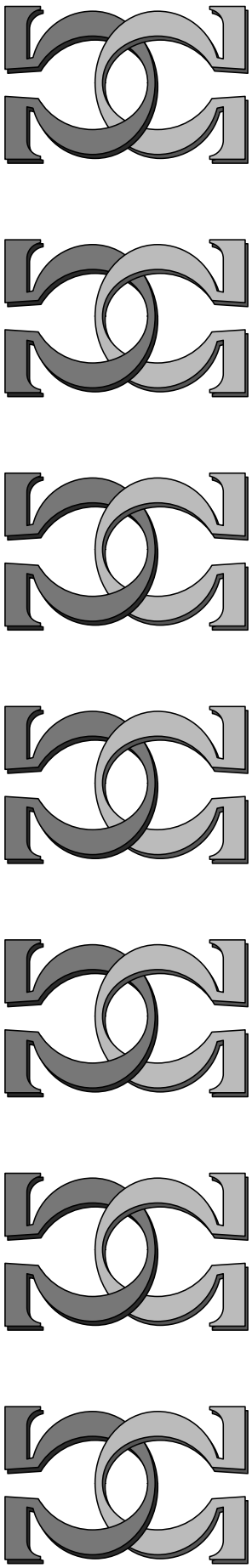

CDMTCS
Research
Report
Series

Characterization of quantum computable decision problems by state discrimination

Karl Svozil
University of Technology, Vienna

CDMTCS-269
June 2005

Centre for Discrete Mathematics and
Theoretical Computer Science

Characterization of quantum computable decision problems by state discrimination

Karl Svozil

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

Abstract. One advantage of quantum algorithms over classical computation is the possibility to spread out, process, analyse and extract information in multipartite configurations in coherent superpositions of classical states. This will be discussed in terms of quantum state identification problems based on a proper partitioning of mutually orthogonal sets of states. The question arises whether or not it is possible to encode equibalanced decision problems into quantum systems, so that a single invocation of a filter used for state discrimination suffices to obtain the result.

OUTLINE

The question as to what might be considered the "essence" of quantum computation, and its possible advantages over classical computation, has been the topic of numerous considerations, both from a physical (e.g., Ref. [1, 2, 3, 4, 5, 6, 7]) as well as from a computer science (e.g., Ref. [8, 9, 10, 11, 12, 13]) perspective. Contributing to this ongoing research, we will present an analysis of novel propositional structures in quantum mechanics; i.e., on the issue of what kind of propositions about quantum computers exist which do not correspond to any classical statement. We will consider coherent superpositions of states and will make explicit use of the fact that in quantum mechanics information can be coded in or "spread among" entangled multipartite systems in such a way that information about the single quanta is not useful for (and even makes impossible) a decryption of the quantum computation.

Alas, it is quite evident that not all decision problems have a proper encoding into some quantum mechanical system such that their resources (computation time, memory usage) is bound by some criterion such as polynomiality or even finiteness. Take, as a concrete example, a particular type of halting problem: Alice presents Bob a black box with input and output interfaces. Bob's task is to find out whether an arbitrary function of n bits encoded in the black box will ever output "0." As this configuration could essentially get as worse as a *busy beaver* problem [14], the time it takes for Alice's box to ever output a "0" may grow faster than any recursive (i.e., computable [15, 16]) function of n.

Is it possible to characterize the exact domain of functions and propositions about them which can be "reasonably" (e.g., polynomially) coded into a quantum computation, given an fairly general set of coding strategies, such as unitary transformations? In what follows, an attempt is made to characterize the class of quantum computable functions whose computational complexity grows *linearly* with the number of bits by considering partitioning of states and the associated propositions and observables [17, 18, 19, 20]. Certain quantum computations such as the Deutsch algorithm will be expressed as state identification problems, resulting in the systematic construction of a great variety of computations corresponding to (incomplete) state identifications based on superposition and interference.

The notation of Mermin [21, 6, 22] will be adopted. Consider at first a single qubit in its most general form $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ with $|\alpha_0|^2 + |\alpha_1|^2 = 1$ as a coherent superposition between some "quasi-classical" states $|0\rangle$ and $|1\rangle$ of the computational basis representable by the set of orthogonal vectors $\{|0\rangle \equiv (1,0)^T, |1\rangle \equiv (0,1)^T\}$ (the superscript T indicates transposition). A 50:50 mixture of the quasi-classical states is obtained by $\mathbf{H}|0\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$ or $\mathbf{H}|1\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle)$ where $\mathbf{H}$ is the normalized Hadamard matrix $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. According to quantum logic [23, 24, 25], the interpretation of $\mathbf{H}|0\rangle$ or $\mathbf{H}|1\rangle$ it is the proposition, *"the quant is in the state associated with the projector* $(1/2)(\mathbf{1} \pm \mathbf{X})$," where $\mathbf{1}$ is the unitity and $\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is the *not*-operator. Classically, neither these states nor the projectors correspond to any opertionalizable physical entity. Quantum mechanically, they have,

for instance, an interpretation in terms of electron or neutron spin states and spin state measurements by a Stern-Gerlach apparatus, or in terms of photon polarization states and polarization measurements. Since $(1/2)(\mathbf{1}\pm\mathbf{X}) = (1/2)\,[\mathbf{1}+\sigma(\theta=\pm\pi/2,\varphi=0)]$ with $\sigma(\theta,\varphi) = \begin{pmatrix} \cos\theta & e^{-i\varphi}\sin\theta \\ e^{i\varphi}\sin\theta & -\cos\theta \end{pmatrix}$ for the polar angle θ and the azimuthal angle φ, the physical proposition corresponding to $\mathbf{H}|0\rangle$ and $\mathbf{H}|1\rangle$ is *"along the polar angle $\pm\pi/2$ and azimuthal angle $\varphi=0$, the particle is in a linear polarization (or positive spin) state."*

IDENTIFYING STATES AMONG CONTEXTS

A *context* can formally be defined [26] as a single (nondegenerate) "maximal" self-adjoint operator $\mathbf{C}$. It has a spectral decomposition into some complete set of orthogonal projectors $\mathbf{E}_i$ which correspond to propositions in the von Neumann-Birkhoff type sense [23, 27]. That is, $\mathbf{C} = \sum_{i=1}^{d} e_i\mathbf{E}_i$ with mutually different real e_i and some orthgonal projectors $\{\mathbf{E}_i \mid i = 1,\ldots d\}$ of d-dimensional Hilbert space. In d dimensions, contexts can be viewed as d-pods or orthogonal bases spanned by the vectors associated with the d mutually orthogonal projectors $\mathbf{E}_1,\mathbf{E}_2,\cdots,\mathbf{E}_d$.

The general problem to (uniquely) identify orthogonal pure states among contexts resulting from k particles in $n=2$ or more dimensions per particle has been solved in Ref. [18, 19, 20] *via* a system of k co-measurable filters $\mathbf{F}_i$, $i=1,\ldots,k$ with the following properties:

(F1) Every filter $\mathbf{F}_i$ corresponds to an operator (or a set of operators) which generates an equi-n-partition of the d-dimensional state space into n slices (i.e., partition elements) containing $d/n = d^{1-1/k} = n^{k-1}$ states per slice. (Note that $d=n^k$.) A filter is said to separate two eigenstates if the eigenvalues are different.

(F2) From each one of the k partitions of (F1), take an arbitrary element. The intersection of the elements of all different partitions results in a *single* one of the $d=n^k$ different states.

(F3) The union of all those single states generated by the intersections of (F2) is the entire set of states.

For $n=2$, an explicit construction of all the systems of filters and their associated propositions can be given in terms of projectors and their orthogonal projectors; every one of them projecting onto a $d/2$-dimensional subspace, such that the serial composition of any complete set of (orthogonal) projectors (one per filter) yields the finest resolution; i.e., some of the d one-dimensional projectors $\mathbf{E}_i$ spanning the context $\mathbf{C}$.

The system of filters resolving $\mathbf{C}$ is not unique; all such systems of filters can be obtained by permutating the columns of the matrix whose rows are the diagonal elements of all the filters in diagonalized form. Different contexts $\mathbf{C}'$ are resolved by different systems of filters which are obtained by transforming $\mathbf{F}_i$, $i=1,\ldots,k$ through the same basis transformation which transforms $\mathbf{C}$ into $\mathbf{C}'$. Several examples and explicit constructions will be given below.

Take, for instance, three two-state quanta, i.e., the case $k=3$, $n=2$, and thus $d=2^3$. The three projectors

$$\begin{aligned} \mathbf{F}_1 &= \mathrm{diag}(1,1,1,1,0,0,0,0), \\ \mathbf{F}_2 &= \mathrm{diag}(1,1,0,0,1,1,0,0), \\ \mathbf{F}_3 &= \mathrm{diag}(1,0,1,0,1,0,1,0), \end{aligned}$$

together with their orthogonal projectors

$$\begin{aligned} \mathbf{F}'_1 &= \mathrm{diag}(0,0,0,0,1,1,1,1), \\ \mathbf{F}'_2 &= \mathrm{diag}(0,0,1,1,0,0,1,1), \\ \mathbf{F}'_3 &= \mathrm{diag}(0,1,0,1,0,1,0,1), \end{aligned}$$

form the system of three filters $\{\{\mathbf{F}_1,\mathbf{F}'_1\},\{\mathbf{F}_2,\mathbf{F}'_2\},\{\mathbf{F}_3,\mathbf{F}'_3\}\}$ which have the desired properties (F1)–(F3). Equivalent filters are obtained by permuting the columns of the diagonal rows of

$$\left(\begin{array}{cccccccc} 1&1&1&1&0&0&0&0 \\ 0&0&0&0&1&1&1&1 \\ \hline 1&1&0&0&1&1&0&0 \\ 0&0&1&1&0&0&1&1 \\ \hline 1&0&1&0&1&0&1&0 \\ 0&1&0&1&0&1&0&1 \end{array}\right). \tag{1}$$

TABLE 1. The binary functions of one bit considered in Deutsch's problem.

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

Different systems of filters are obtained by permutating the columns of the matrix in Eq. 1; e.g.,

$$\left(\begin{array}{cccccccc} 1&1&1&0&0&0&0&1\\ 0&0&0&1&1&1&1&0\\ \hline 1&0&0&1&1&0&0&1\\ 0&1&1&0&0&1&1&0\\ \hline 0&1&0&1&0&1&0&1\\ 1&0&1&0&1&0&1&0 \end{array}\right), \quad \left(\begin{array}{cccccccc} 1&1&0&0&0&0&1&1\\ 0&0&1&1&1&1&0&0\\ \hline 0&0&1&1&0&0&1&1\\ 1&1&0&0&1&1&0&0\\ \hline 1&0&1&0&1&0&1&0\\ 0&1&0&1&0&1&0&1 \end{array}\right), \quad \ldots \tag{2}$$

In the case of $k = 2$, any permutation yields the original system of filters.

Different contexts are reached by transforming every single filter operator through the same unitary transformation. Note that the row permutations and unitary transformations are exhaustive; i.e., there are no other methods available. For $n > 2$, the filter operators cannot correspond to projectors, because they are not binary but n-ary. In this case, for instance, n^k different prime numbers can be used as eigenvalues. A more detailed treatment of this case can be found in Refs. [19, 20].

DEUTSCH'S PROBLEM AND RELATED ALGORITHMS

In what follows, Deutsch's decision problem to find out whether or not an unknown function f that takes a single (classical) bit into a single (classical) bit is constant or not, which is equal to finding the parity of $f : \{0,1\} \to \{0,1\}$, will be interpreted as a state identification problem, which is solved by the methods discussed in the previous section. There are four possible bivalent functions of one bit: the constant functions f_0 and f_3 take any bit value and map it into either 0 or 1, respectively. The two remaining functions f_1 and f_2 correspond to the identity $\mathbf{1}$ and to the *not* operator $\mathbf{X}$, and are thus not constant (cf. Table 1). Hence, with respect to constancy, the set of all functions $\{f_0, f_1, f_2, f_3\}$ is equipartitioned into

$$F_D = \{\{f_0, f_3\}, \{f_1, f_2\}\}. \tag{3}$$

The first and second elements $\{f_0, f_3\}$ and $\{f_1, f_2\}$ of this partition can be interpreted as the proposition, *"the function is (not) constant."*

When coding the Deutsch problem and the computation of f into a state identification problem, one task is to map the binary partition F_D in Eq. (3) into a quantum state filter $\mathbf{F}$ with equivalent separation properties. Presently, there does not exist any algorithmic way (only heuristic ones) to obtain such a quantum encoding, nore is any one likely to exist (cf. the parity problem discussed below).

First note that, as the functions f_0 and f_3 are two-to-one (i.e., irreversible), the input bit needs to be augmented by a second bit to maintain reversibility, which is a necessary condition for the unitarity of the state evolution. Usually, this is accomplished by considering $\mathbf{U}_f(|x\rangle|y\rangle) = |x\rangle|y \oplus f(x)\rangle$, where $\oplus$ is the modulo-2 addition (without carrying).

The encoding Ansatz enumerated in Table 2 represents the evolution of the single terms contributing to $\mathbf{U}_f(\mathbf{H} \otimes \mathbf{H})(\mathbf{X} \otimes \mathbf{X})(|0\rangle|0\rangle)$, resulting in the two different states

$$|\psi_1\rangle = \pm\frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle) \equiv \pm\frac{1}{2}((1,-1)\otimes(1,-1))^T = \pm\frac{1}{2}(1,-1,-1,1)^T \tag{4}$$

for f_0 as well as f_3, and

$$|\psi_2\rangle = \pm\frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \equiv \pm\frac{1}{2}((1,1)\otimes(1,-1))^T = \pm\frac{1}{2}(1,-1,1,-1)^T \tag{5}$$

TABLE 2. State evolution of $\mathbf{U}_f(\mathbf{H}\otimes\mathbf{H})(\mathbf{X}\otimes\mathbf{X})(|0\rangle|0\rangle)$ for the four functions f_0, f_1, f_2, f_3.

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

for f_1 as well as f_2. Together with $|\psi_3\rangle = (\mathbf{H}\otimes\mathbf{H})(|0\rangle|0\rangle) \equiv (1/2)(1,1,1,1)^T$ and $|\psi_4\rangle = (\mathbf{H}\otimes\mathbf{H})(\mathbf{X}\otimes\mathbf{1})(|0\rangle|0\rangle) \equiv (1/2)(1,1,-1,-1)^T$, the four states in $\mathbf{B}^D = \{\psi_1,\psi_2,\psi_3,\psi_4\}$ form an orthonormal basis.

Application of two Hadamard-transformations for each one of the two bits finally yields a representation in the sandard computational basis; i.e.,

$$(\mathbf{H}\otimes\mathbf{H})\mathbf{U}_f(\mathbf{H}\otimes\mathbf{H})(\mathbf{X}\otimes\mathbf{X})(|0\rangle|0\rangle) = \begin{cases} |1\rangle|1\rangle \equiv (0,0,0,1)^T & \text{for } f(0)=f(1), \\ |0\rangle|1\rangle \equiv (0,1,0,0)^T & \text{for } f(0)\neq f(1). \end{cases} \tag{6}$$

We are now in the position to formulate the state identification problem corresponding to the Deutsch algorithm. This is achieved by considering the projector $\mathbf{F}_1 = \mathrm{diag}(1,1,0,0)$, which, together with its orthogonal projector $\mathbf{F}_1' = \mathrm{diag}(0,0,1,1)$, constitutes a filter corresponding to the binary partition F_D in Eq. (3). Note that a second filter $\mathbf{F}_2$, based on the projections $\mathbf{F}_2 = \mathrm{diag}(1,0,1,0)$ and $\mathbf{F}_2' = \mathrm{diag}(0,1,0,1)$, completes the system of filters. It is unable to separate $|11\rangle$ from $|01\rangle$, but separates $|00\rangle$ and $|10\rangle$ from $|01\rangle$ and $|11\rangle$.

Alternatively, we may consider the state identification problem without the final Hadamard transformations as, *"find the observables which separate* ψ_1 *from* ψ_2*."* The complete state identification problem should also contain the observables separating ψ_3 from ψ_4, but in Deutsch's problem one is not primarily interested in uniquely identifying the function itself; rather in its (non)constancy. Hence, it is not necessary to employ the entire system of two filters, but rather a single filter constructed to separate f_0, f_3 from f_1, f_2. This is achieved by transforming the two operators $\mathbf{F}_1 = \mathrm{diag}(1,1,0,0)$ and $\mathbf{F}_2 = \mathrm{diag}(1,0,1,0)$ associated with a binary search type state separation in the basis $\mathbf{B} = \{(1,0,0,0)^T,(0,1,0,0)^T,(0,0,1,0)^T,(0,0,0,1)^T\}$ through $\mathbf{U}\mathbf{F}_1\mathbf{U}^{-1} = \mathbf{F}_1^D$ and $\mathbf{U}\mathbf{F}_2\mathbf{U}^{-1} = \mathbf{F}_2^D$, where

$$\mathbf{U} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 \end{pmatrix} \tag{7}$$

is the unitary transformation which corresponds to a basis change $\mathbf{B} \to \mathbf{U}\mathbf{B} = \mathbf{B}^D$. It is straightforward to check that, by the eigenvalue spectrum, $\mathbf{F}_1^D$ separates between ψ_1 and ψ_3 from ψ_2 and ψ_4 (and at the same time, $\mathbf{F}_2^D$ separates between ψ_1 and ψ_2 from ψ_3 and ψ_4). Hence, $\mathbf{F}_1^D$ generates a partition $\{\{\psi_1,\psi_3\},\{\psi_2,\psi_4\}\}$ of the set $\{\psi_1,\psi_3,\psi_2,\psi_4\}$ of orthogonal states. ($\mathbf{F}_2^D$ generates the partition $\{\{\psi_1,\psi_2\},\{\psi_3,\psi_4\}\}$.) The states ψ_i, however, do not directly correspond to the functions f_j in the Deutsch partition in Eq. (3); they rather represent joint properties of these functions, such as constancy.

Another encoding strategy of the Deutsch problem can be based upon a immediate identification of $\{f_0,f_1,f_2,f_3\}$ with the four states of the computational basis $\mathbf{B}$. The nontrivial part in this case is the mapping of the functions f_i on to $\mathbf{B}$; e.g., by constructing unitary transformations depending on f_i and acting on $|00\rangle$, such as for instance $\mathbf{V}_f|00\rangle = |f(0)f(1)\rangle$. Once this has been achieved, in order to express constancy, the filter would then have to separate the orthogonal (Bell) states $\varphi_{1,4} \equiv (1,0,0,\pm1)^T$ from $\varphi_{2,3} \equiv (0,1,\pm1,0)^T$; a rather straightforward task.

Still another encoding strategy would be to invoke the phase oracle $\mathbf{U}_f(|x\rangle\otimes\mathbf{H}|1\rangle) = (-1)^{f(x)}|x\rangle\otimes\mathbf{H}|1\rangle$. The resulting states are enumerated in Table 3. The phases result in the orthogonality of the two linear subspaces corresponding to f_0 and f_3, with respect to f_1 and f_2.

In a very similar manner, one could discuss the Bernstein-Vazirani algorithm, as well as the Deutsch-Josza and Simon's decision problems (in the latter cases with the proviso discussed later, since the algorithm is not deterministic). Note that this method exhausts all possible decision problems based on equipartitioning of state spaces, but does not give a direct hint about the type of classical algorithmic problem which are solvable that way.

TABLE 3. The phase factors of $(-1)^{f(x)}|xy\rangle$.

	$(-1)^{f(x)}$	
f	$\|0\rangle$	$\|1\rangle$
f_0	$+$	$+$
f_1	$+$	$-$
f_2	$-$	$+$
f_3	$-$	$-$

TABLE 4. Listing of the 16 binary functions of two variables x, y with their parity bits "$\pm$".

$\pm$	f	00	01	10	11
$+$	f_0	0	0	0	0
$-$	f_1	0	0	0	1
$-$	f_2	0	0	1	0
			$\cdots$		
$+$	f_{15}	1	1	1	1

PARITY CHECKING

Deutsch's problem is just the simplest in a particular class of problems: check the parity of an unknown binary function $f : \{0,1\}^k \to \{0,1\}$ of k bits. There are 2^{2^k} such functions. The parity of a function f of k bits depends on whether the number of functional values of $f(x_1,\ldots,x_k) = 1$ on all $x_1,\ldots,x_k \in \{0,1\}$ is even or odd, denoted by "$+$" and "$-$," respectively.

Consider, for the sake of an example, two bits x, y and an unknown function $f(x,y)$ of all the $2^{2^2} = 16$ binary functions partly listed in Tab. 4. The set of 16 functions can be equipartitioned into two groups of 8 functions, according to positive and negative parity; i.e.,

$$F_P = \{\{f_0, f_5, f_6, f_7, f_8, f_9, f_{10}, f_{15}\}, \{f_1, f_2, f_3, f_4, f_{11}, f_{12}, f_{13}, f_{14}\}\}. \tag{8}$$

One might be tempted to speculate that the corresponding proposition corresponds to some realizable quantum filter which separates the two parity classes by some quantum implementation $\mathbf{U}_f$ in a single run. Motivation for this comes from the direct and "local," or "isolated" evaluation of the functional values; without any recursion, iteration, or additional functional and contextual relation between the values. Despite these indications, the parity of a function has been proven quantum computationally hard [28, 11, 29, 30, 31]: It is only possible to go from 2^k classical queries down to $2^k/2$ quantum queries, thereby gaining a factor of 2.

Classically, parity checking grows exponentially 2^k with the number k of bits of the functional arguments, as there is no other was than to compute the functional values on the entire set of 2^k arguments. Quantum mechanically, one may interpret this problem as a particular instance of a generalized Grover algorithm with an unknown number of special states, which can be solved by applying the quantum Fourier transform.

By making use of the phase oracle $\mathbf{U}_f(|x\rangle \otimes \mathbf{H}|1\rangle) = (-1)^{f(x)}|x\rangle \otimes \mathbf{H}|1\rangle$, one obtains, after a second application of a Hadamard transformation,

$$(\mathbf{1} \otimes \mathbf{1} \otimes \mathbf{H})\,\mathbf{U}_f\,(\mathbf{1} \otimes \mathbf{1} \otimes \mathbf{H})\,|x,y\rangle|1\rangle = (-1)^{f(x,y)}|x,y\rangle|1\rangle. \tag{9}$$

Table 5 lists the results of this transformation. As long as the function is "unbalanced," such that the number of values of $f(x_1,\ldots,x_k) = 1$ is small compared to 2^k, a quadratic speedup is achievable. However, this condition does in general not apply.

GENERALIZED DEUTSCH ALGORITHMS

In what follows we shall present a type of quantum algorithm which is directly motivated by the state identification problem. Consider the class of binary functions of two variables which are the sums of two (or more) binary functions of one variable; e.g.,

$$f_{ij}(x,y) = f_i(x) + f_j(y); \quad 0 \le i,j \le 3. \tag{10}$$

TABLE 5. The phases from Eq. (9).

		$(-1)^{f(x)}$			
$\pm$	f	$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$
$+$	f_0	$+$	$+$	$+$	$+$
$-$	f_1	$+$	$+$	$+$	$-$
$-$	f_2	$+$	$+$	$-$	$+$
$-$	f_3	$+$	$-$	$+$	$+$
$-$	f_4	$-$	$+$	$+$	$+$
$+$	f_5	$+$	$+$	$-$	$-$
$+$	f_6	$+$	$-$	$+$	$-$
$+$	f_7	$-$	$+$	$+$	$-$
$+$	f_8	$+$	$-$	$-$	$+$
$+$	f_9	$-$	$+$	$-$	$+$
$+$	f_{10}	$-$	$-$	$+$	$+$
$-$	f_{11}	$+$	$-$	$-$	$-$
$-$	f_{12}	$-$	$+$	$-$	$-$
$-$	f_{13}	$-$	$-$	$+$	$-$
$-$	f_{14}	$-$	$-$	$-$	$+$
$+$	f_{15}	$-$	$-$	$-$	$-$

TABLE 6. The phases from the phase oracle applied to Eq. (10).

	$(-1)^{f_i(x)+f_j(y)}$			
f	$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$
f_{00}	$+$	$+$	$+$	$+$
f_{01}	$+$	$-$	$+$	$-$
f_{02}	$-$	$+$	$-$	$+$
f_{03}	$-$	$-$	$-$	$-$
f_{10}	$+$	$+$	$-$	$-$
f_{11}	$+$	$-$	$-$	$+$
f_{12}	$-$	$+$	$+$	$-$
f_{13}	$-$	$-$	$+$	$+$
f_{20}	$-$	$-$	$+$	$+$
f_{21}	$-$	$+$	$+$	$-$
f_{22}	$+$	$-$	$-$	$+$
f_{23}	$+$	$+$	$-$	$-$
f_{30}	$-$	$-$	$-$	$-$
f_{31}	$-$	$+$	$-$	$+$
f_{32}	$+$	$-$	$+$	$-$
f_{33}	$+$	$+$	$+$	$+$

The binary functions f_i, f_j of one bit are the same as in Deutsch's problem listed in Table 1. The corresponding unitary transformations given by $\mathbf{U}_{f_{ij}} = \mathbf{U}_{f_i} \otimes \mathbf{U}_{f_j}$. In this case, the phase oracle yields phases which are listed in Table 6.

The four orthogonal vectors resulting from the phase enumeration in Table 6 form a basis $\mathbf{B}' = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}$, with

$$\begin{array}{rcl} \varphi_1 & = & (1,1,1,1)^T, \\ \varphi_2 & = & (1,1,-1,-1)^T, \\ \varphi_3 & = & (1,-1,1,-1)^T, \\ \varphi_4 & = & (1,-1,-1,1)^T. \end{array} \quad . \tag{11}$$

Consider the decision problems corresponding to the following propositions:

(D1) *The function $f_{ij}(x,y)$ is constant in the first argument.*

(D2) *The function $f_{ij}(x,y)$ is constant in the second argument.*

(D3) *The function $f_{ij}(x,y)$ is constant in the first argument and not constant in the second argument, or it is constant in the second argument and not constant in the first argument.*

(D4) *The function $f_{ij}(x,y)$ is constant in the first argument and constant in the second argument, or it is not constant in the second argument and not constant in the first argument.*

The partitions corresponding to these decision problems are

$$F_1 = \{\{f_{00},f_{01},f_{02},f_{03},f_{30},f_{31},f_{32},f_{33}\},\{f_{10},f_{11},f_{12},f_{13},f_{20},f_{21},f_{32},f_{33}\}\}, \quad (12)$$
$$F_2 = \{\{f_{00},f_{10},f_{20},f_{30},f_{03},f_{13},f_{23},f_{33}\},\{f_{01},f_{11},f_{21},f_{31},f_{02},f_{12},f_{22},f_{32}\}\}, \quad (13)$$
$$F_3 = \{\{f_{01},f_{02},f_{10},f_{13},f_{20},f_{23},f_{31},f_{32}\},\{f_{00},f_{03},f_{11},f_{12},f_{21},f_{22},f_{30},f_{33}\}\}, \quad (14)$$
$$F_4 = \{\{f_{00},f_{03},f_{11},f_{12},f_{21},f_{22},f_{30},f_{33}\},\{f_{01},f_{02},f_{10},f_{13},f_{20},f_{23},f_{31},f_{32}\}\}. \quad (15)$$

Thus any filter which resolves the associated decision problem at once has to separate (1) φ_1 and φ_3 from φ_2 and φ_4, (2) φ_1 and φ_2 from φ_3 and φ_4, (3) φ_2 and φ_3 from φ_1 and φ_4, (4) φ_1 and φ_4 from φ_2 and φ_3, respectively.

Again, the strategy is to find the unitary transform

$$\mathbf{U}' = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}, \quad (16)$$

which yields a basis change $\mathbf{B} \rightarrow \mathbf{U}'\mathbf{B} = \mathbf{B}'$. Then, measurement of $\mathbf{F}' = (\mathbf{U}')^{-1}\mathbf{F}_i\mathbf{U}'$ with

$$\mathbf{F}_1 = \mathrm{diag}(1,0,1,0), \quad (17)$$
$$\mathbf{F}_2 = \mathrm{diag}(1,1,0,0), \quad (18)$$
$$\mathbf{F}_3 = \mathrm{diag}(0,1,1,0), \quad (19)$$
$$\mathbf{F}_4 = \mathrm{diag}(1,0,0,1), \quad (20)$$

solves the decision problems (D1)–(D4), respectively. This method can be generalized to more than two arguments in a straightforward manner.

INFORMATION SPREAD AMONG QUANTA

So why can the parity of a function not be efficiently coded quantum mechanically? In Ref. [11], Beals *et al.* argue that exponential quantum speed-up can be obtained for partial functions (e.g., problems involving a promise on input [1]), whereas such speedups cannot be obtained for any total function. Another ansatz for an explanation, put forward by Orus *et al.* in Ref. [30], is majorization: The probability distribution associated with the quantum state is step-by-step majorized until it is maximally ordered. Then a measurement provides the solution with high probability.

We propose here that the lack of efficient quantum algorithms is due to the nonexistence of mappings of functions f and decision problems into suitable unitary transformations $\mathbf{U}_f$ which could be used for a system of states and of filter(s) resolving those states corresponding to that particular algorithmic problem and no other one. To give an example, in order for a quantum computation to resolve the equipartition in Eq. (8) by some equivalent quantum state filter, any such filter must be based upon an encoding of the functional parity into some orthogonal set of states. Thereby, in order for the encoding to be efficient, it should not require the separate functional evaluation of all classical cases. On the contrary, the mapping $f \mapsto U_f$, as well as states and filters need to be conceptualized in a way which leaves the single functional values *undefined*, but concentrates on the structural property of parity alone: the even or odd number of occurrence of certain functional values (0 or 1) on the entirety of outputs. If the filters could resolve singular functional values in the standard computational basis, they would essentially model classical information. Any such state preparation or measurement would make impossible the encoding of information "spread among" multipartite states as mentioned above, which seems to be one of the advantages of quantum computing. In this paradigm, entanglement and the suitable superposition of multipartite states become related concepts, as no multipartite state which can be factored could be used to "spread" information among the quanta (or a group of quanta) corresponding to these factors.

---

[1] A partial function is a function which is not defined for some of its domain.

In general, while all classical computable recursive functions f and decision problems can be coded quantum mechanically, there is no guarantee that a problem can be coded efficiently by mapping it into the quantum domain. By an efficient coding of a (binary or n-ary) decision problem we mean that some quantum circuit $\mathbf{U}_f$ exists which outputs a state which is uniquely identifiable by a single filter (or at least by a polynomial number of filters), the outcome of which corresponds to the solution of this problem.

While the parity of a binary function of more than one observable has already been mentioned as an example of quantum computationally "hard" problems, it appears not totally unreasonable to speculate that functional recursions and iterations represent an additional burden on efficiency. Recursions may require a space overhead to keep track of the computational path, in particular if the recursion depth cannot be coded efficiently. From this point of view, quantum implementations of the Ackermann or the Busy Beaver functions, to give just two examples, may even be less efficient than classical implementations, where an effective waste management can get rid of many bits; in particular in the presence of a computable radius of convergence.

STATE IDENTIFICATION AND DENSE CODING

Let us also briefly mention another issue related to state identification if there is a mismatch between the context in which information is prepared and a different context, in which this information is retrieved. Based on such a context mismatch, a "dense coding" scheme has been proposed [32] to probabilistically encode "more" than one classical bits into one quantum bit (despite Holevo's bound). This method is based on the fact that the qubit states $|0\rangle$ and $|1\rangle$ span the computational basis $\{(1,0)^T,(0,1)^T\}$, as already mentioned before, and that any coding of a qubit state which is neither orthogonal nor collinear, such as $(\cos(\pi/8),\sin(\pi/8))^T$, results in a probability of detecting it in the original states governed by its projection onto them. The argument is about efficiency of state identification in the classical and quantum case for "misaligned" systems of states.

Alas, when speaking about coding and representation efficiency of statistical raw data, it is mandatory to take an issue into account which changes the classical framework rather dramatically. As has been pointed out repeatedly by Summhammer [33, 34], the "true" probability of the occurrence of a (classical) bit is unknown. Frequency counts are just approximations to this value. As it turns out, if a *finite* amount of information is used to characterize the probability p by the actually observed relative frequencies L/N, where N is the number of experiments and L is the number of occurrences, then the accuracy varies as a function of p. Thus, a representation of the data has to be chosen which guarantees a constant rate of accuracy over the entire probability range. This results in a redefinition of the functional representation of the relative frequency which is very similar to the quantum mechanical representation by vectors and projectors in Hilbert space. (Compare Mermin's representation [21, 6, 22] of classical information theory and reversible operations on classical bits in linear vector spaces in some analogy to the quantum formalism.) From this point of view, taking the finite coding of probabilities by relative frequencies into account, the classical and the quantum "dense" coding schemes become equivalent.

SUMMARY

We have presented an analysis of quantum computations in terms of state identification whose complexity grows linearly with the number of bits. Thereby, we have characterized this domain by partitions of state space, as well as by unitary transformations of the associated filter systems. Such systems are not bound by the individual classical values, as information about the (parallelized) result of a computation may be "spread among" the quanta in a way which makes it impossible to reconstruct the result by measuring the quanta separately. At the same time, such distributed information could be analyzed a single (or a few) measurement(s) by proper filters resolving the computed proposition.

The method does not yield a constructive, operational method for deciding whether or not (and if so, how) functions or decision problems of practical interest can be efficiently coded into quantum algorithms. From a foundational point of view it is interesting to realize that, while every suitable equipartitioning of state space is equivalent to some proposition which can be interpreted as an outcome of some quantum computation, not all decision problems or functional evaluations which can be rephrased as state partitions can be translated efficiently into the quantum domain.

ACKNOWLEDGMENTS

I am grateful to David Mermin for pointing out a generalization of a two-bit problem to functional parity.

REFERENCES

1. Ekert, A., and Jozsa, R., *Reviews of Modern Physics*, **68**, 733–753 (1996).
2. Preskill, J., *Proceedings of the Royal Society (London) A*, **454**, 469–486 (1998), URL http://dx.doi.org/10.1098/rspa.1998.0171.
3. Preskill, J., Quantum computation, URL http://www.theory.caltech.edu/~preskill/ph219/index.html, lecture notes.
4. Nielsen, M. A., and Chuang, I. L., *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.
5. Galindo, A., and Martin-Delgado, M. A., *Reviews of Modern Physics*, **74**, 347–432 (2002), URL http://dx.doi.org/10.1103/RevModPhys.74.347.
6. Mermin, N. D. (2002-2004), URL http://people.ccmr.cornell.edu/~mermin/qcomp/CS483.html.
7. J. Eisert, M. W., "Quantum computing," in *Handbook Innovative Computing*, edited by A. Zomaya, G. Milburn, J. Dongarra, D. Bader, R. Brent, M. Eshaghian-Wilner, and F. Seredynski, Springer, Berlin, Heidelberg, New York, 2004, pp. 281–283.
8. Gruska, J., *Quantum Computing*, McGraw-Hill, London, 1999.
9. Bennett, C. H., Bernstein, E., Brassard, G., and Vazirani, U., *SIAM Journal on Computing*, **26**, 1510–1523 (1997), URL http://dx.doi.org/10.1137/S0097539796300933.
10. Ozhigov, Y., Quantum computer can not speed up iterated applications of a black box.
11. Beals, R., Buhrman, H., Cleve, R., Mosca, M., and de Wolf, R., *Journal of the ACM*, **48**, 778–797 (2001), URL http://dx.doi.org/10.1145/502090.502097.
12. Cleve, R., "An Introduction to Quantum Complexity Theory," in *Collected Papers on Quantum Computation and Quantum Information Theory*, edited by C. Macchiavello, G. Palma, and A. Zeilinger, World Scientific, Singapore.
13. Fortnow, L., *Theoretical Computer Science*, **292**, 597–610 (2003), URL http://dx.doi.org/10.1016/S0304-3975(01)00377-2.
14. Rado, T., *The Bell System Technical Journal*, **XLI(41)**, 877–884 (1962).
15. Rogers, Jr., H., *Theory of Recursive Functions and Effective Computability*, MacGraw-Hill, New York, 1967.
16. Odifreddi, P., *Classical Recursion Theory*, North-Holland, Amsterdam, 1989.
17. Zeilinger, A., *Foundations of Physics*, **29**, 631–643 (1999).
18. Donath, N., and Svozil, K., *Physical Review A*, **65**, 044302 (2002), URL http://dx.doi.org/10.1103/PhysRevA.65.044302.
19. Svozil, K., *Physical Review A*, **66**, 044306 (2002), URL http://dx.doi.org/10.1103/PhysRevA.66.044306.
20. Svozil, K., *Journal of Modern Optics*, **51**, 811–819 (2004).
21. Mermin, N. D., *American Journal of Physics*, **71**, 23–30 (2003), URL http://dx.doi.org/10.1119/1.1522741.
22. Mermin, N. D., *IBM Journal of Research and Development*, **48**, 53–62 (2004), URL http://dx.doi.org/10.1147/rd.481.0053.
23. Birkhoff, G., and von Neumann, J., *Annals of Mathematics*, **37**, 823–843 (1936).
24. von Neumann, J., *Mathematical Foundations of Quantum Mechanics*, Princeton University Press, Princeton, 1955.
25. Svozil, K., *Quantum Logic*, Springer, Singapore, 1998.
26. Svozil, K., "On Counterfactuals and Contextuality," in *AIP Conference Proceedings 750. Foundations of Probability and Physics-3*, edited by A. Khrennikov, American Institute of Physics, Melville, NY, 2005, pp. 351–360, URL http://dx.doi.org/10.1063/1.1874586.
27. von Neumann, J., *Mathematische Grundlagen der Quantenmechanik*, Springer, Berlin, 1932, English translation in [24].
28. Farhi, E., Goldstone, J., Gutmann, S., and Sipser, M., *Physical Review Letters*, **81**, 5442–5444 (1998), URL http://dx.doi.org/10.1103/PhysRevLett.81.5442.
29. Miao, X., A polynomial-time solution to the parity problem on an NMR quantum computer (2001).
30. Orus, R., Latorre, J. I., and Martin-Delgado, M. A., *European Physical Journal D*, **29**, 119–132 (2004), URL http://dx.doi.org/10.1140/epjd/e2004-00009-3.
31. Stadelhofer, R., Suterand, D., and Banzhaf, W., *Physical Review A*, **71**, 032345 (2005).
32. Ambainis, A., Nayak, A., Ta-Shma, A., and Vazirani, U., *J. ACM*, **49**, 496–511 (2002), ISSN 0004-5411, URL http://dx.doi.org/10.1145/581771.581773.
33. Summhammer, J., *Physics Letters A*, **136**, 183–187 (1989), URL http://dx.doi.org/10.1016/0375-9601(89)90557-4.
34. Summhammer, J., "Maximum predictive Power and the superposition principle," in *Proceedings of the Third International Workshop on Squeezed States and Uncertainty Relations, Maryland, August 10-13, 1993, NASA Conference publication Nr. 3270*, edited by D. Han, Y. S. Kim, N. H. Rubin, Y. Shih, and W. W. Zachary, NASA, Greenbelt, Maryland 20771, 1993, pp. 315–320.