Quantum Information and Computation, Vol. 7, No. 1 (2007) 083–092

HIDDEN SYMMETRY DETECTION ON A QUANTUM COMPUTER

R. SCHÜTZHOLD[a]
Institut für Theoretische Physik, Technische Universität Dresden
01062 Dresden, Germany

W. G. UNRUH[b]
Department of Physics and Astronomy, University of British Columbia
Vancouver, British Columbia, Canada V6T 1Z1
Canadian Institute for Advanced Research Cosmology and Gravity Program

Received June 6, 2005
Revised May 30, 2006

The fastest quantum algorithms (for the solution of classical computational tasks) known so far are basically variations of the hidden subgroup problem with $f(U[x]) = f(x)$. Following a discussion regarding which tasks might be solved efficiently by quantum computers, it will be demonstrated by means of a simple example, that the detection of more general hidden (two-point) symmetries $V\{f(x), f(U[x])\} = 0$ by a quantum algorithm can also admit an exponential speed-up. E.g., one member of this class of symmetries $V\{f(x), f(U[x])\} = 0$ is discrete self-similarity (or discrete scale invariance).

Keywords: quantum algorithms, hidden subgroup problem, exponential speed-up

Communicated by: I Cirac & R Laflamme

1 Introduction

Shor's striking discovery [1], that quantum computers could accomplish tasks such as factoring large numbers exponentially faster than the best (known) classical methods, motivates the quest for further quantum algorithms exhibiting an exponential speed-up, see, e.g., [2] for a review. Together with a number of black-box problems [3, 4, 5, 6], some of which also admit an exponential speed-up, Shor's algorithm can be generalised to the so-called "hidden subgroup problem": given a function f with the property

$$\forall\, x, y \;:\; f(x) = f(y) \;\leftrightarrow\; y \in U^{\mathbb{Z}} x\,, \tag{1}$$

for some transformation U, find U. I.e., f is constant on the co-sets of the subgroup $\{x, Ux, U^2x, U^3x, \dots\}$ generated by U and assumes a different value at each co-set. (Here we restrict our consideration to the case of one generator U only, for more than one generators, the situation is analogous.) For example, in the case of Shor's algorithm, the transformation U is given by $U[x] = x + p$, and for Simon's [6] problem, it is $U[x] = x \oplus p$ with $\oplus$ denoting the bit-wise addition modulo two, e.g., $1001 \oplus 0101 = 1100$. (Note that $x \oplus p \oplus p = x$.)

[a] email: schuetz@theory.phy.tu-dresden.de
[b] email: unruh@physics.ubc.ca

Hence, in comparison with classical methods, the number of known quantum algorithms which are (as far as we know) significantly faster is tiny – but one might hope that there are many more to be discovered. The question we wish to examine is: which other problems – and perhaps further expansions of the known tasks – could (also) admit an exponential speed-up? More precisely, we shall investigate whether there are general features of problems which are important for an exponentially fast quantum algorithm, and give a specific example (in which such a speed-up is accomplished) via an extension of Simons's and Shor's problem.

In particular we shall consider problems which can be cast into the following form: given a function $f : x \to f(x)$ on an exponential number of arguments x, where f is known to possess some property (from a given class of properties), find that property – where the term "property" can refer to any extracted information in general. Evaluating $f(x)$ on a given arbitrary argument x is assumed to be polynomially (in the length of x) implementable.[c] We shall investigate some features [7] of the class of properties with an (apparently) exponential speed-up by a quantum computer over a classical one. We shall also show how such an exponential speed-up can be achieved for a property we call a hidden symmetry.

Note that our discussion will not be concerned with the use of quantum computation to simulate physical systems, nor with the application of quantum phenomena to transmit information (quantum cryptography or super-dense coding, etc.) or to extract information from an external physical system (such as quantum imaging, see, e.g., [8], or Elitzur-Vaidman-type problems [9]), i.e., we only consider quantum information processing.

2 Relevance of arguments

One aspect which seems [7] to be important for an exponential speed-up is the relevance of the arguments x with respect to the property under consideration.

Typically, sequential [10] quantum algorithms for solving problems as described above can be formulated as black-box algorithms which can be cast into the following most general form

$$|\Psi\rangle = \mathcal{U}_m \, \mathcal{U}_f \, \mathcal{U}_{m-1} \ldots \mathcal{U}_1 \, \mathcal{U}_f \, \mathcal{U}_0 \, |0\rangle \ , \tag{2}$$

where the unitary gate $\mathcal{U}_f$ calculates the (black-box) function f, i.e., $\mathcal{U}_f \, |x\rangle \, |y\rangle = |x\rangle \, |y \oplus f(x)\rangle$, with the possible extension $\mathcal{U}_f \to \mathcal{U}_f \otimes \mathbf{1}$; and additional unitary operations $\mathcal{U}_0 \ldots \mathcal{U}_m$. Even if the algorithm originally contained an intermediate measurement, it could still be rewritten in this form by using ancilla qubits and quantum-controlled operations.

In order to achieve an exponential speed-up the number m as well as the realisations of the unitary operations $\mathcal{U}_0 \ldots \mathcal{U}_m$ have to be polynomial. Consequently, if the number of arguments x of the function $f(x)$ that contain relevant information (for the solution of the problem) is exponentially small, then the part of the output state $|\Psi\rangle$ corresponding to this relevant information is apparently [7] also exponentially small, and therefore impossible to extract with a polynomial number of measurements. Supportive (though not conclusive [7]) to this point is inserting the identity

$$\mathcal{U}_f = (\mathcal{P}_{\text{rel}} + \mathcal{P}_{\text{irr}}) \, \mathcal{U}_f \, (\mathcal{P}_{\text{rel}} + \mathcal{P}_{\text{irr}}) \ , \tag{3}$$

into Eq. (2), where $\mathcal{P}_{\text{rel}}$ and $\mathcal{P}_{\text{irr}}$ denote the (orthogonal) projections onto the subspaces of relevant and irrelevant arguments x, respectively. Assuming that the unitary operations $\mathcal{U}_0 \ldots \mathcal{U}_m$

[c] I.e., the problem to be solved must be at least in *PSPACE* – remember that $P \subseteq NP \subseteq PSPACE$, see, e.g., [2].

do not favour [7] the subspace spanned by $\mathcal{P}_{\rm rel}$ (we do not know in advance which arguments x are going to be important and which not) the norm of (the sum of) all terms containing at least one $\mathcal{P}_{\rm rel}$ is exponentially small for the unitary operations are norm-preserving.

As a result, a function with an exponentially small number of relevant arguments x does not seem suitable for an exponential speed-up. Of course, this feature crucially depends on the particular way of encoding the problem to be solved by a function – e.g., a function defined as $f(x) = 1$ if x is a factor of y and $f(x) = 0$ otherwise would not be the best choice for factoring [11]. One should also bear in mind that the above arguments do not exclude polynomial speed-up – the Grover search routine [12] achieves a quadratic speed-up by exploiting the bilinear structure of quantum theory, i.e., the normalisation by $1/\sqrt{N}$ instead of $1/N$.

The task of period-finding, for example, where all arguments x are equally relevant for the solution, is therefore indeed (as it should be) a good candidate for an exponential speed-up by a quantum algorithm. As counter-examples (which are probably not good candidates for an exponential speed-up), we may quote the usual form of the travelling salesman problem [with x being one particular route and $f(x)$ the associated length] or the task of evaluating the position in chess[d]where *a posteriori* almost all arguments x are completely irrelevant – but we do not know *a priori* which.

3 Excess information

Since every quantum computation is (at least in principle) unitary and hence reversible, it is impossible to lose any information during this process – except by the (final) measurement (e.g., the phases are lost) or by transferring the information from the quantum system (computer) alone to its entanglement with the "environment". We want to extract only a certain property of the function f – other details of f are irrelevant – and, therefore, we have to find a way to dispose of this excess information. For example, in Shor's problem $f(x) = f(x+p)$, we only want to know the period p, and not any other details of f. After the measurement of the register $|f\rangle$ one is left with the state

$$|\Psi\rangle = \frac{1}{\sqrt{L}} \sum_{l=0}^{L-1} |x_0 + lp\rangle \ . \tag{4}$$

This state contains very little information – basically just the starting point x_0 and the period p – which, after a quantum Fourier transform, determine the phase and the value of the wave-number, respectively.

Of course, here we have to explain the phrase "very little information". To this end we introduce the notion of the "classical information of a quantum state $|\Psi\rangle$" as the information required to reproduce the state $|\Psi\rangle$ starting from the state $|0\rangle$ in the computational basis via elementary operations [7]. Note that this notion is obviously not a unitarily invariant (quantum) information measure (as $|\Psi\rangle$ is still a pure state). But since we want to speed up the solution of classical problems, we should consider the involved quantum operations from a classical point of view.

[d]If x denotes one possible continuation of the game (a so-called "line") and $f(x)$ the outcome (win, loss, or draw) then the vast majority of arguments x are irrelevant for accessing the position because almost all lines with random moves are completely uninteresting.

In summary, we arrive at an (admittedly rather vague [7]) additional condition – "not too much excess information" – for a (classical) problem which is supposed to admit an exponential (quantum) speed-up. As a counter-example, we might consider the average invertability check (collision problem) of a function $f(x)$ – i.e., for a given (representative) y in the co-domain, how many x satisfy (in average) $f(x) = y$. (This problem is relevant for cryptography.) Although obviously almost all arguments x are equally important, the state after the measurement of f apparently still contains too much excess information[e](the different and independent coordinates x satisfying $f(x) = y$) to get rid of [14].

4 Hidden symmetries

As one would reasonably expect, the hidden subgroup problem satisfies the above requirements – all arguments x are equally relevant and the state after the measurement of f is basically determined by one starting point x_0 and the generator U (e.g., p) of the subgroup. This feature is ensured by the existence of the symmetry (1) connecting the values of the function f at each two points x and $U[x]$ with a certain relation, i.e., $f(x) = f(U[x])$. In view of the above remarks, one might expect a similar effect for a more general hidden two-point symmetry of the form

$$V\{f(x), f(U[x])\} = 0\,, \tag{5}$$

where V is some relation generalising the equality in the hidden subgroup problem (1).

Of course, it remains to be shown whether it is possible to design a quantum algorithm which determines U and V exponentially faster than classical methods. One of the major benefits of quantum computation is the superposition principle allowing us to test all possible values of x at once ("quantum parallelism"). In view of this observation one would expect that it is advantageous to represent the symmetry operations in a (somehow [7]) linear fashion. (This seems to be much easier for Abelian than for non-Abelian symmetry groups.) For this reason, and for the sake of simplicity, we focus on Simon- and Shor-type symmetries in the following.

5 Simon-type symmetry

As an expansion of Simon's problem with the periodicity condition $f(x \oplus p) = f(x)$ we consider

$$V\{f(x), f(U[x])\} = f(x) \oplus f(x \oplus p) \oplus q = 0 \;\rightarrow\; f(x \oplus p) = f(x) \oplus q\,, \tag{6}$$

with $x, f(x), p, q \in \{0,1\}^n$, and the task is to find out p and q. For convenience, we shall identify bit-strings with integers $\{0,1\}^n \leftrightarrow \{0, \ldots, 2^n - 1\}$ via the usual binary representation in the following. I.e., $x, f(x), p, q$ are treated as integers with $0 \le x, f(x), p, q < N = 2^n$.

[e]Note that our notion "classical information of a quantum state $|\Psi\rangle$" is different from the generalisation of the Kolmogorov complexity to the quantum case introduced in [13]. The latter quantity is bounded from above [13] and its upper bound of approximately $2n$ (where n is the number of qubits) would just correspond to the information contained in x_0 and p for Shors algorithm. In contrast, the "classical information of a quantum state $|\Psi\rangle$" introduced here can exceed this bound by far: For the collision problem, the different and independent coordinates x satisfying $f(x) = y$ typically contain much more information. Hence the generalisation of the Kolmogorov complexity proposed in [13] cannot be used to discriminate between the two cases (Shors algorithm and the collision problem).

In complete analogy to Simon's algorithm we apply the usual trick of inquiring all entries at once (quantum parallelism) and obtain the state

$$|\Psi\rangle = \sum_{\{x_0\}}^{(N/2)} \frac{|x_0\rangle\,|f(x_0)\rangle + |x_0 \oplus p\rangle\,|f(x_0) \oplus q\rangle}{\sqrt{N}} \,. \tag{7}$$

But instead of measuring the second register $|f\rangle$ we now perform a multiple application of the Hadamard gate to both, the first $|x\rangle$ and the second $|f\rangle$ register

$$\mathcal{H}^{(2n)}\,|\Psi\rangle = \frac{2}{\sqrt{N^3}} \sum_{\{x_0\}}^{(N/2)} \sum_{\{Y\,:\,R\cdot Y=0\}}^{(N^2/2)} (-1)^{X\cdot Y}\,|Y\rangle \;, \tag{8}$$

where we have introduced the abbreviations $|X\rangle = |x_0\rangle \otimes |f(x_0)\rangle$ and $|R\rangle = |p\rangle \otimes |q\rangle$ as well as the scalar product modulo two given by

$$R \cdot Y = \sum_{l=0}^{2n} R_l Y_l \bmod 2 = \bigoplus_{l=0}^{n} (p_l Y_l \oplus q_l Y_{n+l}) \;. \tag{9}$$

Assuming that the values $f(x_0)$ are pseudo-randomly distributed, i.e., without any internal order (cf. the next Section), the measurement of Y returns arbitrary values satisfying the constraint $R \cdot Y = 0$. Again in complete analogy to Simon's algorithm, after $\mathcal{O}(n)$ runs we have enough measured values of Y for determining R, i.e., p and q, with arbitrarily high probability (exponential speed-up).

6 Requirements

In which cases can the above quantum algorithm fail, i.e., what exactly does the aforementioned condition "without any internal order" imply?

As a counter-example – where the algorithm must fail – consider the function [15]

$$f(x) = \underline{A} \cdot x \oplus b \,, \tag{10}$$

with a binary $N \times N$-matrix $\underline{A}$ and the bit-wise scalar product modulo two as in Eq. (9). This function exhibits a strong internal order and hence a plethora of symmetries: any p and the corresponding q given by

$$q = \underline{A} \cdot p \,, \tag{11}$$

satisfies Eq. (6).

On the other hand, as an example where the above quantum algorithm works, we might construct the function $f(x)$ as follows: After splitting up the set of all arguments $\{x\} = \{0 \ldots N\}$ into two disjoint sets of equal strength $N/2$ via $\{x_0\}$ and $\{x_0 \oplus p\}$, we assign all $f(x_0)$ random values between 0 and N and determine the remaining ones via $f(x \oplus p) = f(x) \oplus q$. In this rather artificial way we can make sure that there is no additional internal order which could spoil the above algorithm.

In summary, we do not allow additional (exact or average) symmetries apart from the one in Eq. (6) which lead to another value $R' \neq R$ with the probability of measuring $R' \cdot Y = 1$ being strongly suppressed.

Let us discuss the relation of the hidden symmetry discussed above to the hidden sub-group problem. Defining new functions such as [17]

$$h_1(x,y) = f(x) \oplus y\,,\; h_2(x,y) = f(x) \oplus f(y)\,, \tag{12}$$

the symmetry $f(x \oplus p) = f(x) \oplus q$ translates into periodicity

$$h_1(x,y) = h_1(x \oplus p, y \oplus q)\,,\; h_2(x,y) = h_2(x \oplus p, y \oplus p)\,. \tag{13}$$

However, this identification does not imply that the property in Eq. (6) can be mapped onto the hidden sub-group problem as in Eq. (1) because the functions $h_{1,2} : \{1,\ldots,N^2\} \to \{1,\ldots,N\}$ are highly degenerate and hence not distinct on different co-sets.

The fact that one can nevertheless find p (and q) by a quantum algorithm (which is not necessary for such a large degeneracy) is caused by the special underlying symmetry $f(x \oplus p) = f(x) \oplus q$ and the assumption discussed above (no additional internal order). Therefore, this is a true expansion of the hidden sub-group problem [17] with the distinctness on different co-sets being replaced by the pseudo-randomness requirement.

7 Shor-type symmetry

As a second example for a hidden (two-point) symmetry, we study the following expansion of Shor's problem $f(x+p) = f(x)$

$$f(x+p) = f(x) + q\,, \tag{14}$$

with $0 \le x, f(x) < N = 2^n$. Similar to the original period-finding algorithm, we demand that p is much smaller than N, say $p = \mathcal{O}(N^\varepsilon)$ with a small but positive number $0 < \varepsilon < 1$, which will be determined below. In addition, we assume $p \gg q$ (but still $q \gg 1$) – otherwise we would have to insert a "modulo N", i.e., $f(x+p) = f(x) + q \mod N$.

In this situation, the usual superposition state after the application of the unitary gate calculating the function f reads

$$|\Psi\rangle \approx \sum_{x_0=0}^{p-1} \sum_{l=0}^{[N/p]} \frac{|x_0 + lp\rangle\,|f(x_0) + lq\rangle}{\sqrt{N}}\,, \tag{15}$$

where $[N/p]$ denotes the integer part of $N/p \gg 1$ and the $\approx$ sign is caused by the corresponding neglect of a small number of arguments x and the fact that not all periods are complete (remember $p \gg q$).

Again we do not measure the second register at this stage but apply a double quantum Fourier transform, i.e., we Fourier transform each register

$$\mathcal{F}^{(2)}\,|\Psi\rangle \approx \sum_{k_x=0}^{N-1} \sum_{k_y=0}^{N-1} \sum_{x_0=0}^{p-1} \frac{e^{2\pi i (x_0 k_x + f(x_0) k_y)/N}}{\sqrt{N^3}} \sum_{l=0}^{[N/p]} \exp\left\{2\pi i\,\frac{pk_x + qk_y}{N}\,l\right\} |k_x\rangle\,|k_y\rangle\,. \tag{16}$$

Although the measurements of k_x and k_y considered separately typically return almost random numbers – provided that there is no structure (e.g., an additional periodicity, cf. the previous

example as well as Sec. 8) in the values $f(x_0)$ – these numbers k_x and k_y display an extremely strong correlation: the above l-sum exhibits a constructive interference if and only if

$$\frac{pk_x + qk_y}{N} \in \mathbb{N} \pm \mathcal{O}\left(\frac{p}{N}\right) \tag{17}$$

holds; and, accordingly, a large fraction of the measured values for k_x and k_y will obey this relation.

However (in contrast to Shor's algorithm) one measurement of k_x and k_y may not suffice for determining p and q in general. To this end, it might be necessary to repeat the whole process a few times – resulting in pairs of measured values (k_x^a, k_y^a) with a labelling the number of the measurement. One possibility to derive p and q is to find a set of $A \in \mathrm{poly}(n)$ integers $\alpha_a \in \mathbb{Z}$ with $|\alpha_a| < M \ll N$ which satisfy

$$\sum_{a=1}^{A} \alpha_a \, k_y^a \mod N = \mathcal{O}(M) \, . \tag{18}$$

Inserting the above condition back into Eq. (17), we obtain (remember $p \gg q$)

$$\frac{p}{N} \sum_{a=1}^{A} \alpha_a \, k_x^a \in \mathbb{N} \pm \mathcal{O}\left(\frac{ApM}{N}\right) \, . \tag{19}$$

Having eliminated q in this way, we may find p via the continued fraction expansion [2] of

$$\xi = \frac{1}{N} \sum_{a=1}^{A} \alpha_a \, k_x^a \in \frac{\mathbb{N}}{p} \pm \mathcal{O}\left(\frac{AM}{N}\right) \, , \tag{20}$$

provided that the denominator p is small enough, i.e., $p \ll \sqrt{N}/\sqrt{AM}$. There are two limits on the size of the auxiliary number M: firstly, it should be small enough to allow the detection of sufficiently large values of p with $p \ll \sqrt{N}/\sqrt{AM}$, and, secondly, M must be adequately large such that a small number of measured pairs (k_x^a, k_y^a) will allow us to satisfy Eq. (18) with the probability that all of these pairs obey the resonance condition (17) not being exponentially suppressed.

For example, choosing $M = \sqrt{N}$, we may find $A = 2$ numbers $|\alpha_1| < \sqrt{N}$ and $|\alpha_2| < \sqrt{N}$ via the continued fraction expansion of the ratio k_y^1/k_y^2 truncated at order $\sqrt{N}$ which then satisfy $\alpha_2/\alpha_1 + k_y^1/k_y^2 = \mathcal{O}(1/N)$ and thus $\alpha_1 k_y^1 + \alpha_2 k_y^2 = \mathcal{O}(\sqrt{N})$. This allows us to find periods p satisfying $p \ll \sqrt[4]{N}$ in two runs of the quantum algorithm with high probability. Note the difference of the above method to Shor's algorithm which requires $p \ll \sqrt{N}$ instead.

More generally, if $p = \mathcal{O}(N^\varepsilon)$ is small enough (e.g., $\varepsilon < 1/4$, see the above example), we are able to determine p (i.e., U) and thereby also q (i.e., V) in polynomial time (exponential speed-up).

8 Discrete self-similarity

Let us give an example where the above algorithm could be useful. Starting from the Shor-type symmetry $f(x+p) = f(x) + q$ in Eq. (14) and setting

$$f = \log(\phi) \, , \quad x = \log(\chi) \, , \tag{21}$$

with respect to some base(s), we arrive at

$$\phi(\alpha\,\chi) = \beta\,\phi(\chi)\,, \tag{22}$$

i.e., the function $\phi(\chi)$ is discretely self-similar. Discrete self-similarity – also called discrete scale invariance – is a characteristic feature of some non-linear systems (e.g., in condensed matter) exhibiting critical phenomena, see, e.g., [18].

For example, let us assume that the unitary gate $\mathcal{U}_\phi$ represents some characteristic parameter in the quantum simulation of a condensed matter system in the critical régime and that this parameter ϕ displays a discretely self-similar but otherwise chaotic dependence on some input χ. For the sake of simplicity, let us further assume that we can calculate the logarithms of the output ϕ and the input χ with respect to suitable bases within an appropriate discretisation (either artificial or natural, e.g., physical lattice). In this way the accomplished generalisation of pure periodicity $f(x+p) = f(x) \leftrightarrow \phi(\alpha\,\chi) = \phi(\chi)$ to discrete self-similarity in Eq. (22) in the presented quantum algorithm allows us to detect the discretely self-similar behaviour exponentially faster than any (known) classical method.

9 Summary

By means of a simple example, it has been demonstrated that the task of finding hidden (two-point) symmetries of a given function described by Eq. (5) – as an expansion of the hidden subgroup problem in Eq. (1) – can also be accomplished exponentially faster by a (probabilistic) quantum algorithm than by classical methods.

There are two main possibilities for generating *NP*-problems (i.e., the solution is potentially hard to find but easy to verify, at least probabilistically) in this way – either both, $U \leftrightarrow p$ and $V \leftrightarrow q$, are unknown or $V \leftrightarrow q$ is given and we have to find "only" $U \leftrightarrow p$ [16]. (Of course, if p was known, the problem would be trivial.)

Note that the task under consideration is very similar to an inverse problem where the input(s) and the output(s) of a function depending on a parameter are given and one has to find the fitting parameter. We consider the main importance of our result in its being a small step towards the goal of better understanding the class of problems which can be solved exponentially faster by quantum algorithms.

10 Outlook

Eq. (5) does not represent the most general (explicit) two-point symmetry, which can be written as

$$V\,\{x, f(x), f\,(U[x, f(x)])\} = 0\,. \tag{23}$$

In this case there is no f-independent co-set in general and it would be interesting to study the possibilities of speeding up these more complicated (consistency, etc.) problems by quantum algorithms. As another extension of Eq. (5), it appears quite natural to ask about relations involving more, say $(m+1)$, points

$$V\,\{f(x), f(U_1[x]), \ldots, f(U_m[x])\} = 0\,. \tag{24}$$

Further interesting symmetries[f] could include other transformations U and relations V – think of gauge symmetries, for example, or permutations (and other possibly non-Abelian groups).

Another point is that, in the examples considered above (and in the hidden subgroup problem, of course), V was invertible, i.e., one could solve the relation Eq. (5) for $f(x)$. Relaxing this invertability condition would be another interesting object of study. As a very simple example, one might consider the following symmetry

$$\bigoplus_{l=0}^{n} f_l(x) \oplus f_l(x \oplus p) = 0\,, \tag{25}$$

where one can determine p (again assuming appropriate conditions) via defining a new function $F(x) = \bigoplus_{l=0}^{n} f_l(x)$.

Acknowledgements

The authors acknowledge valuable conversations with R. Cleve, P. Høyer, A. Kitaev and R. Laflamme. This work was supported by the Alexander von Humboldt foundation, the Canadian Institute for Advanced Research, the Natural Science and Engineering Research Council of Canada, and the Pacific Institute of Theoretical Physics. R. S. gratefully acknowledges financial support by the Emmy-Noether Programme of the German Research Foundation (DFG) under grant No. SCHU 1557/1-1,2.

References

1. P. W. Shor, SIAM J. Comp. **26**, 1484 (1997).
2. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000); A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi, *Classical and Quantum Computation* (American Mathematical Society, Rhode Island, 2002); see also J. Preskill, *Quantum Computation and Information*, lecture notes, URL: `http://www.theory.caltech.edu/people/preskill/ph229`.
3. D. Deutsch, Proc. R. Soc. Lond. A **400**, 97 (1985).
4. D. Deutsch and R. Jozsa, Proc. R. Soc. Lond. A **439**, 553 (1992).
5. E. Bernstein and U. Vazirani, SIAM J. Comp. **26**, 1411 (1997).
6. D. R. Simon, SIAM J. Comp. **26**, 1474 (1997).
7. As it becomes evident from the character of the arguments, they are still intuitive and suggestive and not mathematically rigorous or conclusive. (Counter-examples are welcome.)
8. A. F. Abouraddy *et al.*, Opt. Express **9**, 498 (2001); Phys. Rev. Lett. **87**, 123602 (2001).
9. A. C. Elitzur and L. Vaidman, Found. Phys. **23**, 987 (1993); see also R. Schützhold, Phys. Rev. A **67**, 062311 (2003) and references therein.
10. I.e., for a given input state $|0\rangle$, after several operations, the solution of the problem is encoded in the output state $|\Psi\rangle$. A different possibility would be to encode the solution of the problem under consideration in the ground state of some given Hamiltonian, see, e.g., G. Castagnoli, A. Ekert,

[f] As one possibility one might consider the case where the operations on the argument ("inside") and on the value of the function ("outside") differ. However, one must be careful: For instance, if one defines the problem as, say, $f(x \oplus p) = f(x) + q$ or $f(x + p) = f(x) \oplus q$, the first case is inconsistent in general since another iteration leads to a contradiction $f(x) = f(x) + 2q$; and the second example can be reduced to Shor's case $f(x + 2p) = f(x)$.

and C. Macchiavello, Int. J. Theo. Phys. **37**, 463 (1998); E. Farhi *et al.*, Science **292**, 472 (2001); A. M. Childs *et al.*, Quant. Inf. Comp. **2**, 181 (2002).

11. It can be shown that, for sufficiently complicated or unstructured functions (in a black box), no exponential speed-up is possible, see, e.g., C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, SIAM J. Comp. **26**, 1510 (1997); as well as Ref. [14].
12. L. Grover, Phys. Rev. Lett. **79**, 325 (1997).
13. Paul M. B. Vitanyi, IEEE Trans. Inform. Theory **47**, 2464 (2001); Proc. 15th IEEE Conf. Computational Complexity, 2000.
14. For the so-called "collision problem" (where the task is to determine whether a given function is one-to-one or two-to-one or r-to-one), it has been shown that no quantum algorithm with an exponential speed-up exists, see, e.g., S. Aaronson, in Proc. 34^{th} ACM Symp. Theory of Computing, Montreal, Canada, May 2002, pp. 635 (`quant-ph/0111102`); and Y. Shi, in Proc. 43^{rd} IEEE Symp. Found. of Comp. Science 2002, pp. 513 (`quant-ph/0112086`).
15. We thank R. Cleve for discussing this aspect and suggesting the above example; R. Cleve, private communications.
16. For a given and invertible V, the property $V\{f(x), f(U[x])\} = 0 \rightarrow f(U[x]) = W\{f(x)\}$ is a special case of the hidden translation (or shift) problem $f(U[x]) = g(x)$. However, there is no (known) general efficient quantum algorithm – only in special cases, e.g., for cyclic groups such as $f(x \oplus p) = g(x)$; see, e.g., K. Friedl *et al.*, `quant-ph/0211091`; W. van Dam, S. Hallgren, and L. Ip, in Proc. ACM-SIAM Symp. Discrete Algorithms 2003 (`quant-ph/0211140`).
17. We thank A. Kitaev for discussing this point, A. Kitaev, private communications.
18. D. Sornette, Phys. Rep. **297**, 239 (1998); see also R. J. Creswick, H. A. Farach, and C. P. Poole, Jr., *Introduction to Renormalization Group Methods in Physics* (Wiley, New York, 1992).