CDMTCS
Research
Report
Series

Quantum information: the new frontier

Karl Svozil
Theoretische Physik, Technische
Universität Wien, Viena Austria

CDMTCS-145
September 2000

Centre for Discrete Mathematics and
Theoretical Computer Science

Quantum information: the new frontier

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

http://tph.tuwien.ac.at/~svozil/publ/2000-qitnf.tex .tex

Abstract

Quantum information and computation is the new hype in physics. It is promising, mindboggling and even already applicable in cryptography, with good prospects ahead. A brief, rather subjective outline is presented.

1 Is Nature telling us something?

Friends in experimental physics tell me that the essence of their observations are clicks in some counter. There is a click or there is none. This is experimental physics in a nutshell. There may be some magic in properly designing experiments and some magic in interpreting those clicks, but that is all there is.

A single click represents some elementary physical proposition. It is also an answer to a question which might not even have been posed consciously. It is tempting to state that “Nature wants to tell us something” with these clicks about some formal structures, symmetries, music or numbers beyond the phenomena. Maybe that is the case, and most physicists tend to believe so; but maybe we are just observing crap, erratic emanations devoid of any meaning [1].

Anyway, we have to deal with those clicks, and one way to deal with them is to interpret them as information. For example, in an experimental input-output scheme, information is received, transformed and communicated by the system. One might think of a physical system as a black box with an input and an output interface [2]. The experimenter inputs some information and the black box responds with some information as output.

If we are dealing with mechanical systems, all the conceivable gadgets inside the black box can be isomorphically translated into a sheet or a tape of paper on which finite computations are performed and vice versa. This was Turing's insight.

But if the black box is essentially quantum driven, then the paper metaphor becomes questionable. The quantum is illusive and highly nonintuitive. In the words of John Archibald Wheeler, one is capturing a "smoky [[quantum]] dragon" [3] inside the black box. Or, in Danny Greenberger's dictum, "quantum mechanics is magic" [4]. In addition, quantized systems such as the quantized electromagnetic field have "more" degrees of freedom as compared to their classical correspondents. Therefore, any isomorphic translation into classical mechanistic devices remains very expensive in terms of paper consumption, at best. To make things worse, under certain reasonable side assumption, it can be proven that a complete "mechanical" paper set of all quantum answers is inconsistent.

Because of these novel non-classical features it is so exiting to pursue the quantum information concept. But even if we look aside and do not want to be bothered with the quantum, the quantum catches up on us: due to the progressing miniaturization of circuits forming logical gates, we shall soon be confronted with quantum phenomena there. In the following, some of the recent developments are reviewed below; and some speculations and prospects are mentioned.

2 Formalization of quantum information

In order to be applicable, any formalization of information has to be based on its proper realization in physical terms; i.e., as states of a physical system. In this view, information theory is part of physics; or conversely, physics is part of information theory. And just as the classical bit represents the distinction between two classical physical states, the quantum bit, henceforth often abbreviated by the term *'qubit,'* represents the conceivable states of the most elementary quantized system. As we shall see, qubits feature quantum mechanics 'in a nutshell.' Quantum bits are more general structures than classical bits. That is, classical bits can be represented as the limit of qubits, but not vice versa.

Classical information theory 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 $\#(t) = 1$ and $\#(f) = 0$ ($\#(s)$ stands for the code of s). The states can, for instance, be realized by some condenser which is discharged ($\equiv$ cbit state 0) or charged ($\equiv$ cbit state 1).

In quantum information theory (see Appendix A for a brief outline of quantum mechanics) qubits can be physically represented by a *'coherent superposition'* of the two orthonormal[1] states t and f. The qubit states

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

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

What is a coherent superposition? Formally it is just a sum of two elements (representing quantum states) in Hilbert space, which results in an element (a quantum state) again per definition. So, formally we are on the safe side. Informally speaking, a coherent superposition of two different and classically distinct states contains them both. Now classically this sounds like outright nonsense! A classical bit cannot be true and false at the same time. This would be inconsistent, and inconsistencies in physics sound as absurd as in mathematics [5].

Yet, quantum mechanics (so far consistently) achieves the implementation of classically inconsistent information into a single quantum bit. Why is that possible? Maybe we get a better feeling for this when we take up Erwin Schrödinger's interpretation of the quantum wave function (in our terms: of the qubit states) as a sort of "catalogue of expectation values" [6]. That is, the qubit appears to be a *representation of the state of our knowledge* about a physical system rather than what may be called "its true state." (Indeed we have to be extremely careful here with what we say. The straightforward classical pretension that quantum systems must have "a true state", albeit hidden to us, yields to outright contradictions!)

Why have I mentioned quantum superpositions here? Because they lie at the heart of quantum parallelism. And quantum parallelism lies at the heart of the quantum speedups which caused so much hype recently.

The coding of qubits is discussed in Appendix C.

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

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

what methods it is inferred. It obeys classical logic. It can be copied. No doubts can be left.

By contrast, to mention just a few nonclassical properties of qubits:

- Qubits are contextual [7]. A quantum bit may appear different, depending on the method by which it is inferred.
- Qubits cannot be copied or "cloned" [8, 9, 10, 11, 12, 13]. This due to the fact that the quantum evolution is reversible, i.e., one-to-one.
- Qubits do not necessarily satisfy classical tautologies such as the distributive law [14, 15].
- Qubits obey quantum logic [16] which is different from classical logic.
- Qubits are coherent superpositions of classically distinct, contradicting information.
- Qubits are subject to complementarity.

3 Complementarity and quantum cryptography

Before we proceed to quantum computing, which makes heavy use of the possibility to superpose classically distinct information, we shall mention an area of quantum information theory which has already matured to the point where the applications have almost become commercially available: quantum cryptography. At the moment, this might be seen as *the* "killer app" of quantum information theory.

Quantum cryptography (for a detailed review see [17]) is based on the quantum mechanical feature of *complementarity.* A formalization of quantum complementarity has been attempted by Edward Moore [18] who started finite automata theory with this. (Recent results are contained in Ref. [19] and [20, chapter 10]; see also Appendix B.)

Informally speaking, quantum complementarity stands for the principal impossibility to measure two observables at the same time with arbitrary position. If you decide to precisely measure the first observable, you "loose control" over the second one and vice versa. By measuring one observable, the state of the system undergoes a "state reduction" or, expressed differently, "the wave function collapses" and becomes different from the original one. This randomizes a subsequent measurement of the second, complementary observable: in performing the subsequent measurement, one obtains some measurement results (i.e., clicks, you remember?), but they dont tell us much about the original qubit, they are unusable crap. There is no other way of recoving the original state than by completely "undoing" the first measurement in such a way that no trace is left of the previous measurement result; not even a copy of the "classical measurement"[2] result!

So how can this quantum property of complentarity can be put to use in cryptography? The answer is straightforward (if one knows it already): By taking advantage of complementarity, the sender "Alice" of a secret and the receiver "Bob" are able to monitor the secure quantum communication channel and to know when an eavesdropper is present.

This can be done as follows. Assume that Alice sends Bob a qubit and an eavesdropper is present. This eavesdropper is in an inescapable dilemma: neither can the qubit be copied, nor can it be measured. The former case is forbidden in quantum information theory and the letter case would result in a state reduction which modifies Alice's qubit to the point where it is nonsense for Bob. Bob and Alice can realize this by comparing some of their results over a classical (insecure) channel.[3] The exact protocol can for instance be found in [17]. Another scheme [21] operates with entangled pairs of qubits. Here entanglement means that whatever measurement of a particular type is performed on one qubit, if you perform the same measurement on the other qubit of the pair, the result is the same.

Actually, in the real world, the communication over the insecure classical channel has to go back and forth, and they have to constantly compare a certain amount of their measured qubits in order to be able to assure a guaranteed amount of certainty that no eavesdropper is present. That is by no means trivial [22]. But besides this necessary overhead, the quantum channel can be certified to be secure, at least up to some desired amount of certainty and up to the point where someone comes up with a theory which is "better than quantum mechanics" and which circumvents complementarity somehow. Of course, the contemporaries always believe and assure the authorities that there will never be such a theory!

Quantum cryptographic schemes of the above type have already been demonstrated to work for distances of 1000m (and longer) and net key sizes (after error correction) of 59000 Bits at sustained (105 s) production rates of 850 Bits/s [23]. Yet there is no commercially available solution so far.

[2] I put a quote here because if one is able to "undo a measurement", then this process cannot be classical: per definition, classicality means irreversibility, many-to-oneness.

[3] Actually, if the eavesdropper has total control over the classical channel, this might be used for a reasonable attack strategy.

4 Quantum computing

Quantum computers operate with qubits. We have dealt with qubits already. Now what about the operation of quantum computers on qubits? We have to find something similar than Turing's "paper-and-pencil-operations" on paper or tape. The most natural candidate for a formalization is the unitary time evolution of the quantum states. This is all there is (maybe besides measurement [24]), because there is nothing beyond the unitary time evolution. Unitary operators stand for generalized rotations in complex Hilbert spaces. Therefore, a universal quantum computer can just be represented by the most general unitary operator!

That is a straightforward concept: given a finite dimensional Hilbert space of, say, dimension n, then the most general unitary operator $U(n)$ can for instance be parameterized by composition of unitary operations in two (sub)dimensions $U(2)$ [25]. Now we all know how $U(2)$ looks like (cf. Appendix D), so we know how $U(n)$ looks like. Hence we all know how to properly formalize a universal quantum computer!

This looks simple enough, but where is the advantage? Of course one immediate answer is that it is perfectly all right to simulate a quantized system with a quantum computer — we all know that every system is a perfect copy of itself!

But that is not the whole story. What is really challenging here is that we may be able to use quantum parallelism for speedups. And, as mentioned already, at the heart of quantum parallelism is the superposition principle and quantum entanglement. Superposition enables the quantum programmer to "squeeze" 2^N classical bits into N qubits. In processing 1 qubit state $\alpha t + \beta f$, the computer processes 2 classical bit states t and f at once. In processing N qubit states, the computer may be able to processes 2^N classical bit states at once. Many researchers in quantum computing interpret this (in the so-called "Everett interpretation of quantum mechanics") as an indication that 2^N seperate computer run in 2^N seperate worlds (one computer in each world); thereby running through each one of the computational passes in parallel. That might certainly be a big advantage as compared to a classical routine which might only be able to process the cases consecutively, one after the other.

There are indeed indications that speedups are possible. The most prominent examples are Shor's quantum algorithm for prime factoring [26, 27] and Grover's search algorithm [28] for a single item satisfying a given condition in an unsorted database. A detailed review of the suggested quantum algorithms exceeds the scope of this brief discussion and can for instance be found in Gruska's book [29].

One fundamental feature of the unitary evolution is its bijectivity, its one-to-oneness. This is the reason why copying is not allowed, but this is also the reason why there is no big waste basked where information vanishis into oblivion or nirvana forever. In a quantum computer, one and the same "message" is constantly permutated. It always remains the same but expresses itself through different forms. Information is neither created nor discarded but remains constant at all times.[4]

Is there a price to be pad for parallelism? Let me just mention one important problem here: the problem of the readout of the result. This is no issue in classical computation. But in quantum computation, to use the Everett metaphor, it is by no means trivial how the many parallel entangled universes communicate with each other in such a way that the classical result can be properly communicated. In many cases one has to make sure that, through positive interference, the proper probability amplitudes indicating this result build up. One may even speculate that there is no sufficient buildup of the states if the problem allows for many nonunique solutions [30, 31].

5 Summary and outlook

Let me close with a few observations. So far, quantum information theory has applied the quantum features of complementarity, entanglement and quantum parallelism to more or less real-world applications. Certain other quantum features such as contextuality have not been put to use so far.

There are good prospects for quantum computing; if not for other reasons but because our computer parts will finally reach the quantum domain. We may be just at the very beginning, having conceived the quantum analogies of classical tubes (e.g., quantum optical devices). Maybe in the near future someone comes up with a revolutionary design such as a "quantum transistor" which will radically change the technology of information processing.

This is a very exciting and challenging new field of physics and computer sciences.

[4] This implicit time symmetry spoils the very notion of "progress" or "achievement," since what is a valuable output is purely determined by the subjective meaning the observer associates with it and is devoid of any syntactic relevance.

Appendix A: All (and probably more that) you ever wanted to know about quantum mechanics

“Quantization” has been introduced by Max Planck around 1900 [32, 33, 34]. In a courageous, bold step 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 $P \in \mathbf{N}_0$ is zero or a positive integer and ϵ stands for the *smallest quantum of energy.* ϵ is a linear function of frequency ω and proportional to Planck's fundamental constant $\hbar \approx 10^{-34}$ Js; i.e.,

$$\epsilon = \hbar\omega.$$

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 [35] proposed a quantization of the electromagnetic field. According to the light quantum hypothesis, energy in an electric field mode characterized by the frequency ω can be produced, absorbed and exchanged only in a discrete number n of “lumps” or “quanta” or “photons”

$$E_n = n\hbar\omega\ ,\ n = 0, 1, 2, 3, \ldots\ .$$

The following is a very brief introduction to the principles of quantum mechanics for logicians and computer scientists, as well as a reminder for physicists.[5] 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 [49] is adopted.[6]

Quantum mechanics, just as classical mechanics, can be formalized in terms of a linear space structure, in particular by Hilbert spaces [45]. That is, all objects of quantum physics, in particular the ones used by quantum logic,

[5] Introductions to quantum mechanics can be found in Feynman, Leighton & M. Sands [36], Harris [37], Lipkin [38], Ballentine [39], Messiah [40], Davydov [41], Dirac [42], Peres [43], Mackey [44], von Neumann [45], and Bell [46], among many other expositions. The history of quantum mechanics is reviewed by Jammer [47]. Wheeler & Zurek [48] published a helpful resource book.

[6] 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 $\langle i \mid A \mid j\rangle \equiv A_{ij}$.

ought to be expressed in terms of objects based on concepts of Hilbert space theory—scalar products, linear summations, subspaces, operators, measures and so on.

Unless stated differently, only finite-dimensional Hilbert spaces are considered.[7]

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

We shall make the following identifications between physical and theoretical objects (a *caveat:* this is an incomplete list).

(0) The dimension of the Hilbert space corresponds to the number of degrees of freedom.

(I) A *pure physical state* x is represented either by the one-dimensional linear subspace (closed linear manifold) $^{(}x)=\{y\mid y=\alpha x,\ \alpha\in\mathbf{C},\ x\in\mathcal{H}\}$ spanned by a (normalized) vector x of the Hilbert space $\mathcal{H}$ or by the orthogonal projection operator E_x onto $^{(}x)$. Thus, a vector $x\in\mathcal{H}$ represents a pure physical state.

Every one-dimensional projection E_x onto a one-dimensional linear subspace $^{(}x)$ spanned by $x\in\mathcal{H}$ can be represented by the dyadic product $E_x=|x)(x|$.

If two nonparallel vectors $x,y\in\mathcal{H}$ represent pure physical states, their vector sum $z=x+y\in\mathcal{H}$ is again a vector representing a pure physical state. This state z is called the *superposition* of state x and y.[8]

[7] Infinite dimensional cases and continuous spectra are nontrivial extensions of the finite dimensional Hilbert space treatment. As a heuristic rule, which is not always correct, it might 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 $\mathbf{1}=\int_{-\infty}^{+\infty}|i)(i|\,di$. For a careful treatment, see, for instance, the books by Reed and Simon [50, 51].

[8] $x+y$ is sometimes referred to as "coherent" superposition to indicate the difference to "incoherent" mixtures of state vectors, in which the absolute squares $|x|^2+|y|^2$ are summed up.

Elements $b_i, b_j \in \mathcal{H}$ of the set of orthonormal base vectors satisfy $(b_i, b_j) = \delta_{ij}$, where $\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$ is the Kronecker delta function. Any pure state x can be written as a linear combination of the set of orthonormal base vectors $\{b_1, b_2, \cdots\}$, i.e., $x = \sum_{i=1}^{n} \beta_i b_i$, where n is the dimension of $\mathcal{H}$ and $\beta_i = (b_i, x) \in \mathbf{C}$. In the Dirac bra-ket notation, unity is given by $\mathbf{1} = \sum_{i=1}^{n} |b_i)(b_i|$.

In the nonpure state case, the system is characterized by the density operator ρ, which is nonnegative and of trace class.[9] If the system is in a nonpure state, then the preparation procedure does not specify the decomposition into projection operators (depending on the choice of basis) precisely. ρ can be brought into its spectral form $\rho = \sum_{i=1}^{n} P_i E_i$, where E_i are projection operators and the P_i's are the associated probabilities (nondegenerate case[10]).

(II) *Observables* A are represented by hermitian operators A on the Hilbert space $\mathcal{H}$ such that $(Ax, y) = (x, Ay)$ for all $x, y \in \mathcal{H}$. (Observables and their corresponding operators are identified.) In matrix notation, the adjoint matrix $A^\dagger$ is the complex conjugate of the transposed matrix of A; i.e., $(A^\dagger)_{ij} = (A^*)_{ji}$. Hermiticity means that $(A^\dagger)_{ij} = A_{ij}$.

Any hermitian operator has a spectral representation $A = \sum_{i=1}^{n} \alpha_i E_i$, where the E_i's are orthogonal projection operators onto the orthonormal eigenvectors a_i of A (nondegenerate case).

Note that the projection operators, as well as their corresponding vectors and subspaces, have a double rôle as pure state and elementary proposition (that the system is in that pure state).

Observables are said to be *compatible* or *comeasurable* if they can be defined simultaneously with arbitrary accuracy. Compatible observables are polynomials (Borel measurable functions in the infinite dimensional case) of a single "Ur"-observable.

A criterion for compatibility is the *commutator.* Two observables A, B are compatible if their *commutator* vanishes; i.e., if $[A, B] = AB - BA = 0$. In this case, the hermitian matrices A and B can be simultaneously diagonalized, symbolizing that the observables corre-

[9] Nonnegativity means $(\rho x, x) = (x, \rho x) \geq 0$ for all $x \in \mathcal{H}$, and trace class means trace$(\rho) = 1$.

[10] If the same eigenvalue of an operator occurs more than once, it is called *degenerate.*

sponding to A and B are simultaneously measurable.[11]

It has recently been demonstrated that (by an analog embodiment using particle beams) every hermitian operator in a finite dimensional Hilbert space can be experimentally realized [52].

Actually, one can also measure normal operators N which can be decomposed into the sum of two commuting operators A, B according to $N = A + iB$, with $[A, B] = 0$.

(III) The result of any single measurement of the observable A on an arbitrary state $x \in \mathcal{H}$ can only be one of the real eigenvalues of the corresponding hermitian operator A. (Actually, one can also measure normal operators which can be decomposed into the sum of two commuting If $x = \beta_1 a_1 + \cdots + \beta_i a_i + \cdots + \beta_n a_n$ is in a superposition of eigenstates $\{a_1, \ldots, a_n\}$ of A, the particular outcome of any such single measurement is indeterministic; i.e., it cannot be predicted with certainty. As a result of the measurement, the system is in the state a_i which corresponds to the associated real-valued eigenvalue α_i which is the measurement outcome; i.e.,

$$x \rightarrow a_i.$$

The arrow symbol "→" denotes an irreversible measurement; usually interpreted as a "transition" or "reduction" of the state due to an irreversible interaction of the microphysical quantum system with a classical, macroscopic measurement apparatus. This "reduction" has given rise to speculations concerning the "collapse of the wave function (state)."

As has been argued recently (e.g., by Greenberger and YaSin [53], and by Herzog, Kwiat, Weinfurter and Zeilinger [54]), it is possible to reconstruct the state of the physical system before the measurement; i.e., to "reverse the collapse of the wave function," if the process of measurement is reversible. After this reconstruction, no information about the measurement is left, not even in principle.

[11] Let us first diagonalize A; i.e., $A_{ij} = \text{diag}\,(A_{11}, A_{22}, \ldots, A_{nn})_{ij} = \left\{ \begin{array}{cl} A_{ii} & \text{if } i = j \\ 0 & \text{if } i \neq j \end{array} \right.$. Then, if A commutes with B, the commutator $[A, B]_{ij} = (AB - BA)_{ij} = A_{ik}B_{ki} - B_{ik}A_{kj} = (A_{ii} - A_{jj})B_{ij} = 0$ vanishes. If A is nondegenerate, then $A_{ii} \neq A_{jj}$ and thus $B_{ij} = 0$ for $i \neq j$. In the degenerate case, B can only be block diagonal. That is, each one of the blocks of B corresponds to a set of equal eigenvalues of A such that the corresponding subblockmatrix of A is proportional to the unit matrix. Thus, each block of B can be diagonalized separately without affecting A [43, p. 71].

How did Schrödinger, the creator of wave mechanics, perceive the quantum physical state, or, more specifically, the ψ-function? In his 1935 paper "Die gegenwärtige Situation in der Quantenmechanik" ("The present situation in quantum mechanics" [6, p. 823]), Schrödinger states,[12]

> *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.

It therefore seems not unreasonable to state that, epistemologically,

[12] *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.

quantum mechanics appears more as a theory of knowledge of an (intrinsic) observer rather than the Platonic 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.

(IV) The probability $P_x(y)$ to find a system represented by a normalized pure state x in some normalized pure state y is given by

$$P_x(y) = |(x,y)|^2, \quad |x|^2 = |y|^2 = 1.$$

In the nonpure state case, The probability $P(y)$ to find a system characterized by ρ in a pure state associated with a projection operator E_y is

$$P_\rho(y) = \text{trace}(\rho E_y).$$

(V) The *average value* or *expectation value* of an observable A represented by a hermitian operator A in the normalized pure state x is given by

$$\langle A \rangle_x = \sum_{i=1}^{n} \alpha_i |(x,a_i)|^2, \quad |x|^2 = |a_i|^2 = 1.$$

The *average value* or *expectation value* of an observable A represented by a hermitian operator A in the nonpure state ρ is given by

$$\langle A \rangle = \text{trace}(\rho A) = \sum_{i=1}^{n} \alpha_i \text{trace}(\rho E_i).$$

(VI) The dynamical law or equation of motion between subsequent, irreversible, measurements 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.*[13] Per definition, this evolution is reversible; i.e., bijective, one-to-one. So, in quantum mechanics we have to distinguish between unitary, reversible evolution of the system inbetween measurements, and the "collapse of the wave function" at an irreversible measurement.

[13] Any unitary operator $U(n)$ in finite-dimensional Hilbert space can be represented by the product — the serial composition — of unitary operators $U(2)$ acting in twodimensional subspaces [25, 52].

> The *Schrödinger equation* $i\hbar\frac{\partial}{\partial t}\psi(t) = H\psi(t)$ for some state ψ is obtained by identifying U with $U = e^{-iHt/\hbar}$, where H is a hermitian Hamiltonian ("energy") operator, by partially 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 $i\hbar\frac{\partial}{\partial t}(b_i, \psi(t)) = \sum_j H_{ij}(b_j, \psi(t))$.
>
> For stationary states $\psi_n(t) = e^{-(i/\hbar)E_n t}\psi_n$, the Schrödinger equation can be brought into its time-independent form $H\,\psi_n = E_m\,\psi_m$ (nondegenerate case). Here, $i\hbar\frac{\partial}{\partial t}\psi_m(t) = E_m\,\psi_m(t)$ has been used; E_m and ψ_m stand for the m'th eigenvalue and eigenstate of H, respectively.

Usually, a physical problem is defined by the Hamiltonian H and the Hilbert space in question. The problem of finding the physically relevant states reduces to finding a complete set of eigenvalues and eigenstates of H.

Appendix B: Complementarity and automaton logic

A systematic, formal investigation of the black box system or any finite input/output system can be given by finite automata. Indeed, the study of finite automata was motivated from the very beginning by their analogy to quantum systems [18]. Finite automata are universal with respect to the class of computable functions. That is, universal networks of automata can compute any effectively (Turing-) computable function. Conversely, any feature emerging from finite automata is reflected by any other universal computational device. In this sense, they are "robust". All rationally conceivable finite games can be modeled by finite automata.

Computational complementarity, as it is sometimes called [55], can be introduced as a game between Alice and Bob. The rules of the game are as follows. Before the actual game, Alice gives Bob all he needs to know about the intrinsic workings of the automaton. For example, Alice tells Bob, *"if the automaton is in state 1 and you input the symbol 2, then the automaton will make a transition into state 2 and output the symbol 0,"* and so on. Then Alice presents Bob a black box which contains a realization of the automaton. Attached to the black box are two interfaces: a keyboard for the input of symbols, and an output display, on which the output symbols appear. Again, no other interfaces are allowed. In particular, Bob is not allowed to "screw the box open."

Suppose now that Alice chooses some initial state of the automaton. She may either throw a dice, or she may make clever choices using some formalized system. In any case, Alice does not tell Bob about her choice. All Bob has at his disposal are the input-output interfaces.

Bob's goal is to find out which state Alice has chosen. Alice's goal is to fool Bob.

Bob may simply guess or rely on his luck by throwing a dice. But Bob can also perform clever input-output experiments and analyze his data in order to find out. Bob wins if he gives the correct answer. Alice wins if Bob's guess is incorrect. (So, Alice has to be really mean and select worst-case scenarios).

Suppose that Bob tries very hard. Is cleverness sufficient? Will Bob always be able to uniquely determine the initial automaton state?

The answer to that question is "no." The reason is that there may be situations when Bob's input causes an irreversible transition into a black box state which does not allow any further queries about the initial state.

What has been introduced here as a game between Alice and Bob is what the mathematicians have called the *state identification problem* [18, 56, 57, 58]: given a finite deterministic automaton, the task is to locate an unknown initial state. Thereby it is assumed that only *a single* automaton copy is available for inspection. That is, no second, identical, example of the automaton can be used for further examination. Alternatively, one may think of it as choosing at random a single automaton from a collection of automata in an ensemble differing only by their initial state. The task then is to find out which was the initial state of the chosen automaton.

The logico-algebraic structure of the state identification problem has been introduced in [59], and subsequently studied in [59, 60, 61, 62, 63, 64, 65, 19]. We shall deal with it next.

Step 1: Computation of the experimental equivalence classes.

In the propositional structure of sequential machines, state partitions play an important rôle. Indeed, the set of states is partitioned into equivalence classes with respect to a particular input-output experiment.

Suppose again that the only unknown feature of an automaton is its initial state; all else is known. The automaton is presented in a black box, with input and output interfaces. The task in this *complementary game* is to find (partial) information about the initial state of the automaton [18].

To illustrate this, consider the Mealy automaton M_s discussed above. Input/output experiments can be performed by the input of just one symbol

i (in this example, more inputs yield no finer partitions). Suppose again that Bob does not know the automaton's initial state. So, Bob has to choose between the input of symbols 1,2, or 3. If Bob inputs, say, symbol 1, then he obtains a definite answer whether the automaton was in state 1 — corresponding to output 1; or whether the automaton was not in state 1 — corresponding to output 0. The latter proposition "not 1" can be identified with the proposition that the automaton was either in state 2 or in state 3.

Likewise, if Bob inputs symbol 2, he obtains a definite answer whether the automaton was in state 2 — corresponding to output 1; or whether the automaton was not in state 2 — corresponding to output 0. The latter proposition "not 2" can be identified with the proposition that the automaton was either in state 1 or in state 3. Finally, if Bob inputs symbol 3, he obtains a definite answer whether the automaton was in state 3 — corresponding to output 1; or whether the automaton was not in state 3 — corresponding to output 0. The latter proposition "not 3" can be identified with the proposition that the automaton was either in state 1 or in state 2.

Recall that Bob can actually perform only one of these input-output experiments. This experiment will irreversibly destroy the initial automaton state (with the exception of a "hit"; i.e., of output 1). Let us thus describe the three possible types of experiment as follows.

- Bob inputs the symbol 1.
- Bob inputs the symbol 2.
- Bob inputs the symbol 3.

The corresponding observable propositions are:

$p_{\{1\}} \equiv \{1\}$: On input 1, Bob receives the output symbol 1.

$p_{\{2,3\}} \equiv \{2,3\}$: On input 1, Bob receives the output symbol 0.

$p_{\{2\}} \equiv \{2\}$: On input 2, Bob receives the output symbol 1.

$p_{\{1,3\}} \equiv \{1,3\}$: On input 2, Bob receives the output symbol 0.

$p_{\{3\}} \equiv \{3\}$: On input 3, Bob receives the output symbol 1.

$p_{\{1,2\}} \equiv \{1,2\}$: On input 3, Bob receives the output symbol 0.

Note that, in particular, $p_{\{1\}}, p_{\{2\}}, p_{\{3\}}$ are not comeasurable. Note also that, for $\epsilon_{ijk} \neq 0$, $p'_{\{i\}} = p_{\{j,k\}}$ and $p_{\{j,k\}} = p'_{\{i\}}$; or equivalently $\{i\}' = \{j,k\}$ and $\{j,k\} = \{i\}'$.

In that way, we naturally arrive at the notion of a *partitioning* of automaton states according to the information obtained from input/output experiments. Every element of the partition stands for the proposition that the automaton is in (one of) the state(s) contained in that partition. Every partition corresponds to a quasi-classical Boolean block. Let us denote by $v(x)$ the block corresponding to input (sequence) x. Then we obtain

no input:

$$v(\emptyset) = \{\{1, 2, 3\}\},$$

one input symbol:

input		output 1		output 0
$v(1)$	$=$	$\{\{1\}$	,	$\{2, 3\}\}$
$v(2)$	$=$	$\{\{2\}$	,	$\{1, 3\}\}$
$v(3)$	$=$	$\{\{3\}$	,	$\{1, 2\}\}.$

Conventionally, only the finest partitions are included into the set of state partitions.

Step 2: Pasting of the partitions.

Just as in quantum logic, the *automaton propositional calculus* and the associated *partition logic* is the *pasting* of all the blocks of partitions $v(i)$ on the atomic level. That is, elements of two blocks are identified if and only if the corresponding atoms are identical.

The automaton partition logic based on *atomic* pastings differs from previous approaches [59, 60, 61, 62, 63, 64, 65, 19]. Atomic pasting guarantees that there is no mixing of elements belonging to two different order levels. Such confusions can give rise to the nontransitivity of the order relation [59] in cases where both $p \to q$ and $q \to r$ are operational but incompatible, i.e., complementary, and hence $p \to r$ is not operational.

For the Mealy automaton M_s discussed above, the pasting renders just the horizontal sum — only the least and greatest elements $0, 1$ of each 2^2 is identified—and one obtains a "Chinese lantern" lattice MO_3. The Hasse diagram of the propositional calculus is drawn in Figure 1.

Let us give a formal definition for the procedures sketched so far. Assume a set S and a family of partitions $\mathcal{B}$ of S. Every partition $E \in \mathcal{B}$ can be identified with a Boolean algebra B_E in a natural way by identifying the elements of the partition with the atoms of the Boolean algebra. The pasting

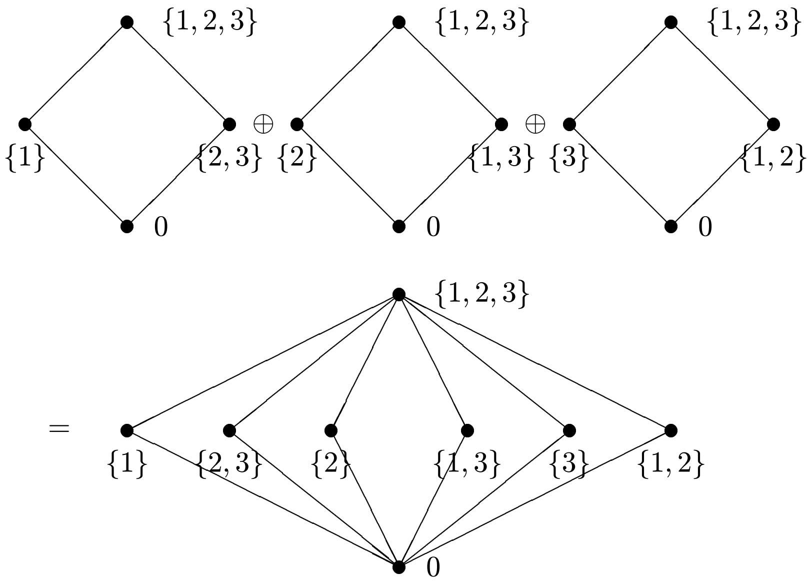

Figure 1: Hasse diagram of the propositional calculus of the Mealy automaton.

of the Boolean algebras $B_E, E \in \mathcal{B}$ on the atomic level is called a partition logic, denoted by $(S, \mathcal{B})$.

The logical structure of the complementarity game (initial-state identification problem) can be defined as follows. Let us call a proposition concerning the initial state of the machine *experimentally decidable* if there is an experiment E which determines the truth value of that proposition. This can be done by performing E, i.e., by the input of a sequence of input symbols $i_1, i_2, i_3, \ldots, i_n$ associated with E, and by observing the output sequence

$$\lambda_E(s) = \lambda(s, i_1), \lambda(\delta(s, i_1), i_2), \ldots, \lambda(\underbrace{\delta(\cdots\delta(s, i_1)\cdots, i_{n-1})}_{n-1 \text{ times}}, i_n).$$

The most general form of a prediction concerning the initial state s of the machine is that the initial state s is contained in a subset P of the state set S. Therefore, we may identify propositions concerning the initial state with subsets of S. A subset P of S is then identified with the proposition that the initial state is contained in P.

Let E be an experiment (a preset or adaptive one), and let $\lambda_E(s)$ denote the obtained output of an initial state s. λ_E defines a mapping of S to the set of output sequences O^*. We define an equivalence relation on the state set S by

$$s \overset{E}{\equiv} t \text{ if and only if } \lambda_E(s) = \lambda_E(t)$$

for any $s, t \in S$. We denote the partition of S corresponding to $\overset{E}{\equiv}$ by $S/\overset{E}{\equiv}$. Obviously, the propositions decidable by the experiment E are the elements of the Boolean algebra generated by $S/\overset{E}{\equiv}$, denoted by B_E.

There is also another way to construct the experimentally decidable propositions of an experiment E. Let $\lambda_E(P) = \bigcup_{s \in P} \lambda_E(s)$ be the direct image of P under λ_E for any $P \subseteq S$. We denote the direct image of S by O_E; i.e., $O_E = \lambda_E(S)$.

It follows that the most general form of a prediction concerning the outcome W of the experiment E is that W lies in a subset of O_E. Therefore, the experimentally decidable propositions consist of all inverse images $\lambda_E^{-1}(Q)$ of subsets Q of O_E, a procedure which can be constructively formulated (e.g., as an effectively computable algorithm), and which also leads to the Boolean algebra B_E.

Let $\mathcal{B}$ be the set of all Boolean algebras B_E. We call the partition logic $R = (S, \mathcal{B})$ an *automaton propositional calculus.*

Appendix C: Quantum coding

In the usual Hilbert space formulization, qubits can then be written as

$$\#(x_\alpha) = e^{i\varphi}(\sin\omega, e^{i\delta}\cos\omega) \in \mathbf{C}^2, \tag{2}$$

with $\alpha = \alpha(\omega, \varphi, \delta)$, $\omega, \varphi, \delta \in \mathbf{R}$ Qubits can be identified with cbits as follows

$$\#(x_{\alpha(\pi/2,\varphi,\delta)}) = (a, 0) \equiv 1 \text{ and } \#(x_{\alpha(0,\varphi,\delta)}) = (0, b) \equiv 0 \quad , \qquad |a|, |b| = 1 \quad , \tag{3}$$

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 qubit is not in a pure classical state. Therefore, any practical determination of the qubit x_α amounts to a measurement of the state amplitude of t or f. According to the quantum postulates, any such *single* measurement will be indeterministic (provided again that $\alpha, \beta \neq 0$). That is, the outcome of a single measurement occurs unpredictably. The probabilities that the qubit x_α is measured in states

t and f are $P_t(x_\alpha) = |(x_\alpha, t)|^2$ and $P_f(x_\alpha) = |(x_\alpha, f)|^2 = 1 - P_t(_{\alpha,\beta})$, respectively.

Appendix D: Universal manipulation of a single qubit: the $U(2)$-gate

It is well known that any n-dimensional unitary matrix U can be composed from elementary unitary transformations in two-dimensional subspaces of $\mathbf{C}^n$. This is usually shown in the context of parameterization of the n-dimensional unitary groups (cf. [25, chapter 2] and [52, 66]). 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 qubits 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.*

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

In what follows, a lossless *Mach-Zehnder* interferometer drawn in Fig. 2 is discussed. The computation proceeds by successive substitution (transition) of states; i.e.,

$$\begin{array}{rcll} S_1: a & \rightarrow & (b+ic)/\sqrt{2} & , \qquad (4) \\ P: b & \rightarrow & be^{i\varphi} & , \qquad (5) \\ S_2: b & \rightarrow & (e+id)/\sqrt{2} & , \qquad (6) \\ S_2: c & \rightarrow & (d+ie)/\sqrt{2} & . \qquad (7) \end{array}$$

The resulting transition is

$$a \rightarrow \psi = i\left(\frac{e^{i\varphi}+1}{2}\right)d + \left(\frac{e^{i\varphi}-1}{2}\right)e \quad . \qquad (8)$$

Assume that $\varphi = 0$, i.e., there is no phase shift at all. Then, equation (8) reduces to $a \rightarrow id$, and the emitted quant is detected only by D_1. Assume

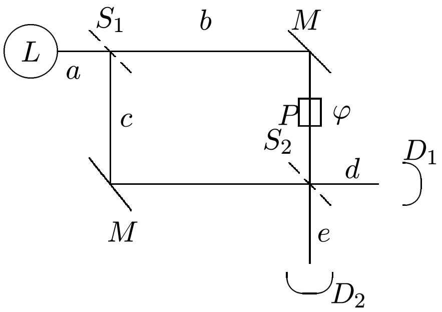

Figure 2: Mach-Zehnder interferometer. A single quantum (photon, neutron, electron *etc*) is emitted in L and meets a lossless beam splitter (half-silvered mirror) S_1, after which its wave function is in a coherent superposition of b and c. In beam path b a phase shifter shifts the phase of state b 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.

that $\varphi = \pi$. Then, equation (8) 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:

$$P_{D_1}(\varphi) = |(d,\psi)|^2 = \cos^2(\frac{\varphi}{2}) \quad , \quad P_{D_2}(\varphi) = |(e,\psi)|^2 = \sin^2(\frac{\varphi}{2}) \quad . \tag{9}$$

For some “mindboggling” features of Mach-Zehnder interferometry, see [67].

The elementary quantum interference device $\mathbf{T}_{21}^{bs}$ depicted in Fig. (3.a) is just a beam splitter followed by a phase shifter in one of the output ports.

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 [68, 69].

$$P_1 : \mathbf{0} \quad \rightarrow \quad \mathbf{0}e^{i\alpha+\beta} \quad , \tag{10}$$

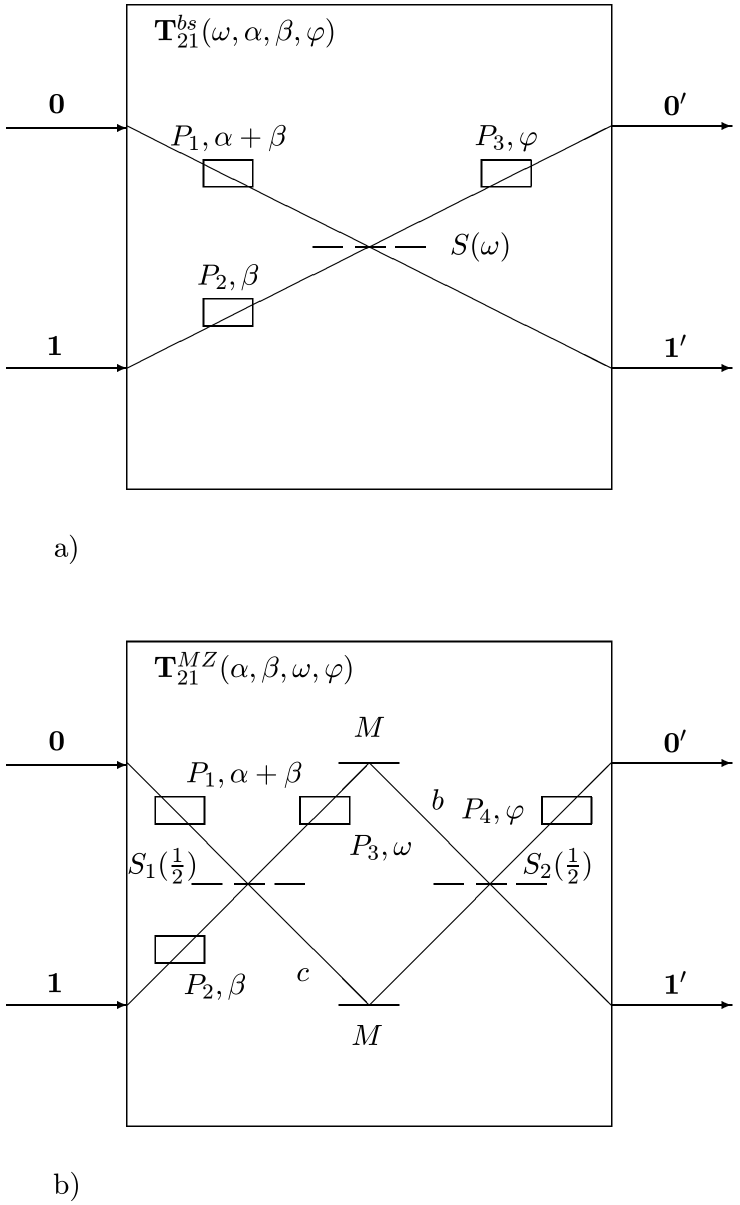

Figure 3: Elementary quantum interference device. An elementary quantum interference device can be realized by a 4-port interferometer with two input ports $\mathbf{0}, \mathbf{1}$ and two output ports $\mathbf{0'}, \mathbf{1'}$. Any two-dimensional unitary transformation can be realized by the devices. 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.

$$\begin{aligned}
P_2:\ \mathbf{1} &\rightarrow \mathbf{1}e^{i\beta} \quad , && (11)\\
S:\ \mathbf{0} &\rightarrow T\,\mathbf{1}' + iR\,\mathbf{0}' \quad , && (12)\\
S:\ \mathbf{1} &\rightarrow T\,\mathbf{0}' + iR\,\mathbf{1}' \quad , && (13)\\
P_3:\ \mathbf{0}' &\rightarrow \mathbf{0}'e^{i\varphi} \quad . && (14)
\end{aligned}$$

If $\mathbf{0} \equiv \mathbf{0}' \equiv \left(\begin{array}{c} 1 \\ 0 \end{array}\right)$ and $\mathbf{1} \equiv \mathbf{1}' \equiv \left(\begin{array}{c} 0 \\ 1 \end{array}\right)$ 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

$$\begin{aligned}
\mathbf{T}_{21}^{bs}(\omega,\alpha,\beta,\varphi) &= \left[e^{i\,\beta} \left(\begin{array}{cc} i\,e^{i(\alpha+\varphi)}\,\sin\omega & e^{i\alpha}\,\cos\omega \\ e^{i\varphi}\,\cos\omega & i\,\sin\omega \end{array}\right)\right]^{-1} \\
&= e^{-i\,\beta} \left(\begin{array}{cc} -i\,e^{-i(\alpha+\varphi)}\,\sin\omega & e^{-i\varphi}\,\cos\omega \\ e^{-i\alpha}\,\cos\omega & -i\,\sin\omega \end{array}\right) \quad . \qquad (15)
\end{aligned}$$

The elementary quantum interference device $\mathbf{T}_{21}^{MZ}$ depicted in Fig. (3.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

$$\begin{aligned}
P_1:\ \mathbf{0} &\rightarrow \mathbf{0}e^{i\alpha+\beta} \quad , && (16)\\
P_2:\ \mathbf{1} &\rightarrow \mathbf{1}e^{i\beta} \quad , && (17)\\
S_1:\ \mathbf{1} &\rightarrow (b+i\,c)/\sqrt{2} \quad , && (18)\\
S_1:\ \mathbf{0} &\rightarrow (c+i\,b)/\sqrt{2} \quad , && (19)\\
P_3:\ c &\rightarrow ce^{i\omega} \quad , && (20)\\
S_2:\ b &\rightarrow (\mathbf{1}'+i\,\mathbf{0}')/\sqrt{2} \quad , && (21)\\
S_2:\ c &\rightarrow (\mathbf{0}'+i\,\mathbf{1}')/\sqrt{2} \quad , && (22)\\
P_4:\ \mathbf{0}' &\rightarrow \mathbf{0}'e^{i\varphi} \quad . && (23)
\end{aligned}$$

When again $\mathbf{0} \equiv \mathbf{0}' \equiv \left(\begin{array}{c} 1 \\ 0 \end{array}\right)$ and $\mathbf{1} \equiv \mathbf{1}' \equiv \left(\begin{array}{c} 0 \\ 1 \end{array}\right)$, 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

$$\mathbf{T}_{21}^{MZ}(\alpha,\beta,\omega,\varphi) = -i\,e^{-i(\beta+\frac{\omega}{2})} \left(\begin{array}{cc} -e^{-i\,(\alpha+\varphi)}\,\sin\frac{\omega}{2} & e^{-i\,\varphi}\,\cos\frac{\omega}{2} \\ e^{-i\,\alpha}\,\cos\frac{\omega}{2} & \sin\frac{\omega}{2} \end{array}\right) \quad . \qquad (24)$$

The correspondence between $\mathbf{T}^{bs}_{21}(T(\omega),\alpha,\beta,\varphi)$ with $\mathbf{T}^{MZ}_{21}(\alpha',\beta',\omega',\varphi')$ in equations (15) (24) 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.,

$$\mathbf{T}^{bs}_{21}(\omega,\alpha,\beta,\varphi)=\mathbf{T}^{MZ}_{21}(\alpha-\frac{\pi}{2},\beta-\omega,2\omega,\varphi-\frac{\pi}{2}) \quad . \tag{25}$$

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 $\mathbf{T}^{bs}_{21}$ and $\mathbf{T}^{MZ}_{21}$; 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 (15) (24) 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 $SU(2)$ [25]

$$\mathbf{T}(\omega,\alpha,\varphi)=\left(\begin{array}{cc} e^{i\,\alpha}\,\cos\omega & -e^{-i\,\varphi}\,\sin\omega \\ e^{i\,\varphi}\,\sin\omega & e^{-i\,\alpha}\,\cos\omega \end{array}\right) \quad , \tag{26}$$

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

$$\mathbf{T}(\omega,\alpha,\beta,\varphi)=e^{-i\,\beta}\mathbf{T}(\omega,\alpha,\varphi) \quad . \tag{27}$$

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

$$\mathbf{T}(\omega,\alpha,\beta,\varphi)=\mathbf{T}^{bs}_{21}(\omega-\frac{\pi}{2},-\alpha-\varphi-\frac{\pi}{2},\beta+\alpha+\frac{\pi}{2},\varphi-\alpha+\frac{\pi}{2}) \quad . \tag{28}$$

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

$$\mathbf{I}=T^{bs}_{21}(-\frac{\pi}{2},-\frac{\pi}{2},\frac{\pi}{2},\frac{\pi}{2})=T^{MZ}_{21}(-\pi,\pi,-\pi,0)=\left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array}\right) \quad . \tag{29}$$

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

$$\texttt{not}=T^{bs}_{21}(0,0,0,0)=T^{MZ}_{21}(-\frac{\pi}{2},0,0,-\frac{\pi}{2})=\left(\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array}\right) \quad . \tag{30}$$

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 $\mathbf{0} \rightarrow \mathbf{0}+\mathbf{1}$, $\mathbf{1} \rightarrow -\mathbf{0}+\mathbf{1}$ and can be realized by

$$\sqrt{\texttt{not}} = T_{21}^{bs}(-\frac{\pi}{4},-\frac{\pi}{2},\frac{\pi}{2},\frac{\pi}{2}) = T_{21}^{MZ}(-\pi,\frac{3\pi}{4},-\frac{\pi}{2},0) = \frac{1}{\sqrt{2}}\left(\begin{array}{cc} 1 & -1 \\ 1 & 1 \end{array}\right) \quad . \tag{31}$$

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

$$\sqrt{\texttt{not}}' = T_{21}^{bs}(-\frac{\pi}{4},0,\frac{\pi}{4},0) = T_{21}^{MZ}(-\frac{\pi}{2},\frac{\pi}{2},-\frac{\pi}{2},-\frac{\pi}{2}) = \frac{1}{2}\left(\begin{array}{cc} 1+i & 1-i \\ 1-i & 1+i \end{array}\right) \quad . \tag{32}$$

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] Cristian Calude and F. Walter Meyerstein. Is the universe lawful? *Chaos, Solitons & Fractals*, 10(6):1075–1084, 1999.

[2] Karl Svozil. Quantum interfaces. e-print `arXiv:quant-ph/0001064` available http://arxiv.org/abs/quant-ph/0001064, 2000.

[3] John A. Wheeler. Law without law. In John A. Wheeler and W. H. Zurek, editors, *Quantum Theory and Measurement*, pages 182–213. Princeton University Press, Princeton, 1983. [48].

[4] Daniel M. Greenberger. Private communication.

[5] David Hilbert. Über das Unendliche. *Mathematische Annalen*, 95:161–190, 1926.

[6] Erwin Schrödinger. Die gegenwärtige Situation in der Quantenmechanik. *Naturwissenschaften*, 23:807–812, 823–828, 844–849, 1935. English translation in [70] and [48, pp. 152-167].

[7] Simon Kochen and Ernst P. Specker. The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics*, 17(1):59–87, 1967. Reprinted in [71, pp. 235–263].

[8] W. K. Wooters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[9] D. Dieks. Communication by EPR devices. *Physics Letters*, 92A(6):271–272, 1982.

[10] L. Mandel. Is a photon amplifier always polarization dependent? *Nature*, 304:188, 1983.

[11] Peter W. Milonni and M. L. Hardies. Photons cannot always be replicated. *Physics Letters*, 92A(7):321–322, 1982.

[12] R. J. Glauber. Amplifiers, attenuators and the quantum theory of measurement. In E. R. Pikes and S. Sarkar, editors, *Frontiers in Quantum Optics*. Adam Hilger, Bristol, 1986.

[13] C. M. Caves. Quantum limits on noise in linear amplifiers. *Physical Review*, D26:1817–1839, 1982.

[14] Simon Kochen and Ernst P. Specker. Logical structures arising in quantum theory. In *Symposium on the Theory of Models, Proceedings of the 1963 International Symposium at Berkeley*, pages 177–189, Amsterdam, 1965. North Holland. Reprinted in [71, pp. 209–221].

[15] Simon Kochen and Ernst P. Specker. The calculus of partial propositional functions. In *Proceedings of the 1964 International Congress for Logic, Methodology and Philosophy of Science, Jerusalem*, pages 45–57, Amsterdam, 1965. North Holland. Reprinted in [71, pp. 222–234].

[16] Garrett Birkhoff and John von Neumann. The logic of quantum mechanics. *Annals of Mathematics*, 37(4):823–843, 1936.

[17] Charles H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5:3–28, 1992.

[18] Edward F. Moore. Gedanken-experiments on sequential machines. In C. E. Shannon and J. McCarthy, editors, *Automata Studies*. Princeton University Press, Princeton, 1956.

[19] Cristian Calude, Elena Calude, Karl Svozil, and Sheng Yu. Physical versus computational complementarity I. *International Journal of Theoretical Physics*, 36(7):1495–1523, 1997.

[20] K. Svozil. *Quantum Logic.* Springer, Singapore, 1998.

[21] Artur Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67:661–663, 1991.

[22] M. Hamrick G. Gilbert. Practical quantum cryptography: A comprehensive analysis (part one). MITRE report MTR 00W0000052 and e-print `arXiv:quant-ph/0009027` available at `http://arxiv.org/abs/quant-ph/0009027`, 2000.

[23] T. Jenewein, G. Weihs, C. Simon, H. Weinfurter, and A. Zeilinger. Poster, 1998.

[24] Karl Svozil. The information interpretation of quantum mechanics. e-print `arXiv:quant-ph/0006033` available http://arxiv.org/abs/quant-ph/0006033, 2000.

[25] F. D. Murnaghan. *The Unitary and Rotation Groups.* Spartan Books, Washington, 1962.

[26] Peter W. Shor. 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*. IEEE Computer Society Press, November 1994. `arXiv:quant-ph/9508027`.

[27] Artur Ekert and Richard Jozsa. Quantum computation and Shor's factoring algorithm. *Reviews of Modern Physics*, 68(3):733–753, 1996.

[28] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, pages 212–219. 1996.

[29] Josef Gruska. *uantum Computing.* McGraw-Hill, London, 1999.

[30] Georg Gottlob. Private communication.

[31] Cristian S. Calude, Michael J. Dinneen, and Karl Svozil. Reflections on quantum computing. *Complexity*, 2000. in print;
e-print `http://www.cs.auckland.ac.nz/CDMTCS//researchreports/130cris.pdf`.

[32] Max Planck. Ueber eine Verbesserung der Wien'schen Spectralgleichung. *Verhandlungen der deutschen physikalischen Gesellschaft*, 2:202, 1900. See also [33].

[33] Max Planck. Ueber das Gesetz der Energieverteilung im Normalspectrum. *Annalen der Physik*, 4:553–566, 1901.

[34] Max Planck. Zur Theorie des Gesetzes der Energieverteilung im Normalspectrum. *Verhandlungen der deutschen physikalischen Gesellschaft*, 2:237, 1900. See also [33].

[35] Albert Einstein. Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt. *Annalen der Physik*, 17:132–148, 1905.

[36] Richard P. Feynman, Robert B. Leighton, and Matthew Sands. *The Feynman Lectures on Physics. Quantum Mechanics*, volume III. Addison-Wesley, Reading, MA, 1965.

[37] E. G. Harris. *A Pedestrian Approach to Quantum Field Theory.* Wiley-Interscience, New York, 1971.

[38] H. J. Lipkin. *Quantum Mechanics, New Approaches to Selected Topics.* North-Holland, Amsterdam, 1973.

[39] L. E. Ballentine. *Quantum Mechanics.* Prentice Hall, Englewood Cliffs, NJ, 1989.

[40] A. Messiah. *Quantum Mechanics*, volume I. North-Holland, Amsterdam, 1961.

[41] A. S. Davydov. *Quantum Mechanics.* Addison-Wesley, Reading, MA, 1965.

[42] P. A. M. Dirac. *The Principles of Quantum Mechanics.* Oxford University Press, Oxford, 1947.

[43] Asher Peres. *Quantum Theory: Concepts and Methods.* Kluwer Academic Publishers, Dordrecht, 1993.

[44] George W. Mackey. *The Mathematical Foundations of Quantum Mechanics.* W. A. Benjamin, Reading, MA, 1963.

[45] John von Neumann. *Mathematische Grundlagen der Quantenmechanik.* Springer, Berlin, 1932. English translation: *Mathematical Foundations of Quantum Mechanics*, Princeton University Press, Princeton, 1955.

[46] John S. Bell. *Speakable and Unspeakable in Quantum Mechanics.* Cambridge University Press, Cambridge, 1987.

[47] Max Jammer. *The Philosophy of Quantum Mechanics.* John Wiley & Sons, New York, 1974.

[48] John Archibald Wheeler and Wojciech Hubert Zurek. *Quantum Theory and Measurement.* Princeton University Press, Princeton, 1983.

[49] N. Dunford and J. T. Schwartz. *Linear Operators I.* Interscience Publishers, New York, 1958.

[50] Michael Reed and Barry Simon. *Methods of Mathematical Physics I: Functional Analysis.* Academic Press, New York, 1972.

[51] Michael Reed and Barry Simon. *Methods of Mathematical Physics II: Fourier Analysis, Self-Adjointness.* Academic Press, New York, 1975.

[52] M. Reck, Anton Zeilinger, H. J. Bernstein, and P. Bertani. Experimental realization of any discrete unitary operator. *Physical Review Letters*, 73:58–61, 1994. See also [25].

[53] Daniel B. Greenberger and A. YaSin. “Haunted” measurements in quantum theory. *Foundation of Physics*, 19(6):679–704, 1989.

[54] Thomas J. Herzog, Paul G. Kwiat, Harald Weinfurter, and Anton Zeilinger. Complementarity and the quantum eraser. *Physical Review Letters*, 75(17):3034–3037, 1995.

[55] David Finkelstein and Shlomit R. Finkelstein. Computational complementarity. *International Journal of Theoretical Physics*, 22(8):753–779, 1983.

[56] Gregory J. Chaitin. An improvement on a theorem by E. F. Moore. *IEEE Transactions on Electronic Computers*, EC-14:466–467, 1965.

[57] J. H. Conway. *Regular Algebra and Finite Machines.* Chapman and Hall Ltd., London, 1971.

[58] W. Brauer. *Automatentheorie.* Teubner, Stuttgart, 1984.

[59] Karl Svozil. *Randomness & Undecidability in Physics.* World Scientific, Singapore, 1993.

[60] Martin Schaller and Karl Svozil. Partition logics of automata. *Il Nuovo Cimento*, 109B:167–176, 1994.

[61] Martin Schaller and Karl Svozil. Automaton partition logic versus quantum logic. *International Journal of Theoretical Physics*, 34(8):1741–1750, August 1995.

[62] Martin Schaller and Karl Svozil. Automaton logic. *International Journal of Theoretical Physics*, 35(5):911–940, May 1996.

[63] Anatolij Dvurečenskij, Sylvia Pulmannová, and Karl Svozil. Partition logics, orthoalgebras and automata. *Helvetica Physica Acta*, 68:407–428, 1995.

[64] Karl Svozil and Roman R. Zapatrin. Empirical logic of finite automata: microstatements versus macrostatements. *International Journal of Theoretical Physics*, 35(7):1541–1548, 1996.

[65] Karl Svozil and Josef Tkadlec. Greechie diagrams, nonexistence of measures in quantum logics and Kochen–Specker type constructions. *Journal of Mathematical Physics*, 37(11):5380–5401, November 1996.

[66] M. Reck and Anton Zeilinger. Quantum phase tracing of correlated photons in optical multiports. In F. De Martini, G. Denardo, and Anton Zeilinger, editors, *Quantum Interferometry*, Singapore, 1994. World Scientific.

[67] Charles H. Bennett. Night thoughts, dark sight. *Nature*, 371:479–480, 1994.

[68] B. Yurke, S. L. McCall, and J. R. Klauder. SU(2) and SU(1,1) interferometers. *Physical Review*, A33:4033–4054, 1986.

[69] R. A. Campos, B. E. A. Saleh, and M. C. Teich. Fourth-order interference of joint single-photon wave packets in lossless optical systems. *Physical Review*, A42:4127, 1990.

[70] J. D. Trimmer. The present situation in quantum mechanics: a translation of Schrödinger's "cat paradox". *Proc. Am. Phil. Soc.*, 124:323–338, 1980. Reprinted in [48, pp. 152-167].

[71] Ernst Specker. *Selecta*. Birkhäuser Verlag, Basel, 1990.