic. It can be copied. No doubts can be left.

By contrast, quantum information is contextual [57, 58]. A quantum bit may appear different, depending on the method by which it is inferred. Quantum bits cannot be copied or "cloned" [102, 37, 72, 75, 46, 26]. Classical tautologies are not necessarily satisfied in quantum information theory. Quantum bits obey quantum logic. And, as has been argued before, they are coherent superpositions of classical information.

3.2 Reading the book of Nature—a short glance at the prediction catalog

To quote Landauer [63], *"What is measurement? If it is simply information transfer, that is done all the time inside the computer, and can be done with arbitrary little dissipation."* And, one may add, *without destroying coherence.*

Indeed, as has been briefly mentioned in **(III)**, there is reason to believe that—at least up to a certain magnitude of complexity—any measurement can be "undone" by a proper reconstruction of the wave-function. A necessary condition for this to happen is that *all* information about the original measurement is lost. In Schrödinger's terms, the prediction catalog (the wave function) can be opened only at one particular page. We may close the prediction catalog before reading this page. Then we can open the prediction catalog at another, complementary, page again. By no way we can open the prediction catalog at one page, read and (irreversible) memorize the page, close it; then open it at another, complementary, page. (Two non-complementary pages which correspond to two co-measurable observables can be read simultaneously.)

Can we then in some sense "undo" knowledge from conscious observation? This question relates to a statement by Wheeler [100, p. 184] that *"no elementary phenomenon is a phenomenon until it is a[[n irreversible]] registered (observed) phenomenon."* Where does this irreversible observation take place? Since the physical laws (with the possible exception of the weak force) are time-reversible, the act of irreversible observation must, according to Wigner [101], occur in the consciousness, thereby violating quantum mechanics.

4 Quantum recursion theory

4.1 Reversible computation and deletion of (q)bits

As a prelude to quantum computation, we briefly review classical reversible computation [61, 8, 45, 9, 66]. This type of computation is characterized by a single-valued inverse transition function. That is, logical functions are performed which do not have a single-valued inverse, such as `AND` or `OR`; i.e., the input cannot be deduced from the output. Also deletion of information or other many (states)-to-one (state) operations are irreversible. Reversible calculation requires every single step to be reversible. Figure 1 [66] draws the difference between one-to-one and many-to-one computation. This logical irreversibility is associated with physical irreversibility and requires a minimal heat generation of the computing machine.

It is possible to embed any irreversible computation in an appropriate environment which makes it reversible. For instance, the computing agent could keep the inputs of previous calculations in successive order. It could save all the information it would otherwise throw away. Or, it could leave markers behind to identify its trail, the *Hänsel and Gretel* strategy described by Landauer [66]. That, of course, might amount to a tremendous overhead in dynamical memory space (and time) and would merely postpone the problem of throwing away unwanted information. But, as has been pointed out by Bennett [8], for classical computations this overhead could be circumvented by making the computer to erase all intermediate results, leaving behind only the desired output and the originally furnished input. Bennett's trick is to do a computation reversible, then copy its output[10] and then, with one output as input for the reversible computation, run the computation backwards. In order not to consume exceedingly large intermediate storage resources, this strategy could be applied after every single step. The price is a doubling of computation time, since it requires one additional step for the back-computation.[11] Since qbits cannot be copied, the trick does not work for quantum computations.

[10] Copying can be done reversible in classical physics, if the memory used for the copy is initially blank. Quantum mechanically, this cannot be done on qbits; cf. below.

[11] If an irreversible computing agent exists which computes the input from a given output, then it is possible to translate an irreversible computation from input to output into one which is reversible and erases everything else except the final output, *including the original input*; i.e., that simply maps inputs into outputs. For details, see Bennett [8, 9].

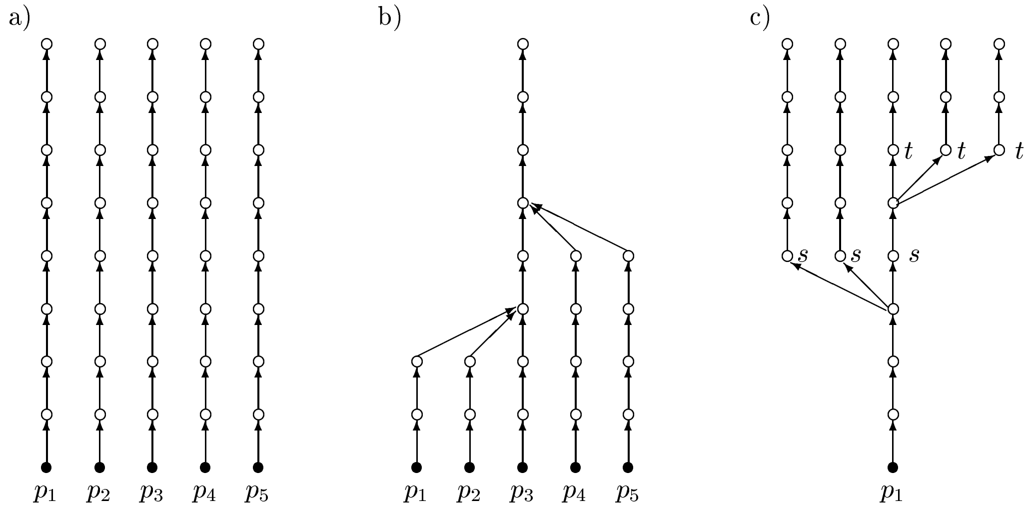


Figure 1: The lowest "root" represents the initial state interpretable as program. Forward computation represents upwards motion through a sequence of states represented by open circles. Different symbols p_i correspond to different initial states, that is, different programs. a) One-to-one computation. 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.

4.2 Selected features of quantum computation

The following features are important, but not sufficient qualities of quantum computers.

- Input, output, program and memory are represented by qbits.
- Any computation (step) can be represented by a unitary transformation of the computer as a whole.
- Any computation is reversible. Because of the unitarity of the quantum evolution operator, a deterministic computation can be performed by a quantum

computer if and only if it is reversible, i.e., if the program does not involve "deletion" of information or "many-to-one" operations. Only one-to-one operations are allowed. Compared to classical irreversible computation, this may result in a space and time overheads. Furthermore, no "one-to-many" operations are allowed. Thus, unless classical, qbits cannot be copied.
- Unless classical, qbits are context-dependent. That is, their value may depend on the method by which they have been inferred, and on the co-measured qbits.
- Measurements may be carried out on any qbit at any stage of the computation. But, unless classical, a qbit cannot be measured by a single experiment with arbitrary accuracy. The computation process and the measurement have to be repeated in order to obtain sufficient statistics.—Any such single measurement will yield merely a "click" on some counter, from which information about the qbit state must be inferred. Thereby, any single measurement is indeterminate and coherence is destroyed. Therefore, it seems more proper to realize that there is no such operational concept of "a single qbit." Because of complementarity, single qbits cannot be determined precisely. What is henceforth called "determination" or "measurement" of a qbit is, in effect, the observation of a successive number of such qbits, one after the other, from "similar" computation processes (same preparation, same evolution). By performing these measurements on "similar" qbits, one can "determine" this qbit within an epsilon-neighborhood only. The parameter epsilon depends on the number of successive measurements made.
- Quantum parallelism: during a computation (step), a quantum computer proceeds down all coherent paths at once. If managed properly, this may give rise to speedups.
- Any subroutine must not leave around any qbits beyond it's computed answer, because the computational paths with different residual information can no longer interfere.

In order to appreciate quantum computation, one should make proper use of the above features—quantum parallelism, unerasability of information, non-copying, context-dependence and impossibility to directly measure the atoms of quantum information, the qbits, related to quantum indeterminism.

Thereby, the "solution" to a decision problem may yield the classical bit values at random. It may depend on other qbits of information which are inferred. It cannot be arbitrarily copied and, in this sense, is unique.

4.2.1 Copying of quantum bits

Can a non-classical qbit be copied? No! — This answer amazes the classical mind.[12] Informally speaking, the reason is that, depending on the strategy, any attempt to copy a coherent superposition of states results either in a state reduction, destroying coherence, or, most important of all, in the addition of noise which manifests itself as the spontaneous excitations of previously nonexisting

[12] Copying of qbits would allow circumvention of the Heisenberg uncertainty relation by measuring two incompatible observables on two identical qbit copies. It would also allow faster-than-light transmission of information, as pointed out by Herbert [53]. Herbert's suggestion stimulated the development of "no-cloning theorems" reviewed here.

field modes [102, 37, 72, 75, 46, 26]. Therefore, *qbits can be copied if and only if they are (known to be) classical. Only one-to-one computation processes depicted in Fig. 1a) are allowed.*

This can be seen by a short calculation [102] which requires the multi-quantum formalism developed in appendix B. A physical realization[13] of the qbit state is a two-mode boson field with the identifications

$$x_{\alpha,\beta} = \alpha f + \beta t \quad , \tag{4}$$
$$f = |\, 0_1, 1_2\rangle \quad , \tag{5}$$
$$t = |\, 1_1, 0_2\rangle \quad . \tag{6}$$

The classical bit states are $|0_1, 1_2\rangle$ (field mode 1 unfilled, field mode 2 filled with one quantum) and $|1_1, 0_2\rangle$ (field mode 1 filled with one quantum, field mode 2 unfilled).

An ideal amplifier, denoted by A, should be able to copy a classical bit state; i.e., it should create an identical particle in the same mode

$$A_i|0_1, 1_2\rangle \to A_f|0_1, 2_2\rangle \quad , \qquad A_i|1_1, 0_2\rangle \to A_f|2_1, 0_2\rangle \quad . \tag{7}$$

Here, A_i and A_f stand for the initial and the final state of the amplifier.

What about copying a proper qbit; i.e., a *coherent superposition* of the cbits $f = |0_1, 1_2\rangle$ and $t = |1_1, 0_2\rangle$? According to the quantum evolution law, the corresponding amplification process should be representable by a linear (unitary) operator; thus

$$A_i(\alpha|0_1, 1_2\rangle + \beta|1_1, 0_2\rangle) \to A_f(\alpha|0_1, 2_2\rangle + \beta|2_1, 0_2\rangle) \quad . \tag{8}$$

Yet, the true copy of that qbit is the state

$$\begin{aligned}(x_{\alpha,\beta})^2 \mid 0_1, 0_2\rangle &= (\alpha\, a_2^\dagger + \beta\, a_1^\dagger)^2 \mid 0_1, 0_2\rangle \\ &= \left[\alpha^2\,(a_2^\dagger)^2 + \alpha\beta\,(a_2^\dagger a_1^\dagger + a_1^\dagger a_2^\dagger) + \beta^2\,(a_1^\dagger)^2\right] \mid 0_1, 0_2\rangle \\ &= \left[\alpha^2\,(a_2^\dagger)^2 + 2\alpha\beta\, a_2^\dagger a_1^\dagger + \beta^2\,(a_1^\dagger)^2\right] \mid 0_1, 0_2\rangle \\ &= \alpha^2|0_1, 2_2\rangle + 2\alpha\beta|1_1, 1_2\rangle + \beta^2|2_1, 0_2\rangle \quad . \end{aligned} \tag{9}$$

By comparing (8) with (9) it can be seen that a reasonable (linear unitary quantum mechanical evolution for an) amplifier which could copy a qbit exists only if the qbit is classical.

A more detailed analysis (cf. [72, 75], in particular [46, 26]) reveals that the copying (amplification) process generates an amplification of the signal but necessarily adds noise at the same time. This noise can be interpreted as spontaneous emission of field quanta (photons) in the process of amplification.

One application of this feature is quantum cryptography [13, 12, 11]. Thereby, the impossibility to copy qbits is used for a cryptographic communication *via* quantum channels.

[13] the most elementary realization is a one-mode field with the symbol **0** corresponding to $|\, 0\rangle$ (empty mode) and **1** corresponding to $|\, 1\rangle$ (one-quantum filled mode).

4.2.2 Context dependence of qbits

This section could be skipped at first reading.

Assume that in an EPR-type arrangement [41] one wants to measure the product

$$P = m_x^1 m_x^2 m_y^1 m_y^2 m_z^1 m_z^2$$

of the direction of the spin components of each one of the two associated particles 1 and 2 along the x, y and z-axes. Assume that the operators are normalized such that $|m_i^j| = 1$, $i \in \{x, y, z\}$, $j \in \{1, 2\}$. One way to determine P is measuring and, based on these measurements, "counterfactually inferring" [78, 73] the three "observables" $m_x^1 m_y^2$, $m_y^1 m_x^2$ and $m_z^1 m_z^2$. By multiplying them, one obtains $+1$. Another, alternative, way to determine P is measuring and, based on these measurements, "counterfactually inferring" the three "observables" $m_x^1 m_x^2$, $m_y^1 m_y^2$ and $m_z^1 m_z^2$. By multiplying them, one obtains -1. In that way, one has obtained either $P = 1$ or $P = -1$. Associate with $P = 1$ the bit state zero **0** and with $P = -1$ the bit state **1**. Then the bit is either in state zero or one, depending on the way or *context* it was inferred.

This kind of contextuality is deeply rooted in the non-Boolean algebraic structure of quantum propositions. Note also that the above argument relies heavily on "counterfactual reasoning," because, for instance, only two of the six observables m_i^j can actually be experimentally determined. Here, the term "counterfactual reasoning" [78, 73] stands for arguments involving results of *incompatible* experiments, i.e., experiments which could never be performed simultaneously, since the associated operators do not commute. The results thus have to be *inferred* rather than *measured*, and the existence of such "elements of physical reality" thus have to be tacitly assumed [41].

4.3 Universal quantum computer based on the U(2)-gate

The "brute force" method of obtaining a (universal) quantum computer [6, 34, 66] by quantizing the "hardware" components of a Turing machine suffers from the same problem as its classical counterpart–it seems technologically unreasonable to actually construct a universal quantum device with a "scaled down" (to nanometer size) model of a Turing machine in mind.

We therefore pursue a more fundamental approach [94, 95]. Recall that an arbitrary quantum time evolution in finite-dimensional Hilbert space is given by $x(t) = Ux(t_0)$, where U is unitary.

It is well known that any n-dimensional unitary matrix U can be composed from elementary unitary transformations in two-dimensional subspaces of C^n. This is usually shown in the context of parameterization of the n-dimensional unitary groups (cf. [76, chapter 2] and [82, 81]). Thereby, a transformation in n-dimensional spaces is decomposed into transformations in 2-dimensional subspaces. This amounts to a successive array of $U(2)$ elements, which in their entirety forms an arbitrary time evolution $U(n)$ in n-dimensional Hilbert space.

Hence, all quantum processes and computation tasks which can possibly be executed must be representable by unitary transformations. Indeed, unitary transformations of qbits are a necessary and sufficient condition for quantum computing. *The group of unitary transformations in arbitrary- but finite-dimensional Hilbert space is a model of universal quantum computer.*

Unitary quantum mechanical operations are a natural extension of Turing's "simple" classical paper and pencil operations on a sheet of (one-dimensional) paper [97, section 9.I]. If one wants to extend that notion further, one would have to extend physical theory, in particular quantum theory. However, at the moment, such a further extension (beyond quantum mechanics) seems only a remote possibility.

It remains to be shown that the universal $U(2)$-gate is physically operationalizable. This is done in appendix D in the framework of Mach-Zehnder interferometry. Note that the number of elementary $U(2)$-transformations is polynomially bounded and does not exceed $\binom{n}{2} = n\,(n-1)/2 = O(n^2)$.

4.4 Other models of universal quantum computation

Deutsch [35] has proposed a model of universal computation based on quantum computation networks. Thereby, the states in a 2^n-dimensional Hilbert space are constructed as the product state of n particles in two-dimensional Hilbert space. A set of gates that consists of all $U(2)$ (one-bit) quantum gates and the two-bit exclusive-or gate (that maps Boolean values (x, y) to $(x, x \oplus y)$) is universal in the sense that all unitary operations on arbitrarily many bits n $(U(2^n))$ can be expressed as compositions of these gates [4].

This approach should be distinguished from the interferometric approach using $U(2)$-gates discussed before, which is based on single particle states in 2^n-dimensional Hilbert space. In the product state model, the addition of one particle effectively doubles the dimensionality of the associated Hilbert space. In the interferometric model, this could only be achieved by doubling the number of input and output ports. This could give rise to non-polynomial space overhead. In the case of the product state model, in order to obtain a mixing between different particle states, `xor`-gates are needed. The interferometric approach does not need `xor`-gates explicitly.

It has been claimed [87, 30] that certain supposedly NP-hard problems such as factoring can be solved in polynomial time on quantum computers. However, it should be noted that this result faces difficulties. For, it might not be easy to keep the quantum computer in a coherent superposition state over sufficient time and space scales in order to be able to execute tasks which are hard to do classically—the computation may "decohere," reducing the qbits to classical ones [59]. Furthermore, in order to obtain sufficient statistical data, a "great" (non-polynomially bounded) number of single particles may be needed [91]. We shall not pursue these matters further [36, 14, 15, 6, 27, 87].

4.5 Nomenclature

Consider a (not necessarily universal) quantum computer C and its ith program p_i, which, at time $\tau \in \mathbf{Z}$, can be described by a quantum state $C(\tau, p_i)$. Let $C(p) = s$ stand for a computer C with program p which outputs s in arbitrary long time. In what follows we shall assume that the program p_i is coded *classically.* That is, we choose a finite code alphabet A and denote by A^* the set of all strings over A. Any program p_i is coded as a classical sequence $\mathrm{p}p_i\mathrm{q} = s_{1i}s_{2i}\cdots s_{ni} \in A^*$, $s_{ji} \in A$. Whenever possible, $\mathrm{p}p_i\mathrm{q}$ will be abbreviated by p_i. We assume prefix coding [51, 29, 28, 92, 23]; i.e., the domain of C is prefix-free such that no admissible program is the prefix of another admissible program. Furthermore, without loss of generality, we consider only empty input strings. $|p|$ stands for the length of p.

4.6 Diagonalization

This is neither the place for a comprehensive review of the diagonalization method [83, 77], nor suffices the author's competence for such an endeavor. Therefore, only a few hallmarks are stated. As already Gödel pointed out in his classical paper on the incompleteness of arithmetic [47], the undecidability theorems of formal logic [31] (and the theory of recursive functions [83, 77]) are based on semantical paradoxes such as the liar [2] or Richard's paradox. A proper translation of the semantic paradoxes results in the diagonalization method. Diagonalization has apparently first been applied by Cantor to demonstrate the non-enumerability of real numbers [25]. It has also been used by Turing for a proof of the recursive undecidability of the halting problem [97].

A brief review of the classical algorithmic argument will be given first. Consider a universal computer C. For the sake of contradiction, consider an arbitrary algorithm $B(X)$ whose input is a string of symbols X. Assume that there exists a "halting algorithm" `HALT` which is able to decide whether B terminates on X or not. The domain of `HALT` is the set of legal programs. The range of `HALT` are cbits (classical case) and qbits (quantum mechanical case).

Using $\mathtt{HALT}(B(X))$ 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 `HALT`. Then, A proceeds as follows: if $\mathtt{HALT}(B(B))$ decides that $B(B)$ halts, then the agent A does not halt; this can for instance be realized by an infinite `DO`-loop; if $\mathtt{HALT}(B(B))$ 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.

4.6.1 Classical case

Assume that A is restricted to classical bits of information. To be more specific, assume that `HALT` outputs the code of a cbit as follows ($\uparrow$ and $\downarrow$ stands for divergence and convergence, respectively):

$$\mathtt{HALT}(B(X)) = \begin{cases} 0 \text{ if } B(X) \uparrow \\ 1 \text{ if } B(X) \downarrow \end{cases} \quad . \tag{10}$$

Then, whenever $A(A)$ halts, $\mathtt{HALT}(A(A))$ outputs 1 and forces $A(A)$ not to halt. Conversely, whenever $A(A)$ does not halt, then $\mathtt{HALT}(A(A))$ outputs 0 and steers $A(A)$ 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 HALT, the impossibility of any such halting algorithm.

4.6.2 Quantum mechanical case

Recall that a quantum computer C evolves according to a unitary operator U such that (τ stands for the discrete time parameter) $C(\tau, p_i) = UC(\tau - 1, p_i) = U^t C(0, p_i)$.

As has been pointed out before, in quantum information theory a qbit may be in a coherent superposition of the two classical states t and f. Due to this possibility of a coherent superposition of classical bit states, the usual *reductio ad absurdum* argument breaks down. Instead, diagonalization procedures in quantum information theory yield qbit solutions which are fixed points of the associated unitary operators.

In what follows it will be demonstrated how the task of the agent A can be performed consistently if A is allowed to process quantum information. To be more specific, assume that the output of the hypothetical "halting algorithm" is a halting qbit

$$\mathtt{HALT}(B(X)) = h_{\alpha,\beta} \quad . \tag{11}$$

One may think of $\mathtt{HALT}(B(X))$ as a universal "watchdog" computer C' simulating C and containing a dedicated *halting bit*, which it outputs at every (discrete) time cycle [34]. Alternatively, it can be assumed that the computer C contains its own halting bit indicating whether it has completed its task or not. Note that the halting qbit $h_{\alpha,\beta}$ can be represented by a normalized[14] vector in two-dimensional complex Hilbert space spanned by the the orthonormal vectors "t" and "f." Let the halting state $h_{1,0} = t$ (up to factors modulus 1) be the physical realization that the computer has "halted;" likewise let $h_{0,1} = f$ (up to factors modulus 1) be the physical realization that the computer has not "halted." Note that, since quantum computations are governed by unitary evolution laws which are reversible, the halting state does not imply that the computer does not change as time evolves. It just means that it has set a signal — the halting bit — to indicated that it has finished its task. α and β are complex numbers which are a quantum mechanical measure of the probability amplitude that the computer is in the halting and the non-halting states, respectively. The corresponding halting and non-halting probabilities are $|a|^2$ and $|a|^2$, respectively.

Initially, i.e., at $t = 0$, the halting bit is prepared to be a 50:50 mixture of the classical halting and non-halting states t and f; i.e., $h_{1/\sqrt{2},1/\sqrt{2}}$. If later C' finds that C converges (diverges) on $B(X)$, then the halting bit of C' is set to the classical value t (f).

The emergence of fixed points can be demonstrated by a simple example. Agent A's diagonalization task can be formalized as follows. Consider for the moment the action of diagonalization on the cbit states. (Since the qbit states are merely a coherent superposition thereof, the action of diagonalization on qbits is straightforward.) Diagonalization effectively transforms the cbit value t into f and *vice versa.* Recall that in equation (10), the state t has been identified with the halting state and the state f with the non-halting state. Since the halting

[14] $(h_{\alpha,\beta}, h_{\alpha,\beta}) = 1$.

state and the non-halting state exclude each other, f, t can be identified with orthonormal basis vectors in a two-dimensional vector space. Thus, the standard basis of Cartesian coordinates can be chosen for a representation of t and f; i.e.,

$$t \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } f \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad . \tag{12}$$

The evolution representing diagonalization (effectively, agent A's task) can be expressed by the unitary operator D by

$$Dt = f \text{ and } Df = t \quad . \tag{13}$$

Thus, D acts essentially as a `not`-gate. In the above state basis, D can be represented as follows:

$$D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad . \tag{14}$$

D will be called *diagonalization* operator, despite the fact that the only nonvanishing components are off-diagonal.

As has been pointed out earlier, quantum information theory allows a coherent superposition $h_{\alpha,\beta} = \alpha t + \beta f$ of the cbit states t and f. D acts on cbits. It has a fixed point at the qbit state

$$h^* := h_{\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}}} = \frac{t+f}{\sqrt{2}} \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad . \tag{15}$$

h^* does not give rise to inconsistencies [90]. If agent A hands over the fixed point state h^* to the diagonalization operator D, the same state h^* is recovered. Stated differently, as long as the output of the "halting algorithm" to input $A(A)$ is h^*, diagonalization does not change it. Hence, even if the (classically) "paradoxical" construction of diagonalization is maintained, quantum theory does not give rise to a paradox, because the quantum range of solutions is larger than the classical one. Therefore, standard proofs of the recursive unsolvability of the halting problem do not apply if agent A is allowed a qbit.

Another, less abstract, application for quantum information theory is the handling of inconsistent information in databases. Thereby, two contradicting cbits of information t and f are resolved by the qbit $h^* = (t + f)/\sqrt{2}$. Throughout the rest of the computation the coherence is maintained. After the processing, the result is obtained by an irreversible measurement. The processing of qbits, however, would require an exponential space overhead on classical computers in cbit base [42]. Thus, in order to remain tractable, the corresponding qbits should be implemented on truly quantum universal computers.

It should be noted, however, that the fixed point qbit "solution" to the above halting problem, as far as problem solving is concerned, is of not much practical help. In particular, if one is interested in the "classical" answer whether or not $A(A)$ halts, then one ultimately has to perform an irreversible measurement on the fixed point state. This causes a state reduction into the classical states corresponding to t and f. Any single measurement will yield an indeterministic result. There is a 50:50 chance that the fixed point state will be either in t or f, since $P_t(h^*) = P_f(h^*) = \frac{1}{2}$. Thereby, classical undecidability is recovered. Stated pointedly: With regards to the question of whether or not a computer halts, the "solution" h^* is equivalent to the throwing of a fair coin.

Therefore, the advance of quantum recursion theory over classical recursion theory is not so much classical problem solving but *the consistent representation of statements* which would give rise to classical paradoxes.

4.6.3 Proper quantum diagonalization

The above argument used the continuity of qbit states as compared to the two cbit states for a construction of fixed points of the diagonalization operator. One could proceed a step further and allow *nonclassical diagonalization procedures.* Such a step, albeit operationalizable, has no classical operational equivalent, and thus no classical interpretation.

Consider the entire range of two-dimensional unitary transformations [76]

$$U(2)(\omega,\alpha,\beta,\varphi)=e^{-i\,\beta}\begin{pmatrix} e^{i\,\alpha}\,\cos\omega & -e^{-i\,\varphi}\,\sin\omega\\ e^{i\,\varphi}\,\sin\omega & e^{-i\,\alpha}\,\cos\omega\end{pmatrix}\quad , \tag{16}$$

where $-\pi\le\beta,\omega\le\pi$, $-\frac{\pi}{2}\le\alpha,\varphi\le\frac{\pi}{2}$, to act on the qbit. A typical example of a nonclassical operation on a qbit is the "square root of not" gate ($\sqrt{\texttt{not}}\sqrt{\texttt{not}}=D$)

$$\sqrt{\texttt{not}}=\frac{1}{2}\begin{pmatrix}1+i & 1-i\\ 1-i & 1+i\end{pmatrix}\quad . \tag{17}$$

Not all these unitary transformations have eigenvectors associated with eigenvalues 1 and thus fixed points. Indeed, it is not difficult to see that only unitary transformations of the form

$$\begin{aligned}&[U(2)(\omega,\alpha,\beta,\varphi)]^{-1}\,\mathrm{diag}(1,e^{i\lambda})\,U(2)(\omega,\alpha,\beta,\varphi)=\\ &=\begin{pmatrix}\cos\omega^2+e^{i\,\lambda}\sin\omega^2 & \frac{-1+e^{i\,\lambda}}{2}e^{-i\,(\alpha+\varphi)}\,\sin(2\,\omega)\\ \frac{-1+e^{i\,\lambda}}{2}e^{i\,(\alpha+\varphi)}\,\sin(2\,\omega) & e^{i\,\lambda}\cos\omega^2+\sin\omega^2\end{pmatrix}\end{aligned} \tag{18}$$

have fixed points.

Applying nonclassical operations on qbits with no fixed points

$$\begin{aligned}D'&=[U(2)(\omega,\alpha,\beta,\varphi)]^{-1}\,\mathrm{diag}(e^{i\mu},e^{i\lambda})U(2)(\omega,\alpha,\beta,\varphi)\\ &=\begin{pmatrix}e^{i\,\mu}\cos(\omega)^2+e^{i\,\lambda}\sin(\omega)^2 & \frac{e^{-i\,(\alpha+p)}}{2}\,\left(e^{i\,\lambda}-e^{i\,\mu}\right)\,\sin(2\,\omega)\\ \frac{e^{i\,(\alpha+p)}}{2}\,\left(e^{i\,\lambda}-e^{i\,\mu}\right)\,\sin(2\,\omega) & e^{i\,\lambda}\cos(\omega)^2+e^{i\,\mu}\sin(\omega)^2\end{pmatrix}\end{aligned} \tag{19}$$

with $\mu,\lambda\neq n\pi$, $n\in\mathrm{N}_0$ gives rise to eigenvectors which are not fixed points, but which acquire nonvanishing phases μ,λ in the generalized diagonalization process.

5 Quantum algorithmic information

Quantum algorithmic information theory can be developed in analogy to algorithmic information theory [29, 28, 23, 68]. Before proceeding, though, one decisive strategic decision concerning the physical character of the program has to be made. This amounts to a restriction to purely *classical* prefix-free programs.

The reason for classical programs, as well as for the requirement of instant decodability, is the desired convergence of the Kraft sum over the exponentially weighted program length $\sum_p \exp(|p| \log k) \leq 1$, where $|p|$ stands for the length of p and k is the base of the code (for binary code, $k = 2$). If arbitrary qbits were allowed as program code, then the Kraft sum would diverge.

Nevertheless, qbits are allowed as output. Since they are objects defined in Hilbert space H, the basic definitions of algorithmic information theory have to be slightly adapted.

The *canonical program* associated with an object $s \in$ H representable as vector in a Hilbert space H is denoted by s^* and defined by

$$s^* = \min_{C(p)=s} p \quad . \tag{20}$$

I.e., s^* is the first element in the ordered set of all strings that is a program for C to calculate s. The string s^* is thus the code of the smallest-size program which, implemented on a quantum computer, outputs s. (If several binary programs of equal length exist, the one is chosen which comes first in an enumeration using the usual lexicographic order relation "$0 < 1$.")

Let again "$|x|$" of an object encoded as (binary) string stand for the length of that string. The *quantum algorithmic information* $H(s)$ of an object $s \in$ H representable as vector in a Hilbert space H is defined as the length of the shortest program p which runs on a quantum computer C and generates the output s:

$$H(s) = |s^*| = \min_{C(p)=s} |p| \quad . \tag{21}$$

If no program makes computer C output s, then $H(s) = \infty$.

The *joint quantum algorithmic information* $H(s,t)$ of two objects $s \in$ H and $t \in$ H representable as vectors in a Hilbert space H is the length of the smallest-size binary program to calculate s and t simultaneously.

The *relative or conditional quantum algorithmic information* $H(s|t)$ of $s \in$ H given $t \in$ N is the length of the smallest-size binary program to calculate s from a *smallest-size program* for t:

$$H(s|t) = \min_{C(p,t^*)=s} |p| \quad . \tag{22}$$

Most features and results of algorithmic information theory hold for quantum algorithmic information as well. In particular, we restrict our attention to universal quantum computers whose quantum algorithmic information content is machine-independent, such that the quantum algorithmic information content of an arbitrary object does not exceed a constant independent of that object. That is, for all objects $s \in$ H and two computers C and C' of this class,

$$|H_C - H_{C'}| = O(1) \quad . \tag{23}$$

Furthermore, let s and t be two objects representable as vectors in Hilbert space. Then (recall that $t \in$ N),

$$H(s,t) = H(t,s) + O(1) \quad ; \tag{24}$$

$$H(s|s) = O(1) \quad ; \tag{25}$$

$$H(H(s)|s) = O(1) \quad ; \tag{26}$$

$$
\begin{aligned}
H(s) &\le H(s,t) + O(1) \quad ; & (27)\\
H(s|t) &\le H(s) + O(1) \quad ; & (28)\\
H(s,t) &= H(s) + H(t|s^*) + O(1) \quad (\text{if } s^* \text{ is classical}) \quad ; & (29)\\
H(s,t) &\le H(s) + H(t) + O(1) \quad (\text{subadditivity}) \quad ; & (30)\\
H(s,s) &= H(s) + O(1) \quad ; & (31)\\
H(s,H(s)) &= H(s) + O(1) \quad . & (32)
\end{aligned}
$$

Notice that there exist sets of objects $S = \{s_1, \ldots, s_n\}$, $n < \infty$ whose algorithmic information content $H(S)$ is arbitrary small compared to the algorithmic information content of some unspecified *single* elements $s_i \in S$; i.e.,

$$H(S) < \max_{s_i \in S} H(s_i) \quad . \tag{33}$$

6 Quantum omega

Chaitin's Ω [29, 28, 89, 23] is a magic number. It is a measure for arbitrary programs to take a finite number of execution steps and then halt. It contains the solution of all halting problems, and hence of questions codable into halting problems, such as Fermat's theorem. It contains the solution of the question of whether or not a particular exponential Diophantine equation has infinitely many or a finite number of solutions. And, since Ω is provable "algorithmically incompressible," it is Martin-Löf/Chaitin/Solovay random. Therefore, Ω is both: a mathematician's "fair coin," and a formalist's nightmare.

Here, Ω is generalized to quantum computations.[15]

In the orthonormal halting basis $\{t, f\}$, the computer C with classical input p_i can be represented by $C(\tau, p_i) = t\,(t, C(\tau, p_i)) + f\,(f, C(\tau, p_i))$.

Recall that initially, i.e., at time $\tau = 0$, the halting bit is in a coherent 50:50-superposition; i.e., in terms of the halting basis, $C(0, p_i) = (t + f)/\sqrt{2}$ for all $p_i \in A^*$. This corresponds to the fact that initially it is unknown whether or not the computer halts on p_i. When during the time evolution the computer has completed its task, the halting bit value is switched to t by some internal operation. If the computer never halts, the halting bit value is switched to f by some internal operation. Otherwise it remains in the coherent 50:50-superposition.

Alternatively, the computer could be initially prepared in the non-halting state f. After completion of the task, the halting bit is again switched to the halting state t.

In analogy to the fully classical case [29, 28, 88, 23], the *quantum halting amplitude*[16] Ω can be defined as a weighted expectation over all computations of C with classical input p_i ($|p_i|$ stands for the length of p_i)

$$\Omega \equiv \sum_{C(p_i) \in \mathrm{H}} 2^{-|p_i|/2} (t, C(p_i)) \quad . \tag{34}$$

---

[15] The quantum omega was invented in a meeting of G. Chaitin, A. Zeilinger and the author in a Viennese coffee house (Café Bräunerhof) in January 1991. Thus, the group should be credited for the original invention, whereas any blame should remain with the author.

[16] The definition of Ω and Υ differ slightly from the ones introduced by the author previously [93].

Likewise, the halting amplitude for a particular output state s,

$$\Upsilon(s) \equiv \sum_{C(p_i)=s} 2^{-|p_i|/2}(t, C(p_i)) \quad . \tag{35}$$

For a set of output states $S = \{s_1, s_2, s_3, \ldots, s_n\}$ which correspond to mutually orthogonal vectors in Hilbert space,

$$\Upsilon(S) \equiv \sum_{C(p_i)\in S} 2^{-|p_i|/2}(t, C(p_i)) \quad . \tag{36}$$

Terms corresponding to different programs and states have to be summed up incoherently. Thus, the corresponding probabilities are

$$|\Omega|^2 = \sum_{C(p_i)\in \mathrm{H}} 2^{-|p_i|}|(t, C(p_i))|^2 \tag{37}$$

$$P(s) \equiv |\Upsilon(s)|^2 = \sum_{C(p_i)=s} 2^{-|p_i|}|(t, C(p_i))|^2 \tag{38}$$

$$P(S) \equiv \sum_{C(p_i)\in S} |\Upsilon(s)|^2 = \sum_{C(p_i)\in S} 2^{-|p_i|}|(t, C(p_i))|^2 \quad . \tag{39}$$

The following relations hold,

$$\Upsilon(S) = \sum_{s_i\in S} \Upsilon(s_i) \quad , \tag{40}$$

$$\Omega = \Upsilon(\mathrm{H}) = \sum_{s_i\in \mathrm{H}} \Upsilon(s_i) \quad . \tag{41}$$

For $s \subset S \subset \mathrm{H}$,

$$0 \leq P(s) \leq P(S) \leq |\Omega|^2 \leq 1 \quad . \tag{42}$$

Alternatively, the *quantum halting probability* and the *quantum algorithmic information* by the quantum algorithmic information content. That is,

$$P^*(s) = 2^{-|s^*|} = 2^{-H(s)} \tag{43}$$

$$P^*(S) = \sum_{s_i\in S} P^*(s) = \sum_{s\in S} 2^{-H(s)} \tag{44}$$

$$P^*(\mathrm{H}) = |\Omega^*|^2 = \sum_{n\in \mathrm{H}} 2^{-H(n)} \quad . \tag{45}$$

$$|\Omega^*|^2 \leq |\Omega|^2 \quad , \tag{46}$$

$$P^*(s) \leq P(s) \quad , \tag{47}$$

$$P^*(S) \leq P(S) \quad . \tag{48}$$

The following relations are either a direct consequence of the definition (43) or follow from the fact that for programs in prefix code, the algorithmic probability is concentrated on the minimal size programs, or alternatively, that there are few minimal programs:

$$H(s) = -\log_2 P^*(s) \quad ; \tag{49}$$

$$H(s) = -\log_2 P(s) + O(1) \quad . \tag{50}$$

Notice again that, because of complementarity, single qbits cannot be determined precisely. They just appear experimentally as some clicks in a counter. What we can effectively do is to observe a successive number of such qbits, one after the other, from "similar" computation processes (same preparation, same evolution). By performing these measurements on "similar" qbits, one can "determine" this qbit within an ε-neighborhood only.

For nontrivial choices of the quantum computer C, several remarks are in order. (In what follows, we mention only Ω, but the comments apply to Υ as well.) If the program is also coded in qbits, the above sum becomes an integral over continuously many states per code symbol of the programs. In this case, the Kraft sum needs not converge. Just as for the classical analogue it is possible to "compute" Ω as a limit from below by considering in the t'th computing step (time τ) all programs of length τ which have already halted. (This "computation" suffers from a radius of convergence which decreases slower than any recursive function.) The quantum Ω is complex. $|\Omega|^2$ can be interpreted as a measure for the halting probability of C; i.e., the probability that an arbitrary (prefix-free) program halts on C.

Finally, any irreversible measurement of $|\Omega|^2$ causes a state collapse. Since $C(\tau, p_i)$ may not be in a pure state, the series in (34) and (35) will not be uniquely defined even for *finite* times. Thus the *nondeterministic* character of Ω is not only based on classical recursion theoretic arguments [29, 28] but also on the metaphysical assumption that God plays the quantum dice.

Appendices

A Two-state system

Having set the stage of the quantum formalism, an elementary two-dimensional example of a two-state system shall be exhibited ([44, pp. 8-11]). Let us denote the two base states by 1 and 2. Any arbitrary physical state ψ is a coherent superposition of 1 and 2 and can be written as $\psi = 1(1,\psi) + 2(2,\psi)$ with the two coefficients $(1,\psi),(2,\psi) \in$ C.

Let us discuss two particular types of evolutions.

First, let us discuss the Schrödinger equation with diagonal Hamilton matrix, i.e., with vanishing off-diagonal elements,

$$H_{ij} = \begin{pmatrix} E_1 & 0 \\ 0 & E_2 \end{pmatrix} \quad . \tag{51}$$

In this case, the Schrödinger equation decouples and reduces to

$$i\hbar \frac{\partial}{\partial t}(1,\psi(t)) = E_1(1,\psi(t)) \quad , \qquad i\hbar \frac{\partial}{\partial t}(2,\psi(t)) = E_2(2,\psi(t)) \quad , \tag{52}$$

resulting in

$$(1,\psi(t)) = ae^{-iE_1t/\hbar} \quad , \qquad (2,\psi(t)) = be^{-iE_2t/\hbar} \quad , \tag{53}$$

with $a,b \in$ C, $|a|^2+|b|^2=1$. These solutions correspond to *stationary states* which do not change in time; i.e., the probability to find the system in the two states is constant

$$|(1,\psi)|^2 = |a|^2 \quad , \qquad |(2,\psi)|^2 = |b|^2 \quad . \tag{54}$$

Second, let us discuss the Schrödinger equation with with non-vanishing but equal off-diagonal elements $-A$ and with equal diagonal elements E of the Hamiltonian matrix; i.e.,

$$H_{ij} = \begin{pmatrix} E & -A \\ -A & E \end{pmatrix} \quad . \tag{55}$$

In this case, the Schrödinger equation reads

$$i\hbar\frac{\partial}{\partial t}(1,\psi(t)) = E(1,\psi(t)) - A(2,\psi(t)) \quad , \tag{56}$$

$$i\hbar\frac{\partial}{\partial t}(2,\psi(t)) = E(2,\psi(t)) - A(1,\psi(t)) \quad . \tag{57}$$

These equations can be solved in a number of ways. For example, taking the sum and the difference of the two, one obtains

$$i\hbar\frac{\partial}{\partial t}((1,\psi(t)) + (2,\psi(t))) = (E-A)((1,\psi(t)) + (2,\psi(t))) \quad , \tag{58}$$

$$i\hbar\frac{\partial}{\partial t}((1,\psi(t)) - (2,\psi(t))) = (E+A)((1,\psi(t)) - (2,\psi(t))) \quad . \tag{59}$$

The solution are again two stationary states

$$(1,\psi(t)) + (2,\psi(t)) = ae^{-(i/\hbar)(E-A)t} \quad , \tag{60}$$

$$(1,\psi(t)) - (2,\psi(t)) = be^{-(i/\hbar)(E+A)t} \quad . \tag{61}$$

Thus,

$$(1,\psi(t)) = \frac{a}{2}e^{-(i/\hbar)(E-A)t} + \frac{b}{2}e^{-(i/\hbar)(E+A)t} \quad , \tag{62}$$

$$(2,\psi(t)) = \frac{a}{2}e^{-(i/\hbar)(E-A)t} - \frac{b}{2}e^{-(i/\hbar)(E+A)t} \quad . \tag{63}$$

Assume now that initially, i.e., at $t=0$, the system was in state $,1) =, \psi(t = 0))$. This assumption corresponds to $(1,\psi(t=0)) = 1$ and $(2,\psi(t=0)) = 0$. What is the probability that the system will be found in the state 2 at the time $t>0$, or that it will still be found in the state 1 at the time $t>0$? Setting $t=0$ in equations (62) and (63) yields

$$(1,\psi(t=0)) = \frac{a+b}{2} = 1 \quad , \qquad (2,\psi(t=0)) = \frac{a-b}{2} = 0 \quad , \tag{64}$$

and thus $a = b = 1$. Equations (62) and (63) can now be evaluated at $t > 0$ by substituting 1 for a and b,

$$(1, \psi(t)) = e^{-(i/\hbar)Et} \left[\frac{e^{(i/\hbar)At} + e^{-(i/\hbar)At}}{2} \right] = e^{-(i/\hbar)Et} \cos \frac{At}{\hbar} \quad , \qquad (65)$$

$$(2, \psi(t)) = e^{-(i/\hbar)Et} \left[\frac{e^{(i/\hbar)At} - e^{-(i/\hbar)At}}{2} \right] = i\, e^{-(i/\hbar)Et} \sin \frac{At}{\hbar} \quad . \qquad (66)$$

Finally, the probability that the system is in state $|1\rangle$ and $|2\rangle$ is

$$|(1, \psi(t))|^2 = \cos^2 \frac{At}{\hbar} \quad , \qquad |(2, \psi(t))|^2 = \sin^2 \frac{At}{\hbar} \quad , \qquad (67)$$

respectively. This results in an oscillation of the transition probabilities.

Let us shortly mention one particular realization of a two-state system which, among many others, has been discussed in the Feynman lectures [44]. Consider an ammonia (NH_3) molecule. If one fixes the plane spanned by the three hydrogen atoms, one observes two possible spatial configurations $|1\rangle$ and $|2\rangle$, corresponding to position of the nitrogen atom in the lower or the upper hemisphere, respectively (cf. Fig. 2). The nondiagonal elements of the Hamiltonian $H_{12} = H_{21} = -A$ correspond to a nonvanishing transition probability from one such configuration into the other. If the ammonia has been originally in state $|1\rangle$,

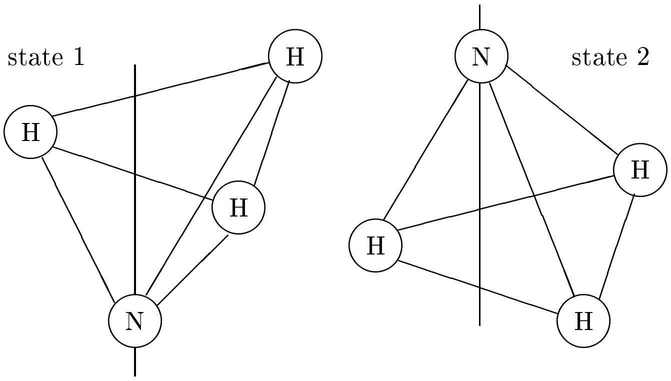


Figure 2: The two equivalent geometric arrangements of the ammonia (NH_3) molecule.

it will constantly swing back and forth between the two states, with a probability given by equations (67).

B From single to multiple quanta — "second" field quantization

The quantum formalism introduced in the main text is about *single* quantized objects. What if one wants to consider many such objects? Do we have to add assumptions in order to treat such multi-particle, multi-quanta systems appropriately?

The answer is yes. Experiment and theoretical reasoning (the representation theory of the Lorentz group [86] and the spin-statistics theorem [56, 71, 17, 54]) indicate that there are (at least) two basic types of states (quanta, particles): *bosonic* and *fermionic* states. Bosonic states have what is called "integer spin;" i.e., $s_b = 0, \tilde{}, 2\tilde{}, 3\tilde{}, \ldots$, whereas fermionic states have "half-integer spin;" $s_f = \frac{1\tilde{}}{2}, \frac{3\tilde{}}{2}, \frac{5\tilde{}}{2} \ldots$. Most important, they are characterized by the way identical copies of them can be "brought together." Consider two boxes, one for identical bosons, say photons, the other one for identical fermions, say electrons. For the first, bosonic, box, the probability that another identical boson is added *increases with the number of identical bosons* which are already in the box. There is a tendency of bosons to "condensate" into the same state. The second, fermionic box, behaves quite differently. If it is already occupied by one fermion, another identical fermion cannot enter. This is expressed in the *Pauli exclusion principle:* A system of fermions can never occupy a configuration of individual states in which two individual states are identical.

How can the bose condensation and the Pauli exclusion principle be implemented? There are several forms of implementation (e.g., fermionic behavior via Slater-determinants), but the most compact and widely practiced form uses operator algebra. In the following we shall present this formalism in the context of quantum field theory [52, 69, 56, 71, 17, 54, 46].

A *classical* field can be represented by its Fourier transform ("$*$" stands for complex conjugation)

$$A(x,t) = A^{(+)}(x,t) + A^{(-)}(x,t) \tag{68}$$

$$A^{(+)}(x,t) = [A^{(-)}(x,t)]^* \tag{69}$$

$$A^{(+)}(x,t) = \sum_{k_i,s_i} a_{k_i,s_i} u_{k_i,s_i}(x) e^{-i\omega_{k_i} t} \quad , \tag{70}$$

where $\nu = \omega_{k_i}/2\pi$ stands for the frequency in the field mode labeled by momentum k_i and s_i is some observable such as spin or polarization. u_{k_i,s_i} stands for the polarization vector (spinor) at k_i, s_i, and, most important with regards to the quantized case, *complex-valued* Fourier coefficients $a_{k_i,s_i} \in$ C.

¿From now on, the k_i, s_i-mode will be abbreviated by the symbol i; i.e., $1 \equiv k_1, s_1$, $2 \equiv k_2, s_2$, $3 \equiv k_3, s_3$, $\ldots$, $i \equiv k_i, s_i$, $\ldots$.

In (second[17]) quantization, the classical Fourier coefficients a_i become reinterpreted as *operators*, which obey the following algebraic rules (scalars would not do the trick). For *bosonic* fields (e.g., for the electromagnetic field), the

[17] of course, there is only "the one and only" quantization, the term "second" often refers to operator techniques for multiquanta systems; i.e., quantum field theory

commutator relations are ("†" stands for self-adjointness):

$$\left[a_i, a_j^\dagger\right] = a_i a_j^\dagger - a_j^\dagger a_i = \delta_{ij} \quad , \tag{71}$$

$$[a_i, a_j] = \left[a_i^\dagger, a_j^\dagger\right] = 0 \quad . \tag{72}$$

For *fermionic* fields (e.g., for the electron field), the *anti-commutator* relations are:

$$\{a_i, a_j^\dagger\} = a_i a_j^\dagger + a_j^\dagger a_i = \delta_{ij} \quad , \tag{73}$$

$$\{a_i, a_j\} = \{a_i^\dagger, a_j^\dagger\} = 0 \quad . \tag{74}$$

The anti-commutator relations, in particular $\{a_j^\dagger, a_j^\dagger\} = 2(a_j^\dagger)^2 = 0$, are just a formal expression of the Pauli exclusion principle stating that, unlike bosons, two or more identical fermions cannot co-exist.

The operators $a_i^\dagger$ and a_i are called *creation* and *annihilation* operators, respectively. This terminology suggests itself if one introduces *Fock states* and the *occupation number formalism.* $a_i^\dagger$ and a_i are applied to Fock states to following effect.

The Fock space associated with a quantized field will be the direct product of all Hilbert spaces H_i; i.e.,

$$\prod_{i\in \mathrm{I}} \mathrm{H}_i \quad , \tag{75}$$

where I is an index set characterizing all different field modes labeled by i. Each boson (photon) field mode is equivalent to a harmonic oscillator [46, 70]; each fermion (electron, proton, neutron) field mode is equivalent to the Larmor precession of an electron spin.

In what follows, only finite-size systems are studied. The Fock states are based upon the Fock vacuum. The Fock vacuum is a direct product of states $\mid 0_i\rangle$ of the i'th Hilbert space H_i characterizing mode i; i.e.,

$$\begin{aligned} \mid 0\rangle &= \prod_{i\in \mathrm{I}} \mid 0\rangle_i = \mid 0\rangle_1 \otimes \mid 0\rangle_2 \otimes \mid 0\rangle_3 \otimes \cdots \\ &= \mid \bigcup_{i\in \mathrm{I}} \{0_i\}\rangle = \mid \{0_1, 0_2, 0_3, \ldots\}\rangle \quad , \end{aligned} \tag{76}$$

where again I is an index set characterizing all different field modes labeled by i. "0_i" stands for 0 (no) quantum (particle) in the state characterized by the quantum numbers i. Likewise, more generally, "N_i" stands for N quanta (particles) in the state characterized by the quantum numbers i.

The annihilation operators a_i are designed to destroy one quantum (particle) in state i:

$$a_j \mid 0\rangle = 0 \quad , \tag{77}$$

$$\begin{aligned} &a_j \mid \{0_1, 0_2, 0_3, \ldots, 0_{j-1}, N_j, 0_{j+1}, \ldots\}\rangle = \\ &\quad = \sqrt{N_j} \mid \{0_1, 0_2, 0_3, \ldots, 0_{j-1}, (N_j - 1), 0_{j+1}, \ldots\}\rangle \quad . \end{aligned} \tag{78}$$

The creation operators $a_i^\dagger$ are designed to create one quantum (particle) in state i:

$$a_j^\dagger \mid 0\rangle = \mid \{0_1, 0_2, 0_3, \ldots, 0_{j-1}, 1_j, 0_{j+1}, \ldots\}\rangle \quad . \tag{79}$$

More generally, N_j operators $(a_j^\dagger)^{N_j}$ create an N_j-quanta (particles) state

$$(a_j^\dagger)^{N_j} \mid 0\rangle \propto \mid \{0_1, 0_2, 0_3, \ldots, 0_{j-1}, N_j, 0_{j+1}, \ldots\}\rangle \quad . \tag{80}$$

For fermions, $N_j \in \{0,1\}$ because of the Pauli exclusion principle. For bosons, $N_j \in \mathrm{N}_0$. With proper normalization [which can motivated by the (anti-)commutator relations and by $|(X,X)|^2 = 1$], a state containing N_1 quanta (particles) in mode 1, N_2 quanta (particles) in mode 2, N_3 quanta (particles) in mode 3, *etc.*, can be generated from the Fock vacuum by

$$\mid \bigcup_{i\in \mathrm{I}} \{N_i\}\rangle \equiv \mid \{N_1, N_2, N_3, \ldots\}\rangle = \prod_{i\in \mathrm{I}} \frac{(a_i^\dagger)^{N_i}}{\sqrt{N_i!}} \mid 0\rangle \quad . \tag{81}$$

As has been stated by Glauber [46, p. 64],

> … in quantum theory, there is an infinite set of complex numbers which specifies the state of a single mode. This is in contrast to classical theory where each mode may be described by a single complex number. This shows that there is vastly more freedom in quantum theory to invent states of the world than there is in the classical theory. We cannot think of quantum theory and classical theory in one-to-one terms at all. In quantum theory, there exist whole spaces which have no classical analogues, whatever.

C Quantum interference

In what follows, we shall make use of a simple "toolbox"-scheme of combining lossless elements of an experimental setup for the theoretical calculation [49]. The elements of this "toolbox" are listed in Table 1. These "toolbox" rules can be rigorously motivated by the full quantum optical calculations (e.g., [103, 24]) but are much easier to use. In what follows, the factor i resulting from a phase shift of $\pi/2$ associated with the reflection at a mirror M is *omitted.* However, at a half-silvered mirror beam splitter, the relative factor i resulting from a phase shift of $\pi/2$ *is* kept. (A detailed calculation [18] shows that this phase shift of $\pi/2$ is an approximation which is exactly valid only for particular system parameters). T and $R = \sqrt{1-T^2}$ are transmission and reflection coefficients. Notice that the "generic" beam splitter can be realized by a half-silvered mirror and a successive phase shift of $\varphi = -\pi/2$ in the reflected channel; i.e., $a \rightarrow (b+ic)/\sqrt{2} \rightarrow (b + ie^{-i\pi/2}c)/\sqrt{2} \rightarrow (b+c)/\sqrt{2}$. Note also that, in the "second quantization" notation, for $i<j$,

$$\mid i\rangle \mid j\rangle \equiv a_i^\dagger a_j^\dagger \mid 0\rangle = \mid i\rangle \otimes \mid j\rangle = \mid 0_1, 0_2, 0_3, \ldots, 0_{i-1}, 1_i, 0_{i+1}, \ldots, 0_{j-1}, 1_j, 0_{j+1}, \ldots\rangle \quad . \tag{82}$$

In present-day quantum optical nonlinear devices (NL), parametric up- or down-conversion, i.e., the production of a single quant (particle) from two field quanta

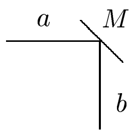
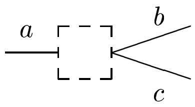
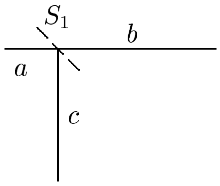
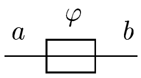
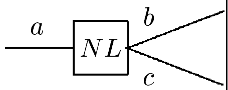
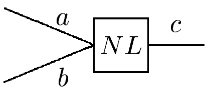
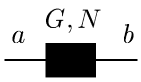
physical process	symbol	state transformation
reflection at mirror		$a \to b = ia$
"generic" beam splitter		$a \to (b+c)/\sqrt{2}$
transmission/reflection by a beam splitter (half-silvered mirror)		$a \to (b+ic)/\sqrt{2}$ $a \to Tb + iRc$, $T^2 + R^2 = 1$, $T, R \in [0,1]$
phase-shift φ		$a \to b = ae^{i\varphi}$
parametric down-conversion		$\lvert a\rangle \to \eta \lvert b\rangle \lvert c\rangle$
parametric up-conversion		$\lvert a\rangle \mid b\rangle \to \eta \lvert c\rangle$
amplification		$A_i a \to \lvert b; G, N\rangle$

Table 1: "Toolbox" of lossless elements for quantum interference devices.

(particles) and the production of two field quanta (particles) from a single one occurs at the very low amplitude rate of $\eta \approx 10^{-6}$.

In what follows, a lossless *Mach-Zehnder* interferometer drawn in Fig. 3 is discussed. The computation proceeds by successive substitution (transition) of

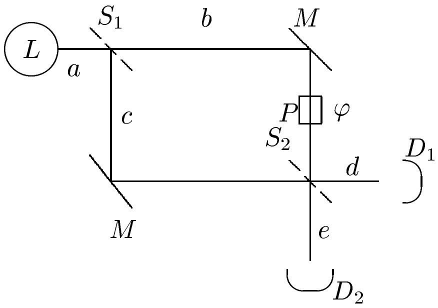


Figure 3: Mach-Zehnder interferometer. A single quantum (photon, neutron, electron *etc*) is emitted in L and meets a lossless beam splitter (half-silvered mirror) S_1, after which its wave function is in a coherent superposition of b and c. In beam path b a phase shifter shifts the phase of state b 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.

states; i.e.,

$$S_1: \; a \rightarrow (b+ic)/\sqrt{2} \quad , \tag{83}$$

$$P: \; b \rightarrow be^{i\varphi} \quad , \tag{84}$$

$$S_2: \; b \rightarrow (e+id)/\sqrt{2} \quad , \tag{85}$$

$$S_2: \; c \rightarrow (d+ie)/\sqrt{2} \quad . \tag{86}$$

The resulting transition is

$$a \rightarrow \psi = i\left(\frac{e^{i\varphi}+1}{2}\right)d + \left(\frac{e^{i\varphi}-1}{2}\right)e \quad . \tag{87}$$

Assume that $\varphi = 0$, i.e., there is no phase shift at all. Then, equation (87) reduces to $a \rightarrow id$, and the emitted quant is detected only by D_1. Assume that $\varphi = \pi$. Then, equation (87) reduces to $a \rightarrow -e$, and the emitted quant is detected only by D_2. If one varies the phase shift φ, one obtains the following detection probabilities:

$$P_{D_1}(\varphi) = |(d,\psi)|^2 = \cos^2(\frac{\varphi}{2}) \quad , \quad P_{D_2}(\varphi) = |(e,\psi)|^2 = \sin^2(\frac{\varphi}{2}) \quad . \tag{88}$$

For some "mindboggling" features of Mach-Zehnder interferometry, see [10].

D Universal 2-port quantum gate

The elementary quantum interference device $\mathbf{T}_{21}^{bs}$ depicted in Fig. (4.a) is just a beam splitter followed by a phase shifter in one of the output ports. According to the "toolbox" rules of appendix C, the process can be quantum mechanically described by[18]

$$
\begin{aligned}
P_1 &: \ \mathbf{0} \rightarrow \mathbf{0} e^{i\alpha+\beta} \quad , && (89)\\
P_2 &: \ \mathbf{1} \rightarrow \mathbf{1} e^{i\beta} \quad , && (90)\\
S &: \ \mathbf{0} \rightarrow T\,\mathbf{1}' + iR\,\mathbf{0}' \quad , && (91)\\
S &: \ \mathbf{1} \rightarrow T\,\mathbf{0}' + iR\,\mathbf{1}' \quad , && (92)\\
P_3 &: \ \mathbf{0}' \rightarrow \mathbf{0}' e^{i\varphi} \quad . && (93)
\end{aligned}
$$

If $\mathbf{0} \equiv \mathbf{0}' \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\mathbf{1} \equiv \mathbf{1}' \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and $R(\omega) = \sin\omega$, $T(\omega) = \cos\omega$, then the corresponding unitary evolution matrix which transforms any coherent superposition of $\mathbf{0}$ and $\mathbf{1}$ into a superposition of $\mathbf{0}'$ and $\mathbf{1}'$ is given by

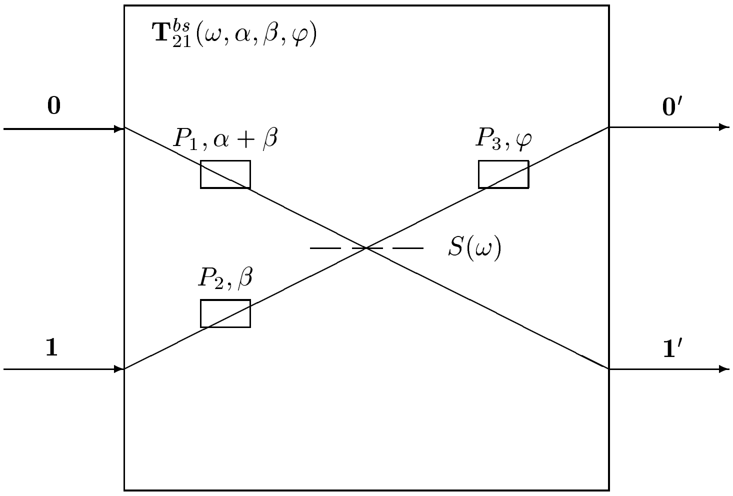
$$
\begin{aligned}
\mathbf{T}_{21}^{bs}(\omega,\alpha,\beta,\varphi) &= \left[e^{i\,\beta} \begin{pmatrix} i\,e^{i(\alpha+\varphi)}\ \sin\omega & e^{i\alpha}\ \cos\omega \\ e^{i\varphi}\ \cos\omega & i\ \sin\omega \end{pmatrix} \right]^{-1} \\
&= e^{-i\,\beta} \begin{pmatrix} -i\,e^{-i(\alpha+\varphi)}\ \sin\omega & e^{-i\varphi}\ \cos\omega \\ e^{-i\alpha}\ \cos\omega & -i\ \sin\omega \end{pmatrix} \quad . \qquad (94)
\end{aligned}
$$

The elementary quantum interference device $\mathbf{T}_{21}^{MZ}$ depicted in Fig. (4.b) is a (rotated) Mach-Zehnder interferometer with *two* input and output ports and three phase shifters. According to the "toolbox" rules, the process can be quantum mechanically described by

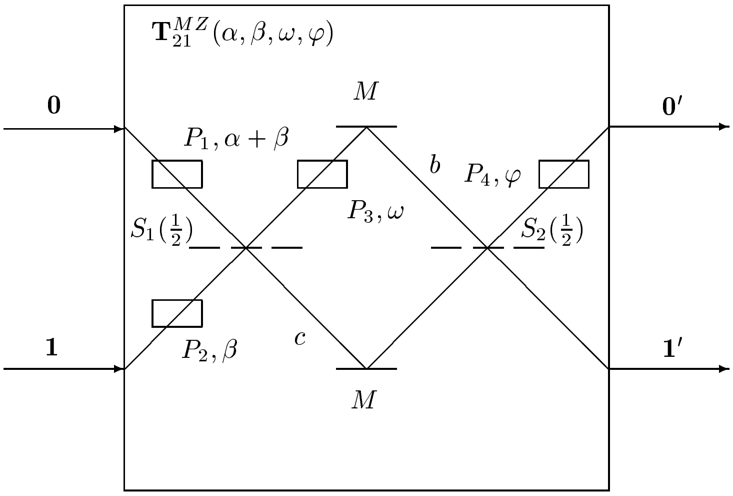
$$
\begin{aligned}
P_1 &: \ \mathbf{0} \rightarrow \mathbf{0} e^{i\alpha+\beta} \quad , && (95)\\
P_2 &: \ \mathbf{1} \rightarrow \mathbf{1} e^{i\beta} \quad , && (96)\\
S_1 &: \ \mathbf{1} \rightarrow (b + i\,c)/\sqrt{2} \quad , && (97)\\
S_1 &: \ \mathbf{0} \rightarrow (c + i\,b)/\sqrt{2} \quad , && (98)\\
P_3 &: \ c \rightarrow c e^{i\omega} \quad , && (99)\\
S_2 &: \ b \rightarrow (\mathbf{1}' + i\,\mathbf{0}')/\sqrt{2} \quad , && (100)\\
S_2 &: \ c \rightarrow (\mathbf{0}' + i\,\mathbf{1}')/\sqrt{2} \quad , && (101)\\
P_4 &: \ \mathbf{0}' \rightarrow \mathbf{0}' e^{i\varphi} \quad . && (102)
\end{aligned}
$$

---

[18] Alternatively, the action of a lossless beam splitter may be described by the matrix $\begin{pmatrix} T(\omega) & i\,R(\omega) \\ i\,R(\omega) & T(\omega) \end{pmatrix} = \begin{pmatrix} \cos\omega & i\ \sin\omega \\ i\ \sin\omega & \cos\omega \end{pmatrix}$. A phase shifter in a two-dimensional Hilbert space is represented by either $\begin{pmatrix} e^{i\varphi} & 0 \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$. The action of the entire device consisting of such elements is calculated by multiplying the matrices in reverse order in which the quanta pass these elements [103, 24].



a)



b)

Figure 4: Elementary quantum interference device. An elementary quantum interference device can be realized by a 4-port interferometer with two input ports $\mathbf{0}, \mathbf{1}$ and two output ports $\mathbf{0}', \mathbf{1}'$. Any two-dimensional unitary transformation can be realized by the devices. a) shows a realization by a single beam splitter $S(T)$ with variable transmission t and three phase shifters P_1, P_2, P_3; b) shows a realization with 50:50 beam splitters $S_1(\frac{1}{2})$ and $S_2(\frac{1}{2})$ and four phase shifters P_1, P_2, P_3, P_4.

When again $\mathbf{0} \equiv \mathbf{0}' \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\mathbf{1} \equiv \mathbf{1}' \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, then the corresponding unitary evolution matrix which transforms any coherent superposition of $\mathbf{0}$ and $\mathbf{1}$ into a superposition of $\mathbf{0}'$ and $\mathbf{1}'$ is given by

$$\mathbf{T}_{21}^{MZ}(\alpha,\beta,\omega,\varphi) = -i\, e^{-i(\beta+\frac{\omega}{2})} \begin{pmatrix} -e^{-i\,(\alpha+\varphi)}\, \sin\frac{\omega}{2} & e^{-i\,\varphi}\, \cos\frac{\omega}{2} \\ e^{-i\,\alpha}\, \cos\frac{\omega}{2} & \sin\frac{\omega}{2} \end{pmatrix} \quad . \tag{103}$$

The correspondence between $\mathbf{T}_{21}^{bs}(T(\omega),\alpha,\beta,\varphi)$ with $\mathbf{T}_{21}^{MZ}(\alpha',\beta',\omega',\varphi')$ in equations (94) (103) can be verified by comparing the elements of these matrices. The resulting four equations can be used to eliminate the four unknown parameters $\omega' = 2\omega$, $\beta' = \beta - \omega$, $\alpha' = \alpha - \pi/2$, $\beta' = \beta - \omega$ and $\varphi' = \varphi - \pi/2$; i.e.,

$$\mathbf{T}_{21}^{bs}(\omega,\alpha,\beta,\varphi) = \mathbf{T}_{21}^{MZ}(\alpha - \frac{\pi}{2}, \beta - \omega, 2\omega, \varphi - \frac{\pi}{2}) \quad . \tag{104}$$

Both elementary quantum interference devices are *universal* in the sense that *every* unitary quantum evolution operator in two-dimensional Hilbert space can be brought into a one-to-one correspondence to $\mathbf{T}_{21}^{bs}$ and $\mathbf{T}_{21}^{MZ}$; with corresponding values of T,α,β,φ or $\alpha,\omega,\beta,\varphi$. This can be easily seen by a similar calculation as before; i.e., by comparing equations (94) (103) with the "canonical" form of a unitary matrix, which is the product of a $U(1) = e^{-i\,\beta}$ and of the unimodular unitary matrix $SU(2)$ [76]

$$\mathbf{T}(\omega,\alpha,\varphi) = \begin{pmatrix} e^{i\,\alpha}\, \cos\omega & -e^{-i\,\varphi}\, \sin\omega \\ e^{i\,\varphi}\, \sin\omega & e^{-i\,\alpha}\, \cos\omega \end{pmatrix} \quad , \tag{105}$$

where $-\pi \le \beta,\omega \le \pi$, $-\frac{\pi}{2} \le \alpha,\varphi \le \frac{\pi}{2}$. Let

$$\mathbf{T}(\omega,\alpha,\beta,\varphi) = e^{-i\,\beta}\mathbf{T}(\omega,\alpha,\varphi) \quad . \tag{106}$$

A proper identification of the parameters $\alpha,\beta,\omega,\varphi$ yields

$$\mathbf{T}(\omega,\alpha,\beta,\varphi) = \mathbf{T}_{21}^{bs}(\omega - \frac{\pi}{2}, -\alpha - \varphi - \frac{\pi}{2}, \beta + \alpha + \frac{\pi}{2}, \varphi - \alpha + \frac{\pi}{2}) \quad . \tag{107}$$

Let us examine the realization of a few primitive logical "gates" corresponding to (unitary) unary operations on qbits. The "identity" element I is defined by $\mathbf{0} \to \mathbf{0}$, $\mathbf{1} \to \mathbf{1}$ and can be realized by

$$\mathrm{I} = T_{21}^{bs}(-\frac{\pi}{2}, -\frac{\pi}{2}, \frac{\pi}{2}, \frac{\pi}{2}) = T_{21}^{MZ}(-\pi, \pi, -\pi, 0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad . \tag{108}$$

The "`not`" element is defined by $\mathbf{0} \to \mathbf{1}$, $\mathbf{1} \to \mathbf{0}$ and can be realized by

$$\texttt{not} = T_{21}^{bs}(0,0,0,0) = T_{21}^{MZ}(-\frac{\pi}{2}, 0, 0, -\frac{\pi}{2}) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad . \tag{109}$$

The next element, "$\sqrt{\texttt{not}}$" is a truly quantum mechanical; i.e., nonclassical, one, since it converts a classical bit into a coherent superposition of $\mathbf{0}$ and $\mathbf{1}$. $\sqrt{\texttt{not}}$ is defined by $\mathbf{0} \to \mathbf{0} + \mathbf{1}$, $\mathbf{1} \to -\mathbf{0} + \mathbf{1}$ and can be realized by

$$\sqrt{\texttt{not}} = T_{21}^{bs}(-\frac{\pi}{4}, -\frac{\pi}{2}, \frac{\pi}{2}, \frac{\pi}{2}) = T_{21}^{MZ}(-\pi, \frac{3\pi}{4}, -\frac{\pi}{2}, 0) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \quad . \tag{110}$$

Note that $\sqrt{\texttt{not}}\cdot\sqrt{\texttt{not}} = \texttt{not}\cdot \mathrm{diag}(1,-1) = \texttt{not} \,(\mathrm{mod}\, 1)$. The relative phases in the output ports showing up in $\mathrm{diag}(1,-1)$ can be avoided by defining

$$\sqrt{\texttt{not}}' = T_{21}^{bs}(-\frac{\pi}{4},0,\frac{\pi}{4},0) = T_{21}^{MZ}(-\frac{\pi}{2},\frac{\pi}{2},-\frac{\pi}{2},-\frac{\pi}{2}) = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix} \quad . \tag{111}$$

With this definition, $\sqrt{\texttt{not}}'\sqrt{\texttt{not}}' = \texttt{not}$.

It is very important that the elementary quantum interference device realizes an arbitrary quantum time evolution of a two-dimensional system. The performance of the quantum interference device is determined by four parameters, corresponding to the phases $\alpha,\beta,\varphi,\omega$.

References

1. Albert, D. Z. On quantum-mechanical automata. *Physics Letters 94A*, 5,6 (1983), 249–252.
2. Anderson, A. R. St. Paul's epistle to Titus. In *The Paradox of the Liar*, R. L. Martin, Ed. Yale University Press, New Haven, 1970. The Bible contains a passage which refers to Epimenides, a Crete living in the capital city of Cnossus: *"One of themselves, a prophet of their own, said, 'Cretans are always liars, evil beasts, lazy gluttons.' "*,— St. Paul, Epistle to Titus I (12-13).
3. Ballentine, L. E. *Quantum Mechanics.* Prentice Hall, Englewood Cliffs, NJ, 1989.
4. Barenco, A., Bennett, C. H., Cleve, R., DiVincenzo, D. P., Margolus, N., Shor, P., Sleator, T., Smolin, J., and Weinfurter, H. Elementary gates for quantum computation.
e-print http://xxx.lanl.gov/abs/quant-ph/9503016.
5. Bell, J. S. *Speakable and Unspeakable in Quantum Mechanics.* Cambridge University Press, Cambridge, 1987.
6. Benioff, P. A. Quantum mechanical hamiltonian models of turing machines. *Journal of Statistical Physics 29*, 3 (1982), 515–546.
7. Benioff, P. A. Quantum mechanical hamiltonian models of computers. *Annals of the New York Akademy of Sciences 480* (1986), 475–486.
8. Bennett, C. H. Logical reversibility of computation. *IBM Journal of Research and Development 17* (1973), 525–532. Reprinted in [67, pp. 197-204].
9. Bennett, C. H. The thermodynamics of computation—a review. In *International Journal of Theoretical Physics* [67], pp. 905–940. Reprinted in [67, pp. 213-248].
10. Bennett, C. H. Night thoughts, dark sight. *Nature 371* (1994), 479–480.
11. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., and Smolin, J. Experimental quantum cryptography. *Journal of Cryptology 5* (1992), 3–28.
12. Bennett, C. H., and Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (1984), IEEE Computer Society Press, pp. 175–179.
13. Bennett, C. H., Brassard, G., Breidbart, S., and Wiesner, S. Quantum cryptography, or unforgable subway tokens. In *Advances in Cryptography: Proceedings of Crypto '82* (New York, 1982), Plenum Press, pp. 78–82.
14. Bernstein, E., and Vazirani, U. Quantum complexity theory. In *Proceedings of the 25th Annual ACM Symposium on Theory of Computing, San Diego, California, May 16-18, 1993* (1993), ACM Press, pp. 11–20.

15. Berthiaume, A., and Brassard, G. The quantum challenge to structural complexity theory. In *Proceedings, Structure in Complexity Theory, seventh annual conference, Boston University, Boston, Massachusetts, June 22-25, 1992* (1992), IEEE Computer Society Press, pp. 132–137.
16. Bishop, E., and Bridges, D. S. *Constructive Analysis.* Springer, Berlin, 1985.
17. Bogoliubov, N. N., and Shirkov, D. V. *Introduction to the Theory of Quantized Fields.* Wiley-Interscience, New York, 1959.
18. Born, M., and Wolf, E. *Principles of Optics: Electromagnetic Theory of Propagation, Interference and Diffraction of Light*, 6th ed. Pergamon Press, Oxford, 1993.
19. Bridges, D., and Richman, F. *Varieties of Constructive Mathematics.* Cambridge University Press, Cambridge, 1987.
20. Bridges, D. S. *Computability.* Springer, New York, 1994.
21. Bridgman, P. W. A physicists second reaction to Mengenlehre. *Scripta Mathematica 2* (1934), 101–117, 224–234. Cf. R. Landauer [65].
22. Bridgman, P. W. *Reflections of a Physicist.* Philosophical Library, New York, 1950.
23. Calude, C. *Information and Randomness—An Algorithmic Perspective.* Springer, Berlin, 1994.
24. Campos, R. A., Saleh, B. E. A., and Teich, M. C. Fourth-order interference of joint single-photon wave packets in lossless optical systems. *Physical Review A42* (1990), 4127.
25. Cantor, G. Gesammelte Abhandlungen. Springer, Berlin, 1932.
26. Caves, C. M. Quantum limits on noise in linear amplifiers. *Physical Review D26* (1982), 1817–1839.
27. Černý, V. Quantum computers and intractable (NP-complete) computing problems. *Physical Review A48* (1993), 116–119.
28. Chaitin, G. J. *Algorithmic Information Theory.* Cambridge University Press, Cambridge, 1987.
29. Chaitin, G. J. *Information, Randomness and Incompleteness*, second ed. World Scientific, Singapore, 1990. This is a collection of G. Chaitin's publications.
30. Chuang, I., Laflamme, R., Shor, P., and Zurek, W. Quantum computers, factoring, and decoherence. e-print http://xxx.lanl.gov/abs/quant-ph/9503007.
31. Davis, M. *Computability and Unsolvability.* McGraw-Hill, New York, 1958.
32. Davis, M. *The Undecidable.* Raven Press, New York, 1965.
33. Davydov, A. S. *Quantum Mechanics.* Addison-Wesley, Reading, MA, 1965.
34. Deutsch, D. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society London A 400* (1985), 97–119.
35. Deutsch, D. Quantum computational networks. *Proceedings of the Royal Society London A 425* (1989), 73–90.
36. Deutsch, D., and Jozsa, R. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society London A 439* (1992), 553–558.
37. Dieks, D. Communication by EPR devices. *Physics Letters 92A*, 6 (1982), 271–272.
38. Dirac, P. A. M. *The Principles of Quantum Mechanics.* Oxford University Press, Oxford, 1947.
39. Dunford, N., and Schwartz, J. T. *Linear Operators I.* Interscience Publishers, New York, 1958.
40. Einstein, A. Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt. *Annalen der Physik 17* (1905), 132–148.
41. Einstein, A., Podolsky, B., and Rosen, N. Can quantum-mechanical description of physical reality be considered complete? *Physical Review 47* (1935), 777–780. Reprinted in [100, pp. 138-141].

42. Feynman, R. P. Simulating physics with computers. *International Journal of Theoretical Physics 21* (1982), 467–488.
43. Feynman, R. P. Quantum mechanical computers. *Optics News 11* (February 1985), 11–20.
44. Feynman, R. P., Leighton, R. B., and Sands, M. *The Feynman Lectures on Physics. Quantum Mechanics*, vol. III. Addison-Wesley, Reading, MA, 1965.
45. Fredkin, E., and Toffoli, T. Conservative logic. *International Journal of Theoretical Physics 21* (1982), 219–253.
46. Glauber, R. J. Amplifyers, attenuators and the quantum theory of measurement. In *Frontiers in Quantum Optics*, E. R. Pikes and S. Sarkar, Eds. Adam Hilger, Bristol, 1986.
47. Gödel, K. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme. *Monatshefte für Mathematik und Physik 38* (1931), 173–198. English translation in [48], and in [32].
48. Gödel, K. In *Collected Works. Publications 1929-1936. Volume I*, S. Feferman, J. W. Dawson, S. C. Kleene, G. H. Moore, R. M. Solovay, and J. van Heijenoort, Eds. Oxford University Press, Oxford, 1986.
49. Greenberger, D. B., Horne, M., and Zeilinger, A. Multiparticle interferometry and the superposition principle. *Physics Today 46* (August 1993), 22–29.
50. Greenberger, D. B., and YaSin, A. "Haunted" measurements in quantum theory. *Foundation of Physics 19*, 6 (1989), 679–704.
51. Hamming, R. W. *Coding and Information Theory*, second ed. Prentice-Hall, Englewood Cliffs, NJ, 1980.
52. Harris, E. G. *A Pedestrian Approach to Quantum Field Theory.* Wiley-Interscience, New York, 1971.
53. Herbert, N. FLASH—a superluminal communicator based upon a new kind of quantum measurement. *Foundation of Physics 12*, 12 (1982), 1171–1179.
54. Itzykson, C., and Zuber, J.-B. *Quantum Field Theory.* MacGraw-Hill, New York, 1980.
55. Jammer, M. *The Philosophy of Quantum Mechanics.* John Wiley & Sons, New York, 1974.
56. Jauch, J. M., and Rohrlich. *The Theory of Photons and Electrons.* Addison-Wesley, Cambridge, MA, 1955.
57. Kochen, S., and Specker, E. P. Logical structures arising in quantum theory. In *Symposium on the Theory of Models, Proceedings of the 1963 International Symposium at Berkeley* (Amsterdam, 1965), North Holland, pp. 177–189.
58. Kochen, S., and Specker, E. P. The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics 17*, 1 (1967), 59–87.
59. Landauer, R. Letter, june 1st, 1994.
60. Landauer, R. Fundamental physical limitations of the computational process; an informal commentary. *Cybernetics Machine Group Newsheet* (1/1/1987).
61. Landauer, R. Irreversibility and heat generation in the computing process. In *IBM Journal of Research and Development* [67], pp. 183–191. Reprinted in [67, pp. 188-196].
62. Landauer, R. Wanted: a physically possible theory of physics. *IEEE Spectrum 4* (1967), 105–109.
63. Landauer, R. Computation, measurement, communication and energy dissipation. In *Selected Topics in Signal Processing*, S. Haykin, Ed. Prentice Hall, Englewood Cliffs, NJ, 1989, p. 18.
64. Landauer, R. Information is physical. *Physics Today 44* (May 1991), 23–29.
65. Landauer, R. Advertisement for a paper I like. In *On Limits*, J. L. Casti and J. F. Traub, Eds. Santa Fe Institute Report 94-10-056, Santa Fe, NM, 1994, p. 39.
66. Landauer, R. Zig-zag path to understanding. In *Proceedings of the Workshop on Physics and Computation PHYSCOMP '94* (Los Alamitos, CA, 1994), IEEE Computer Society Press, pp. 54–59.

67. Leff, H. S., and Rex, A. F. *Maxwell's Demon.* Princeton University Press, Princeton, 1990.
68. Li, M., and Vitányi, P. M. B. Kolmogorov complexity and its applications. In *Handbook of Theoretical Computer Sciences.* Elsevier Science Publishers, Amsterdam, 1990. [98].
69. Lipkin, H. J. *Quantum Mechanics, New Approaches to Selected Topics.* North-Holland, Amsterdam, 1973.
70. Loudon, R., and Knight, P. L. Squeezed light. *Journal of Modern Optics 34* (1987), 709–759.
71. Luriè, D. *Particles and Fields.* Interscience Publishers, New York, 1968.
72. Mandel, L. Is a photon amplifier always polarization dependent? *Nature 304* (1983), 188.
73. Mermin, N. D. What's wrong with these elements of reality? *Physics Today 43*, 6 (June 1990), 9–10.
74. Messiah, A. *Quantum Mechanics*, vol. I. North-Holland, Amsterdam, 1961.
75. Milonni, P. W., and Hardies, M. L. Photons cannot always be replicated. *Physics Letters 92A*, 7 (1982), 321–322.
76. Murnaghan, F. D. *The Unitary and Rotation Groups.* Spartan Books, Washington, 1962.
77. Odifreddi, P. *Classical Recursion Theory.* North-Holland, Amsterdam, 1989.
78. Peres, A. *Quantum Theory: Concepts and Methods.* Kluwer Academic Publishers, Dordrecht, 1993.
79. Planck, M. Ueber eine Verbesserung der Wien'schen Spectralgleichung. *Verhandlungen der deutschen physikalischen Gesellschaft 2* (1900), 202.
80. Planck, M. Die physikalische Struktur des Phasenraumes. *Annalen der Physik 50* (1916), 385–418.
81. Reck, M., and Zeilinger, A. Quantum phase tracing of correlated photons in optical multiports. In *Quantum Interferometry* (Singapore, 1994), F. D. Martini, G. Denardo, and A. Zeilinger, Eds., World Scientific.
82. Reck, M., Zeilinger, A., Bernstein, H. J., and Bertani, P. Experimental realization of any discrete unitary operator. *Physical Review Letters 73* (1994), 58–61.
83. Rogers, Jr., H. *Theory of Recursive Functions and Effective Computability.* MacGraw-Hill, New York, 1967.
84. Rosen, R. Effective processes and natural law. In *The Universal Turing Machine. A Half-Century Survey*, R. Herken, Ed. Kammerer & Unverzagt, Hamburg, 1988, p. 523.
85. Schrödinger, E. Die gegenwärtige Situation in der Quantenmechanik. *Naturwissenschaften 23* (1935), 807–812, 823–828, 844–849. English translation in [100, pp. 152-167].
86. Sexl, R. U., and Urbantke, H. K. *Relativität, Gruppen, Teilchen.* Springer, Vienna, 1976.
87. Shor, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium of on Foundations of Computer Science, Santa Fe, NM, Nov. 20-22, 1994* (November 1994), IEEE Computer Society Press.
e-print http://xxx.lanl.gov/abs/quant-ph/9508027.
88. Solomonoff, R. J. A formal theory of inductive inference. part i. *Information and Control 7* (1964), 1–22.
89. Solovay, R. M. unpublished manuscript.
90. Svozil, K. The consistent use of paradoxes. Foundations of Physics Letters, in press.
91. Svozil, K. Speedup in quantum computation is associated with attenuation of processing probability.

e-print http://tph.tuwien.ac.at/~svozil/publ/kraft.ps
e-print http://xxx.lanl.gov/abs/hep-th/9412046.

92. Svozil, K. *Randomness & Undecidability in Physics.* World Scientific, Singapore, 1993.
93. Svozil, K. Halting probability amplitude of quantum computers. *Journal of Universal Computer Science 1*, 3 (March 1995).
94. Svozil, K. Quantum computation and complexity theory. part I. *Bulletin of the European Association of Theoretical Computer Sciences 55* (1995), 170–207. e-print http://tph.tuwien.ac.at/~svozil/publ/qct1.ps.
95. Svozil, K. Quantum computation and complexity theory. part II. *Bulletin of the European Association of Theoretical Computer Sciences 56* (1995), 116–136. e-print http://tph.tuwien.ac.at/~svozil/publ/qct2.ps.
96. Svozil, K. Set theory and physics. *Foundations of Physics 25* (1995), 1541–1560.
97. Turing, A. M. On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society, Series 2 42 and 43* (1936-7 and 1937), 230–265 and 544–546. reprinted in [32].
98. van Leeuwen, J. *Algorithms and Complexity*, vol. A. Elsevier and MIT Press, Amsterdam and Cambridge, MA, 1990.
99. von Neumann, J. *Mathematische Grundlagen der Quantenmechanik.* Springer, Berlin, 1932. English translation: Mathematical Foundations of Quantum Mechanics, Princeton University Press, Princeton, 1955.
100. Wheeler, J. A., and Zurek, W. H. *Quantum Theory and Measurement.* Princeton University Press, Princeton, 1983.
101. Wigner, E. P. The unreasonable effectiveness of mathematics in the natural sciences. Richard Courant Lecture delivered at New York University, May 11, 1959. *Communications on Pure and Applied Mathematics 13* (1960), 1.
102. Wooters, W. K., and Zurek, W. H. A single quantum cannot be cloned. *Nature 299* (1982), 802–803.
103. Yurke, B., McCall, S. L., and Klauder, J. R. SU(2) and SU(1,1) interferometers. *Physical Review A33* (1986), 4033–4054.