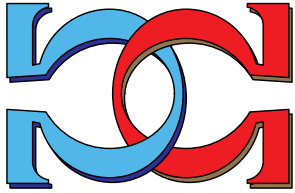


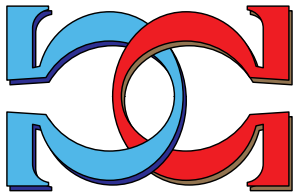
CDMTCS



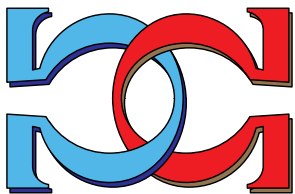
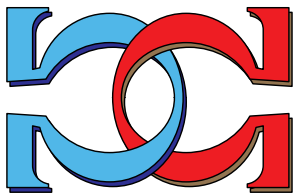
Research

Report

Series

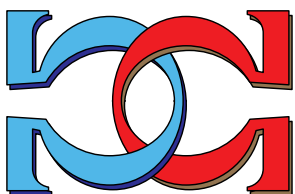


**The diagonalization method in
quantum recursion theory**



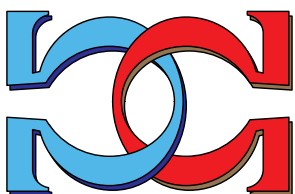
Karl Svozil

Vienna University of Technology



CDMTCS-361

April 2009



Centre for Discrete Mathematics and
Theoretical Computer Science

The diagonalization method in quantum recursion theory

Karl Svozil*

*Institute for Theoretical Physics, Vienna University of Technology,
Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria*

Abstract

As quantum parallelism allows the effective co-representation of classical mutually exclusive states, the diagonalization method of classical recursion theory has to be modified. Quantum diagonalization involves unitary operators whose eigenvalues are different from one.

PACS numbers: 03.67.Hk, 03.65.Ud

Keywords: Quantum information, quantum recursion theory, halting problem

INTRODUCTION

The reasoning in formal logic and the theory of recursive functions and effective computability [1–6], at least insofar as their applicability to worldly things is concerned [7], makes implicit assumptions about the physical meaningfulness of the entities of discourse; e.g., their actual physical representability and operationalizability [8]. It is this isomorphism or correspondence between the phenomena and theory and *vice versa* — postulated by the Church-Turing thesis [9] — which confers power to the formal methods. Therefore, any finding in physics presents a challenge to the formal sciences; at least insofar as they claim to be relevant to the physical universe, although history shows that the basic postulates have to be re-considered very rarely.

For example, the fundamental atom of classical information, the bit, is usually assumed to be in one of two possible mutually exclusive states, which can be represented by two distinct states of a classical physical system. These issues have been extensively discussed in the context of energy dissipation associated with certain logical operations and universal (ir)reversible computation [10–13].

In general, all varieties of physical states, as well as their evolution and transformations, are relevant for propositional logic as well as for a generalized theory of information. Quantum logic [14], partial algebras [15, 16], empirical logic [17, 18] and continuous time computations [19] are endeavors in this direction. These states need not necessarily be mapped into or bounded by classical information. Likewise, physical transformations and manipulations available, for instance, in quantum information and classical continuum theory, may differ from the classical paper-and-pencil operations modeled by universal Turing machines. Hence, the computational methods available as “elementary operations” have to be adapted to cope with the additional physical capabilities [20].

Indeed, in what follows it is argued that, as quantum theory offers nonclassical states and operators available in quantum information theory, several long-held assumptions on the character and transformation of classical information have to be adapted. As a consequence, the formal techniques in manipulating information in the theory of recursive functions and effective computability have to be revised. Particular emphasis is given to undecidability and the diagonalization method.

QUANTUM INFORMATION THEORY

As several fine presentations of quantum information and computation theory exist (cf. Refs. [21–29] for a few of them), there is no need of an extended exposition. In what follows, we shall mainly follow Mermin’s notation [29, 30]. For the representation of both a single classical and quantum bit, suppose a two-dimensional Hilbert space. (For physical purposes a linear vector space endowed with a scalar product will be sufficient.) Let the superscript “ T ” indicate transposition, and let $|0\rangle \equiv (1, 0)^T$ and $|1\rangle \equiv (0, 1)^T$ be the orthogonal vector representations of the classical states associated with “falsity” and “truth,” or “0” and “1,” respectively.

From the varieties of properties featured by quantum information, one is of particular importance for quantum recursion theory: the ability to co-represent classically distinct, contradictory states of information *via* the generalized quantum bit state

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \equiv \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}, \quad (1)$$

with the normalization $|\alpha_0|^2 + |\alpha_1|^2 = 1$. This feature is also known as *quantum parallelism*, alluding to the fact that n quantum bits can co-represent 2^n classical mutually exclusive states $\{|i_1 i_2 \cdots i_n\rangle \mid i_j \in \{0, 1\}, j = 1, \dots, n\}$ of n classical bits.

As will be argued below, recursion theoretic diagonalization can be symbolized by the diagonalization or “not” operator $\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, transforming $|0\rangle$ into $|1\rangle$, and *vice versa*. The eigensystem of the diagonalization operator $\mathbf{X}$ is given by the two 50:50 mixtures of $|0\rangle$ and $|1\rangle$ with the two eigenvalues 1 and -1 ; i.e.,

$$\mathbf{X} \frac{1}{\sqrt{2}} (|0\rangle \pm |1\rangle) = \pm \frac{1}{\sqrt{2}} (|0\rangle \pm |1\rangle) = \pm |\psi_{\pm}\rangle. \quad (2)$$

In particular, the state $|\psi_+\rangle$ associated with the eigenvalue $+1$ is a *fixed point* of the operator $\mathbf{X}$.

Note that, provided that $|\psi\rangle \notin \{|0\rangle, |1\rangle\}$, a quantum bit is not in a pure classical state “relative to” the propositions corresponding to the projectors $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$. Any practical determination of the quantum bit amounts to a measurement of the state “along” one context [31] or base, such as the base “spanned” by $\{|0\rangle, |1\rangle\}$. Any such *single* measurement will be indeterministic (provided that the basis does not coincide with $\{|\psi_+\rangle, |\psi_-\rangle\}$); in particular, $|\langle\psi_{\pm}|0\rangle|^2 = |\langle\psi_{\pm}|1\rangle|^2 = 1/2$. That is, if the fixed point state and the measurement context mismatch, by Born’s postulate [32, 33], the outcome of a *single* measurement occurs indeterministically, unpredictably and at random.

Hence, in terms of the quantum states $|0\rangle$ and $|1\rangle$ corresponding to the classical states, the fixed point remains indeterminate.

In what follows it is argued that, due to the superposition principle, the quantum recursion theoretic diagonalization method has to be reformulated as a fixed point argument. Application of the diagonal operator $\mathbf{X}$ yields no *reductio ad absurdum*. Instead, undecidability is recovered as a natural consequence of quantum coherence and of the unpredictability of certain quantum events.

DIAGONALIZATION

For comprehensive reviews of recursion theory and the diagonalization method the reader is referred to Refs. [1–6]. Therefore, only a few hallmarks will be stated. As already pointed out by Gödel in his classical paper on the incompleteness of arithmetic [34], the undecidability theorems of formal logic [2] are based on semantical paradoxes such as the liar [35] or Richard’s paradox. A proper translation of the semantic paradoxes into formal proofs results in the diagonalization method. Diagonalization has apparently first been applied by Cantor to demonstrate the uncountability of real numbers [36]. It has also been used by Turing for a proof of the recursive undecidability of the halting problem [37].

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 classical bits (classical case) and quantum bits (quantum mechanical case).

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

Classical case

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

$$\text{HALT}(B(X)) = \begin{cases} |0\rangle & \text{if } B(X) \uparrow \\ |1\rangle & \text{if } B(X) \downarrow \end{cases} . \quad (3)$$

Then, whenever $A(A)$ halts, $\text{HALT}(A(A))$ outputs $|1\rangle$ and forces $A(A)$ not to halt. Conversely, whenever $A(A)$ does not halt, then $\text{HALT}(A(A))$ outputs $|0\rangle$ 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.

Quantum mechanical case

As has been argued above, in quantum information theory a quantum bit may be in a linear coherent superposition of the two classical states $|0\rangle$ and $|1\rangle$. Due to the superposition of classical bit states, the usual *reductio ad absurdum* argument breaks down. Instead, diagonalization procedures in quantum information theory yield quantum bit 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 quantum bit

$$\text{HALT}(B(X)) = |\psi\rangle . \quad (4)$$

We may think of $\text{HALT}(B(X))$ as a universal computer C' simulating C and containing a dedicated *halting bit*, which is the output of C' at every (discrete) time cycle. Initially (at time zero), this halting bit is prepared to be a 50:50 mixture of the classical halting and non-halting states $|0\rangle$ and $|1\rangle$ with equal phase; i.e., $|\psi_+\rangle$. If later C' finds that C converges (diverges) on $B(X)$, then the halting bit of C' is set to the “classical” values $|1\rangle$ or $|0\rangle$.

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 classical bit states. (Since the quantum bit states are merely a linear coherent superposition

thereof, the action of diagonalization on quantum bits is straightforward.) Diagonalization effectively transforms the classical bit value $|0\rangle$ into $|1\rangle$ and *vice versa*. Recall that in equation (3), the state $|1\rangle$ has been identified with the halting state and the state $|0\rangle$ with the non-halting state.

The evolution representing diagonalization (effectively, agent A 's task) can be expressed by the unitary operator $\mathbf{D}$ as

$$\mathbf{D}|0\rangle = |1\rangle \text{ and } \mathbf{D}|1\rangle = |0\rangle \quad . \quad (5)$$

Thus, $\mathbf{D}$ acts essentially as a not-gate corresponding to the operator $\mathbf{X}$. In the above state basis, $\mathbf{D}$ can be represented by

$$\mathbf{D} = \mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad . \quad (6)$$

$\mathbf{D}$ 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 linear coherent superposition $|\psi\rangle$ of the “classical” bit states $|0\rangle$ and $|1\rangle$. $\mathbf{D}$ has a fixed point at the quantum bit state

$$|\psi_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad . \quad (7)$$

$|\psi_+\rangle$ does not give rise to inconsistencies [38]: If agent A hands over the fixed point state $|\psi_+\rangle$ to the diagonalization operator $\mathbf{D}$, the same state $|\psi_+\rangle$ is recovered. Stated differently, as long as the output of the “halting algorithm” to input $A(A)$ is $|\psi_+\rangle$, i.e., $\text{HALT}(A(A)) = |\psi_+\rangle$, 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 quantum bit. The consequences for quantum recursion theory are discussed below.

CONSEQUENCES FOR QUANTUM RECURSION THEORY

Several critical remarks are in order. It should be noted that the fixed point quantum bit “solution” of the above halting problem 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 $|0\rangle$ and $|1\rangle$. Any single measurement will yield an indeterministic result. There is a 50:50 chance that the fixed point state will be either in $|0\rangle$ or $|1\rangle$, since as has been argued before, $|\langle\psi_+|0\rangle|^2 = |\langle\psi_+|1\rangle|^2 = 1/2$. Thereby, classical undecidability is recovered.

Thus, as far as problem solving is concerned, classical bits are not much of an advance. If a classical information is required, then quantum bits are not better than probabilistic knowledge. With regards to the question of whether or not a computer halts, the “solution” is effectively equivalent to the throwing of a fair coin [39]. 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.

The above argument used the continuity of quantum bit states as compared to the two discrete classical bit states for a construction of fixed points of the diagonalization operator. One could proceed a step further and allow *nonclassical diagonalization procedures*. Thereby, one could extend diagonalization to the entire range of two-dimensional unitary transformations [40], which need not have fixed points corresponding to eigenvalues of exactly one. Note that the general diagonal form of finite-dimensional unitary transformations in matrix notation is $\text{diag}(e^{i\varphi_1}, e^{i\varphi_2}, \dots, e^{i\varphi_n})$; i.e., the eigenvalues of a unitary operator are complex numbers of unit modulus (e.g., Ref. [41, p. 39], or Ref. [42, p. 161]). Fixed points only occur if at least one of the phases φ_i , $i \in \{1, 2, \dots, n\}$ is a multiple of 2π . In what follows, we shall study the physical realizability of general unitary operators associated with generalized beam splitters [43–46]. We will be particularly interested in those transformations whose spectra do not contain the eigenvalue one and thus do not allow a fixed point eigenvector.

In what follows, lossless devices will be considered. In order to be able to realize a universal unitary transformation in two-dimensional Hilbert space, one needs to consider gates with two input and two output ports representing beam splitters and Mach-Zehnder interferometers equipped with an appropriate number of phase shifters. For the sake of demonstration, consider the two realizations depicted in Fig. 1. The elementary quantum interference device $\mathbf{T}^{bs}$ in Fig. 1a) is a unit consisting of two phase shifters P_1 and P_2 in the input ports, followed by a beam splitter S , which is followed by a phase shifter P_3 in one of the output ports. The device can be quantum

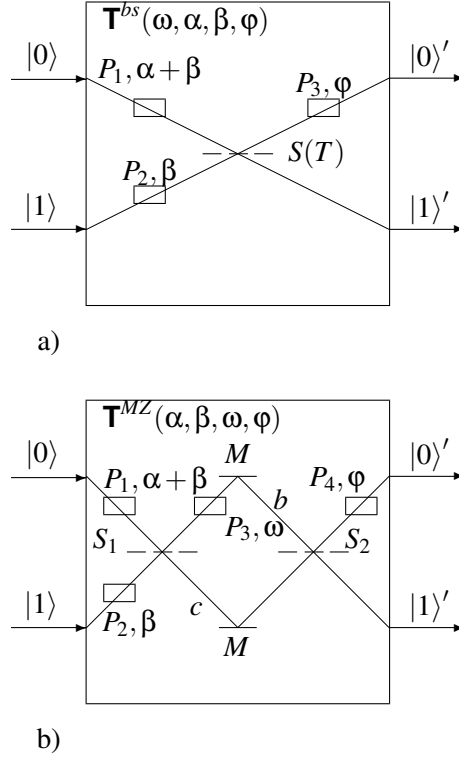


FIG. 1: A universal quantum interference device operating on a qubit can be realized by a 4-port interferometer with two input ports $|0\rangle, |1\rangle$ and two output ports $|0'\rangle, |1'\rangle$; a) realization by a single beam splitter $S(T)$ with variable transmission T and three phase shifters P_1, P_2, P_3 ; b) realization by two 50:50 beam splitters S_1 and S_2 and four phase shifters P_1, P_2, P_3, P_4 .

mechanically represented by [47]

$$\begin{aligned}
 P_1 : |0\rangle &\rightarrow |0\rangle e^{i(\alpha+\beta)}, \\
 P_2 : |1\rangle &\rightarrow |1\rangle e^{i\beta}, \\
 S : |0\rangle &\rightarrow \sqrt{T} |1'\rangle + i\sqrt{R} |0'\rangle, \\
 S : |1\rangle &\rightarrow \sqrt{T} |0'\rangle + i\sqrt{R} |1'\rangle, \\
 P_3 : |0'\rangle &\rightarrow |0'\rangle e^{i\varphi},
 \end{aligned} \tag{8}$$

where every reflection by a beam splitter S contributes a phase $\pi/2$ and thus a factor of $e^{i\pi/2} = i$ to the state evolution. Transmitted beams remain unchanged; i.e., there are no phase changes. Global phase shifts from mirror reflections are omitted. With $\sqrt{T(\omega)} = \cos \omega$ and $\sqrt{R(\omega)} = \sin \omega$, the

corresponding unitary evolution matrix is given by

$$\mathbf{T}^{bs}(\omega, \alpha, \beta, \varphi) = \begin{pmatrix} i e^{i(\alpha+\beta+\varphi)} \sin \omega & e^{i(\beta+\varphi)} \cos \omega \\ e^{i(\alpha+\beta)} \cos \omega & i e^{i\beta} \sin \omega \end{pmatrix}. \quad (9)$$

Alternatively, the action of a lossless beam splitter may be described by the matrix [54]

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

A phase shifter in two-dimensional Hilbert space is represented by either $\text{diag}(e^{i\varphi}, 1)$ or $\text{diag}(1, e^{i\varphi})$. 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 [48, 49]; i.e.,

$$\mathbf{T}^{bs}(\omega, \alpha, \beta, \varphi) = \begin{pmatrix} e^{i\varphi} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} i \sin \omega & \cos \omega \\ \cos \omega & i \sin \omega \end{pmatrix} \begin{pmatrix} e^{i(\alpha+\beta)} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\beta} \end{pmatrix}. \quad (10)$$

The elementary quantum interference device $\mathbf{T}^{MZ}$ depicted in Fig. 1b) is a Mach-Zehnder interferometer with two input and output ports and four phase shifters. The process can be quantum mechanically described by

$$\begin{aligned} P_1 : |0\rangle &\rightarrow |0\rangle e^{i(\alpha+\beta)}, \\ P_2 : |1\rangle &\rightarrow |1\rangle e^{i\beta}, \\ S_1 : |1\rangle &\rightarrow (|b\rangle + i|c\rangle)/\sqrt{2}, \\ S_1 : |0\rangle &\rightarrow (|c\rangle + i|b\rangle)/\sqrt{2}, \\ P_3 : |b\rangle &\rightarrow |b\rangle e^{i\omega}, \\ S_2 : |b\rangle &\rightarrow (|1'\rangle + i|0'\rangle)/\sqrt{2}, \\ S_2 : |c\rangle &\rightarrow (|0'\rangle + i|1'\rangle)/\sqrt{2}, \\ P_4 : |0'\rangle &\rightarrow |0'\rangle e^{i\varphi}. \end{aligned} \quad (11)$$

The corresponding unitary evolution matrix is given by

$$\mathbf{T}^{MZ}(\alpha, \beta, \omega, \varphi) = i e^{i(\beta+\frac{\omega}{2})} \begin{pmatrix} -e^{i(\alpha+\varphi)} \sin \frac{\omega}{2} & e^{i\varphi} \cos \frac{\omega}{2} \\ e^{i\alpha} \cos \frac{\omega}{2} & \sin \frac{\omega}{2} \end{pmatrix}. \quad (12)$$

Alternatively, $\mathbf{T}^{MZ}$ can be computed by matrix multiplication; i.e.,

$$\mathbf{T}^{MZ}(\alpha, \beta, \omega, \varphi) = i e^{i(\beta+\frac{\omega}{2})} \begin{pmatrix} e^{i\varphi} & 0 \\ 0 & 1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix} \begin{pmatrix} e^{i\omega} & 0 \\ 0 & 1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix} \begin{pmatrix} e^{i(\alpha+\beta)} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\beta} \end{pmatrix}. \quad (13)$$

Both elementary quantum interference devices $\mathbf{T}^{bs}$ and $\mathbf{T}^{MZ}$ are universal in the sense that every unitary quantum evolution operator in two-dimensional Hilbert space

$$\mathbf{U}_2(\omega, \alpha, \beta, \varphi) = e^{-i\beta} \begin{pmatrix} e^{i\alpha} \cos \omega & -e^{-i\varphi} \sin \omega \\ e^{i\varphi} \sin \omega & e^{-i\alpha} \cos \omega \end{pmatrix}, \quad (14)$$

where $-\pi \leq \beta, \omega \leq \pi$, $-\frac{\pi}{2} \leq \alpha, \varphi \leq \frac{\pi}{2}$ [40] corresponds to $\mathbf{T}^{bs}(\omega', \alpha', \beta', \varphi')$ and $\mathbf{T}^{MZ}(\omega'', \alpha'', \beta'', \varphi'')$, where $\omega, \alpha, \beta, \varphi$ are arguments of the (double) primed parameters [46].

A typical example of a nonclassical operation on a quantum bit is the “square root of not” gate ($\sqrt{\text{not}}\sqrt{\text{not}} = \mathbf{X}$)

$$\sqrt{\text{not}} = \frac{1}{2} \begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}. \quad (15)$$

Although $\sqrt{\text{not}}$ still has a eigenstate associated with a fixed point of unit eigenvalue, not all of these unitary transformations have eigenvectors associated with eigenvalues one that can be identified with fixed points. Indeed, only unitary transformations of the form

$$[\mathbf{U}_2(\omega, \alpha, \beta, \varphi)]^{-1} \text{diag}(1, e^{i\lambda}) \mathbf{U}_2(\omega, \alpha, \beta, \varphi) = \begin{pmatrix} \cos \omega^2 + e^{i\lambda} \sin \omega^2 & \frac{-1+e^{i\lambda}}{2} e^{-i(\alpha+\varphi)} \sin(2\omega) \\ \frac{-1+e^{i\lambda}}{2} e^{i(\alpha+\varphi)} \sin(2\omega) & e^{i\lambda} \cos \omega^2 + \sin \omega^2 \end{pmatrix} \quad (16)$$

have fixed points.

Applying nonclassical operations on quantum bits with no fixed points

$$\mathbf{D}^* = [\mathbf{U}_2(\omega, \alpha, \beta, \varphi)]^{-1} \text{diag}(e^{i\mu}, e^{i\lambda}) \mathbf{U}_2(\omega, \alpha, \beta, \varphi) = \begin{pmatrix} e^{i\mu} \cos(\omega)^2 + e^{i\lambda} \sin(\omega)^2 & \frac{e^{-i(\alpha+p)}}{2} (e^{i\lambda} - e^{i\mu}) \sin(2\omega) \\ \frac{e^{i(\alpha+p)}}{2} (e^{i\lambda} - e^{i\mu}) \sin(2\omega) & e^{i\lambda} \cos(\omega)^2 + e^{i\mu} \sin(\omega)^2 \end{pmatrix}, \quad (17)$$

with $\mu, \lambda \neq 2n\pi$, $n \in \mathbb{N}_0$ gives rise to eigenvectors which are not fixed points, but which acquire nonvanishing phases μ, λ in the generalized diagonalization process.

SUMMARY

It has been argued that, because of quantum parallelism, i.e., the effective co-representation of classical mutually exclusive states, the diagonalization method of classical recursion theory has to be modified. Quantum diagonalization involves unitary operators whose eigenvalues carry phases strictly different from multiples of 2π . The quantum fixed point “solutions” of halting problems

can be 50:50 mixtures of the classical halting and nonhalting states, and therefore do not contribute to classical deterministic solutions of the associated decision problems.

Another, less abstract, application for quantum information theory is the handling of inconsistent information in databases. Thereby, two contradicting classical bits of information $|0\rangle$ and $|1\rangle$ are resolved, i.e., co-represented, by the quantum bit $|\psi_+\rangle$. Throughout the rest of the computation the coherence is maintained. After the processing, the result is obtained by an irreversible measurement. The processing of quantum bits, however, would require an exponential space overhead on classical computers in classical bit base [10]. Thus, in order to remain tractable, the corresponding quantum bits should be implemented on truly quantum universal computers.

* Electronic address: `svozil@tuwien.ac.at`; URL: `http://tph.tuwien.ac.at/~svozil`

- [1] H. Rogers, Jr., *Theory of Recursive Functions and Effective Computability* (MacGraw-Hill, New York, 1967).
- [2] M. Davis, *The Undecidable. Basic Papers on Undecidable, Unsolvable Problems and Computable Functions* (Raven Press, Hewlett, N.Y., 1965).
- [3] J. Barwise, *Handbook of Mathematical Logic* (North-Holland, Amsterdam, 1978).
- [4] H. Enderton, *A Mathematical Introduction to Logic* (Academic Press, San Diego, 2001), second edn.
- [5] P. Odifreddi, *Classical Recursion Theory, Vol. 1* (North-Holland, Amsterdam, 1989).
- [6] G. S. Boolos, J. P. Burgess, and R. C. Jeffrey, *Computability and Logic* (Cambridge University Press, Cambridge, 2007), fifth edn.
- [7] R. Landauer, “Information is Physical,” *Physics Today* **44**, 23–29 (1991).
<http://dx.doi.org/10.1063/1.881299>
- [8] P. W. Bridgman, “A Physicist’s Second Reaction to Mengenlehre,” *Scripta Mathematica* **2**, 101–117, 224–234 (1934), cf. R. Landauer [50].
- [9] A. Olszewski, J. Woleński, and R. Janusz, *Church’s Thesis After 70 Years* (Ontos, Berlin, 2006).
- [10] R. P. Feynman, “Simulating physics with computers,” *International Journal of Theoretical Physics* **21**, 467–488 (1982).
- [11] E. Fredkin and T. Toffoli, “Conservative Logic,” *International Journal of Theoretical Physics* **21**, 219–253 (1982), reprinted in [51, Part I, Chapter 3].

<http://dx.doi.org/10.1007/BF01857727>

- [12] H. S. Leff and A. F. Rex, *Maxwell's Demon* (Princeton University Press, Princeton, 1990).
- [13] R. P. Feynman, *The Feynman lectures on computation* (Addison-Wesley Publishing Company, Reading, MA, 1996), edited by A.J.G. Hey and R. W. Allen.
- [14] G. Birkhoff and J. von Neumann, "The Logic of Quantum Mechanics," *Annals of Mathematics* **37**, 823–843 (1936).
- [15] S. Kochen and E. P. Specker, "Logical Structures arising in quantum theory," in *Symposium on the Theory of Models, Proceedings of the 1963 International Symposium at Berkeley* pp. 177–189 (1965), reprinted in [52, pp. 209–221].
- [16] S. Kochen and E. P. Specker, "The calculus of partial propositional functions," in *Proceedings of the 1964 International Congress for Logic, Methodology and Philosophy of Science, Jerusalem* pp. 45–57 (1965), reprinted in [52, pp. 222–234].
- [17] D. J. Foulis, C. Piron, and C. H. Randall, "Realism, operationalism, and quantum mechanics," *Foundations of Physics* **13**, 813–841 (1983), invited papers dedicated to Günther Ludwig.
<http://dx.doi.org/10.1007/BF01906271>
- [18] C. H. Randall and D. J. Foulis, "Properties and operational propositions in quantum mechanics," *Foundations of Physics* **13**, 843–857 (1983), invited papers dedicated to Günther Ludwig.
<http://dx.doi.org/10.1007/BF01906272>
- [19] O. Bournez and M. L. Campagnolo, "A Survey on Continuous Time Computations," in *New Computational Paradigms. Changing Conceptions of What is Computable*, S. Cooper, B. Löwe, and A. Sorbi, eds. (Springer Verlag, New York, 2008), pp. 383–423.
<http://www.lix.polytechnique.fr/bournez/pmwiki/uploads/Main/SurveyContinuousTime.pdf>
- [20] D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer," *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences* (1934–1990) **400**, 97–117 (1985).
<http://dx.doi.org/10.1098/rspa.1985.0070>
- [21] J. Gruska, *Quantum Computing* (McGraw-Hill, London, 1999).
- [22] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
- [23] H.-K. Lo, S. Popescu, and T. Spiller, *Introduction to Quantum Computation and Information* (World Scientific Publishing Company, Singapore, 2001).

- [24] R. K. Brylinski, G. Chen, and B. K. Brylinski, *Mathematics of Quantum Computation* (Chapman & Hall/CRC Press, London, 2002).
- [25] M. Hayashi, *Quantum Information. An Introduction* (Springer-Verlag, Berlin, Heidelberg, 2006).
- [26] H. Imai and M. Hayashi, *Quantum Computation and Information. From Theory to Experiment* (Springer-Verlag, Berlin, Heidelberg, 2006).
- [27] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, “The Security of Practical Quantum Key Distribution,” (2008).
<http://arxiv.org/abs/0802.4155>
- [28] G. Jaeger, *Quantum Information. An Overview* (Springer, New York, 2007).
- [29] N. D. Mermin, *Quantum Computer Science* (Cambridge University Press, Cambridge, 2007).
<http://people.ccmr.cornell.edu/~mermin/qcomp/CS483.html>
- [30] N. D. Mermin, “From Cbits to Qbits: Teaching computer scientists quantum mechanics,” *American Journal of Physics* **71**, 23–30 (2003).
<http://dx.doi.org/10.1119/1.1522741>
- [31] K. Svozil, “Contexts in quantum, classical and partition logic,” in *Handbook of Quantum Logic and Quantum Structures*, K. Engesser, D. M. Gabbay, and D. Lehmann, eds. (Elsevier, Amsterdam, 2008), pp. 551–586.
<http://arxiv.org/abs/quant-ph/0609209>
- [32] M. Born, “Zur Quantenmechanik der Stoßvorgänge,” *Zeitschrift für Physik* **37**, 863–867 (1926).
<http://dx.doi.org/10.1007/BF01397477>
- [33] A. Zeilinger, “The message of the quantum,” *Nature* **438**, 743 (2005).
<http://dx.doi.org/10.1038/438743a>
- [34] K. Gödel, “Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme,” *Monatshefte für Mathematik und Physik* **38**, 173–198 (1931), English translation in [53], and in [2].
- [35] A. R. Anderson, “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).
- [36] G. Cantor, “Gesammelte Abhandlungen,” (Springer, Berlin, 1932).
- [37] A. M. Turing, “On computable numbers, with an application to the Entscheidungsproblem,” *Proceedings of the London Mathematical Society, Series 2* **42 and 43**, 230–265 and 544–546 (1936-7 and

- 1937), reprinted in [2].
- [38] K. Svozil, “Consistent use of paradoxes in deriving constraints on the dynamics of physical systems and of no-go-theorems,” *Foundations of Physics Letters* **8**, 523–535 (1995).
 - [39] P. Diaconis, S. Holmes, and R. Montgomery, “Dynamical Bias in the Coin Toss,” *SIAM Review* **49**, 211–235 (2007).
<http://dx.doi.org/10.1137/S0036144504446436>
 - [40] F. D. Murnaghan, *The Unitary and Rotation Groups* (Spartan Books, Washington, D.C., 1962).
 - [41] R. Shankar, *Principles of Quantum Mechanics, 2nd Edition* (Kluwer Academic/Plenum Publishers, New York, 1980,1994).
 - [42] P. R. Halmos, *Finite-dimensional vector spaces* (Springer, New York, Heidelberg, Berlin, 1974).
 - [43] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, “Experimental realization of any discrete unitary operator,” *Physical Review Letters* **73**, 58–61 (1994).
<http://dx.doi.org/10.1103/PhysRevLett.73.58>
 - [44] M. Reck and A. Zeilinger, “Quantum phase tracing of correlated photons in optical multiports,” in *Quantum Interferometry*, F. D. Martini, G. Denardo, and A. Zeilinger, eds., pp. 170–177 (1994).
 - [45] M. Zukowski, A. Zeilinger, and M. A. Horne, “Realizable higher-dimensional two-particle entanglements via multiport beam splitters,” *Physical Review A (Atomic, Molecular, and Optical Physics)* **55**, 2564–2579 (1997).
<http://dx.doi.org/10.1103/PhysRevA.55.2564>
 - [46] K. Svozil, “Noncontextuality in multipartite entanglement,” *J. Phys. A: Math. Gen.* **38**, 5781–5798 (2005).
<http://dx.doi.org/10.1088/0305-4470/38/25/013>
 - [47] D. M. Greenberger, M. A. Horne, and A. Zeilinger, “Multiparticle interferometry and the superposition principle,” *Physics Today* **46**, 22–29 (1993).
 - [48] B. Yurke, S. L. McCall, and J. R. Klauder, “SU(2) and SU(1,1) interferometers,” *Physical Review A (Atomic, Molecular, and Optical Physics)* **33**, 4033–4054 (1986).
<http://dx.doi.org/10.1103/PhysRevA.33.4033>
 - [49] 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 A (Atomic, Molecular, and Optical Physics)* **42**, 4127–4137 (1990).
<http://dx.doi.org/10.1103/PhysRevA.42.4127>

- [50] R. Landauer, “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.
<http://www.santafe.edu/research/publications/workingpapers/94-10-056.pdf>
- [51] A. Adamatzky, *Collision-based computing* (Springer, London, 2002).
- [52] E. Specker, *Selecta* (Birkhäuser Verlag, Basel, 1990).
- [53] K. Gödel, 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).
- [54] The standard labeling of the input and output ports are interchanged, therefore sine and cosine are exchanged in the transition matrix.