Period finding with adiabatic quantum computation

I. Hen

Information Sciences Institute, University of Southern California - Marina del Rey, CA 90292, USA

received 13 January 2014; accepted in final form 5 March 2014
published online 24 March 2014

PACS 03.67.Ac – Quantum algorithms, protocols, and simulations
PACS 03.67.Lx – Quantum computation architectures and implementations

Abstract – We outline an efficient quantum-adiabatic algorithm that solves Simon’s problem, in which one has to determine the “period”, or xor mask, of a given black-box function. We show that the proposed algorithm is exponentially faster than its classical counterpart and has the same complexity as the corresponding circuit-based algorithm. Together with other related studies, this result supports a conjecture that the complexity of adiabatic quantum computation is equivalent to the circuit-based computational model in a stronger sense than the well-known, proven polynomial equivalence between the two paradigms. We also discuss the importance of the algorithm and its theoretical and experimental implications for the existence of an adiabatic version of Shor’s integer factorization algorithm that would have the same complexity as the original algorithm.

Introduction. – Theoretical research on quantum computing is motivated by the exciting possibility that quantum computers are inherently more efficient than classical computers due to the advantages that the laws of quantum mechanics provide, such as parallelism, tunneling and entanglement. The actual implementation of quantum computing devices is however hindered by many challenging difficulties, the most prominent of which being the control or removal of quantum decoherence [1]. Recent theoretical work [2–4], as well as promising experimental research findings [5–7] in the field of Adiabatic Quantum Computing (AQC) suggest that a leading candidate to be the first device to solve practical classically hard problems using quantum principles is the so-called “quantum annealer”, which implements the simple yet potentially powerful quantum-adiabatic algorithmic approach proposed by Farhi et al. [8] about a decade ago.

Within the Quantum-Adiabatic Algorithm (QAA) approach, the solution to an optimization problem is encoded in the ground state of a “problem” Hamiltonian \( \hat{H}_p \). To find the solution, the system is prepared in the ground state of another “driver” Hamiltonian \( \hat{H}_d \) that must not commute \( \hat{H}_p \) and has a ground state that is fairly easy to prepare. The Hamiltonian of the system is then slowly modified from \( \hat{H}_d \) to \( \hat{H}_p \), using the linear interpolation, i.e., \( \hat{H}(s) = s\hat{H}_p + (1-s)\hat{H}_d \), where \( s(t) \) is a parameter varying smoothly with time from 0 to 1. If this process is done slowly enough, the system will stay close to the ground state of the instantaneous Hamiltonian throughout the evolution [9,10], so that one finally obtains a state close to the ground state of \( \hat{H}_p \). At this point, measuring the state will give the solution of the original problem with high probability. The running time \( T \) of the algorithm determines the efficiency, or complexity, of the QAA and normally scales inversely with a small power of the minimum gap of the system \([8,11]\).

The experimental studies mentioned above, as well as other theoretical work such as the theorem of polynomial equivalence between AQC and circuit-based computing \([12,13]\), provide ample motivation for searching for adiabatic algorithms that would reveal the inherent potential encompassed in AQC. However, despite intensive research (see, e.g., refs. [14–20] and references therein), to date, most attempts aimed at finding practical efficient AQC algorithms have failed.

Valuable insight into why this is so, may be obtained by considering, in the context of AQC, problems for which there are known circuit-based algorithms that exhibit “quantum speedups”. Devising “optimal” adiabatic algorithms for these, that would have the same complexity as their circuit analogues, may reveal important features of AQC that have perhaps not been properly utilized thus far1. Several known examples for adiabatic analogues

1In that respect, the prescription proposed by the polynomial-equivalence theorem [12] may be viewed as “artificial” by construction and impractical for actual implementation. Additionally, it will in general be suboptimal, as it is expected to yield unnecessary polynomial overheads.
to circuit-based algorithms are Grover’s unstructured search problem [21] and Quantum Counting [22], both of which have successfully recovered the quadratic quantum speedups exhibited by their circuit-model counterparts, thereby hinting at the potential power of AQC.

Perhaps the most important class of problems exhibiting quantum speedups is that of the Hidden Subgroup Problem (HSP) [23], which encompasses most of the quantum algorithms found so far that are exponentially faster than their classical counterparts (e.g., period-finding, order-finding and discrete logarithms). In HSPs, one is given a function from a finitely generated group to a finite set. The function is known to be constant on the cosets of a subgroup whose generating set needs to be found. Finding adiabatic algorithms for problems in this class have the same complexities as their circuit-based counterparts, is therefore of considerable importance.

The simplest HSP considered in the context of AQC is the problem of Deutsch and Josza [24], which has been shown to have an $O(1)$ complexity, similarly to the circuit-based result, and is therefore exponentially faster than the deterministically classical algorithm [25] (see also refs. [26,27]). Here, we devise a QAA for a more challenging HSP, namely, Simon’s problem [28], which was the first to exhibit exponential speedup over classical probabilistic algorithms.

In Simon’s problem one is asked to find the “period” of a function from $n$-bit strings to $(n - 1)$-bit strings that is “promised” to be constant only over inputs that are related by an unknown xor mask (the period). Although of a somewhat artificial nature, the significance of Simon’s problem stems from the fact that it shares many similarities with, and in fact was also the motivation for, Shor’s integer factorization algorithm [29], which in itself is based on a “genuine” period-finding problem. A derivation of a quantum-adiabatic integer factorization algorithm that would have the same complexity as Shor’s original circuit, together with the aforementioned significant experimental advancements in the construction and operation of quantum annealers, may have considerable theoretical as well as practical impact and implications in the field of quantum computing and beyond it, as Shor’s algorithm may be used to break the RSA public-key cryptosystem. In that sense, a quantum-adiabatic Simon’s problem algorithm is an important first step towards that goal.

Before we consider the full complexity of Simon’s problem, let us first study the related, albeit simpler, HSP devised by Bernstein and Vazirani (BV) [30]. The algorithm given here will help lay the groundwork for the discussion of the more elaborate algorithm for Simon’s problem.

The Bernstein-Vazirani problem. – In the BV problem, one is given a black box that evaluates the function

$$f(w) = \left( \sum_{k=0}^{n-1} w_k a_k \right) \bmod 2,$$

where $w_k$ and $a_k$ ($k = 0, \ldots, n - 1$) are the bits of the two integers $w$ and $a$, respectively, and the function $f(\cdot)$ takes the integer $w$ into the modulo-2 sum of the products of corresponding bits of $a$ and $w$. The task is to find the integer $a$ with as few queries of $f(\cdot)$ as possible.

While the best classical algorithm to do this requires $n$ queries of $f(\cdot)$ (e.g., with the inputs $w = 2^k$ ($k = 0, \ldots, n - 1$) revealing the bits of $a$ one at a time), quantum circuit-based algorithms have been shown to require $O(1)$ queries to perform the same task [30]. Here, we show that, similarly to the quantum circuit algorithm, there is a corresponding adiabatic algorithm that requires a running time that does not scale with input size.

To show this, we first note that the function $f(\cdot)$ can be encoded as the following problem Hamiltonian:

$$\hat{H}_p = -\frac{1}{2} \sum_{w \in \{0,1\}^n} (|w\rangle\langle w|^A) \otimes \left[ 1 + (-1)^{f(w)} \sigma_z^B \right],$$

$$= - \sum_{w \in \{0,1\}^n} (|w\rangle\langle w|^A) \otimes (|f(w)\rangle\langle f(w)|^B). \quad (2)$$

Here, $\sigma_z$ ($\sigma_x$) denotes a Pauli matrix in the z-direction (x-direction), the letter $(A)$ labels the $n$-bit subspace for the input states $|w\rangle$ and $(B)$ denotes a 1-bit “output” subspace for the outcome $|f(w)\rangle = |0\rangle$ or $|1\rangle$ (the state $|0\rangle$ shall represent a spin pointing in the positive z-direction). For all configurations $|w\rangle$ of the input bits for which $f(w) = 1$, $\hat{H}_p$ has value $-1$ if the output qubit is $|1\rangle$ and $0$ if the output qubit is $|0\rangle$. For all configurations $|w\rangle$ for which $f(w) = 0$, $\hat{H}_p$ has value $-1$ if the output qubit is $|0\rangle$ and $0$ otherwise. Combining both cases, we see that the ground state of $\hat{H}_p$ has energy $-1$ and is $2^n$-fold degenerate: $|w\rangle^A \otimes |f(w)\rangle^B$ for all $w \in \{0,1\}^n$. The action of $\hat{H}_p$ on “classical” configurations $|w\rangle \otimes |0\rangle$ will give an eigen-energy of $-1$ if $f(w) = 0$ and zero otherwise. The above encoding may therefore be considered as the Hermitian analogue of the unitary oracle of the analogous circuit-based problem. It should be noted nonetheless, that as an oracle, the problem Hamiltonian for the Bernstein-Vazirani problem suggested above (as well as that of Simon’s problem discussed next) is not expected to, nor will it be in the general case, easily implementable. This is of course also true for the corresponding classical oracle as well as the unitary oracle of the quantum circuit-model algorithm.

Before moving on to describing a quantum adiabatic algorithm for the BV problem, let us first make the following simple yet important observation. Given a system described by a Hamiltonian of the form $\hat{H} = \sum_w (|w\rangle\langle w|^A) \otimes \hat{H}_w^B$, where $w$ labels basis states in subsystem $(A)$, and an initial state $|\psi(t = 0)\rangle = \sum_w c_w|w\rangle^A \otimes |\psi(t = 0)\rangle^B_w$, where $c_w$ are complex coefficients obeying $\sum_w |c_w|^2 = 1$, the state of the system at time $t$ may be written as $|\psi(t)\rangle = \sum_w c_w|w\rangle^A \otimes |\psi(t)\rangle^B_w$, where $|\psi(t)\rangle^B_w$ is a wave function evolving under $\hat{H}_w^B$. For each state $|w\rangle$ in subsystem $A$, there is an
independently evolving state in subsystem $B$ that is not affected by the evolutions corresponding to other states $|w\rangle$. This statement may be readily verified by plugging $|\psi(t)\rangle$ into the Schrödinger equation for $\hat{H}$. The above "parallelism" will be used in what follows to construct many-qubit adiabatic Hamiltonians that would simultaneously execute a multitude of two-level adiabatically evolving systems. Since the runtime for the evolution of each subsystem will not depend on the size of the entire system, the resultant total evolution will likewise not require a running time that scales with system size. This unusual property [15,18,20] will be key in the construction of the adiabatic BV and Simon’s algorithms, which we address next.

To construct a QAA for the BV problem we shall choose the driver Hamiltonian:

$$\hat{H}_d = \frac{1}{2} \left[ (1)^{(A)} \otimes (1 - \sigma_x)^{(B)} \right]$$

$$= \frac{1}{2} \sum_{w \in \{0, 1\}^n} (|w\rangle\langle w|)^{(A)} \otimes (1 - \sigma_x)^{(B)}. \tag{3}$$

(We shall henceforth omit the subspace labels $(A)$ and $(B)$ in favor of a more compact notation.) The total Hamiltonian can therefore be written as

$$\hat{H} = \sum_{w \in \{0, 1\}^n} |w\rangle\langle w| \otimes \hat{H}_w, \tag{4}$$

where each $\hat{H}_w$ acts only inside the second subspace and, following eqs. (2), (3) and (4), it can be written as

$$\hat{H}_w = \frac{1}{2} \left[ (1 - s)(1 - \sigma_x) - s \left( 1 + (-1)^{f(w)} \sigma_x \right) \right]. \tag{5}$$

Having set up the problem and driver Hamiltonians, the QAA is as follows.

- Step 1: As the initial state, prepare the equal superposition of all computational-basis states

$$|\psi(t = 0)\rangle = \frac{1}{\sqrt{2^n}} \sum_{w \in \{0, 1\}^n} |w\rangle \otimes |+\rangle = |+\rangle \otimes |+\rangle, \tag{6}$$

where $|+\rangle$ denotes the state of all spins of the appropriate subsystem pointing in the positive (negative) $x$-direction (note that this is easily done).

- Step 2: Evolve the system under the Hamiltonian, eq. (4), where $s$, the adiabatic parameter, is varied at a constant rate from $s = 0$ at $t = 0$ to $s = 1$ at $t = T$ for some $n$-independent runtime $T$.

Utilizing the observation made above, the evolution of the total wave function is split into $2^n$ decoupled 1-qubit evolutions, each described by the simple gapped two-level system $\hat{H}_w$, eq. (5), with the initial condition $|\psi(t = 0)\rangle_w = |+\rangle$. Therefore, an appropriately long (but $n$-independent) runtime $T$ will evolve each $|\psi(t = 0)\rangle_w$ into the ground state of the problem Hamiltonian of $\hat{H}_w$, namely, into $|\psi(t = T)\rangle_w = |f(w)\rangle$ with an arbitrarily high accuracy that depends on $T$. It is important to note that there will be no relative phases between the different final states $|f(w)\rangle$. As a result, the final state of the entire system will be

$$|\psi(t = T)\rangle = \frac{1}{\sqrt{2^n}} \sum_{w \in \{0, 1\}^n} |w\rangle \otimes |f(w)\rangle. \tag{7}$$

The above decoupled evolution may be viewed as "adiabatic quantum parallelism" as it describes the (coherent) evolution of many adiabatic systems that evolve in parallel, such that the coherent superposition of the end states may be utilized to extract important information about the system (as is shown in the next step).

- Step 3: At the end of the evolution, perform an $x$-basis measurement of the qubit of the second subsystem. Noting that $|f(w)\rangle$ may be written as

$$|f(w)\rangle = \frac{1}{\sqrt{2}} \left( |+\rangle + (-1)^{f(w)} |-\rangle \right), \tag{8}$$

the measurement will collapse the wave function into one of two states with equal probability:

$$|\psi_+\rangle = \frac{1}{\sqrt{2^n}} \sum_{w \in \{0, 1\}^n} |w\rangle \otimes |+\rangle = |+\rangle \otimes |+\rangle \tag{9}$$

or

$$|\psi_-\rangle = \frac{1}{\sqrt{2^n}} \sum_{w \in \{0, 1\}^n} (-1)^{f(w)} |w\rangle \otimes |-\rangle \tag{10} = \bigotimes_{k=0}^{n-1} \left( |0\rangle + (-1)^{a_k} |1\rangle \right) \otimes |-\rangle.$$

Now, if $|\psi_+\rangle$ is obtained, then one must go back to Step 1 and restart the algorithm, as the resulting state will contain no information about $a$ (in fact, $|\psi_+\rangle$ is the initial state). Otherwise, the resulting state will encode all the bits of $a$, namely $a_k$, each corresponding to a different orientation of the spin along the $x$-axis. The probability that the algorithm would fail after $r$ runs of the QAA is exponentially small, namely, $P_{\text{failure}} = 2^{-r}$ but more importantly, $n$-independent.

We have thus shown that the BV problem can be solved using a quantum-adiabatic algorithm in $O(1)$ runtime, i.e., with complexity that is equivalent to that of the corresponding circuit-based algorithm, which requires only one call to the unitary quantum oracle.

Before moving on, we note here that while the problem Hamiltonian, eq. (2), is diagonal, the state of the system at the end of the adiabatic evolution is a superposition with complexity that is equivalent to that of the corresponding circuit-based algorithm, which requires only one call to the unitary quantum oracle.
of computational-basis states. In practice, this would require a high level of coherence, a property that is sometimes not strictly necessary for other adiabatic quantum computations.

We now turn to address the somewhat more complicated HSP devised by Simon [28], utilizing for that purpose the concepts presented above.

Simon’s problem. – The problem devised by Simon [28] was the first to demonstrate a quantum algorithm solving a black-box problem that is exponentially faster than any probabilistic classical algorithm. In Simon’s problem, we are given a promise that there is an $n$-bit positive integer $a$ such that for any two $n$-bit inputs $w \neq y$, a black-box function $g(\cdot) : \{0,1\}^n \to \{0,1\}^{n-1}$ would output the $(n-1)$-bit integers $g(w) = g(y)$ if and only if $w \oplus y = a$. The symbol $\oplus$ denotes here the bitwise-xor operation. We are then asked to find the “period” (or, “xor mask”) of the function, namely $g(\cdot)$ as possible. While classical algorithms require $O(2^{n/2})$ queries of $g(\cdot)$, Simon [28] devised a circuit-based quantum algorithm that can perform this task with $O(n)$ queries [31].

In the context of QAA, the oracle $g(\cdot)$ can be encoded as the problem Hamiltonian

$$ H_p = \sum_{w \in \{0,1\}^n} |w \rangle \langle w| \otimes \sum_{y \in \{0,1\}^{n-1}} h[y, g(w)] |y \rangle \langle y|, \quad (11) $$

where $h[y, g(w)]$ is the Hamming distance between $y$ and $g(w)$. Here, $y \in \{0,1\}^{n-1}$ labels a bit configuration in the second subsystem. The ground state of the total Hamiltonian is $2^n$-fold degenerate, namely, $|w \rangle \otimes |g(w)\rangle$ for all $w \in \{0,1\}^n$. An alternative and more illuminating way to write $H_p$ would be

$$ \hat{H}_p = \frac{1}{2} \sum_{w \in \{0,1\}^n} |w \rangle \langle w| \otimes \sum_{k=1}^{n-1} \left[ 1 - (-1)^{g_k(w)} \sigma_k^z \right], \quad (12) $$

where $\sigma_k^z$ denotes a Pauli matrix acting on the $k$-th bit of the second subsystem and $g_k(w)$ is the $k$-th bit of $g(w)$. This illustrates the fact that the spins of the second subsystem for each $w$ are not coupled to one another.

Similarly to the BV problem, we shall choose the driver Hamiltonian for Simon’s algorithm to be the transverse-field Hamiltonian on the second subsystem, namely

$$ \hat{H}_d = \frac{1}{2} \left[ \frac{1}{\sqrt{2}} \sum_{k=1}^{n-1} (1 - \sigma_k^z) \right]. \quad (13) $$

The total Hamiltonian can therefore be written as $\hat{H} = \sum_w |w \rangle \langle w| \otimes \hat{H}_w$, where $\hat{H}_w$ acts only on the second subsystem and can be written as

$$ \hat{H}_w = \frac{1}{2} \sum_{k=1}^{n-1} \left[ (1 - s) (1 - \sigma_k^z) + s \left( 1 - (-1)^{g_k(w)} \sigma_k^z \right) \right]. \quad (14) $$

Having constructed the problem and driver Hamiltonians, the algorithm is as follows.

- Step 1: As the initial state, prepare the equal superposition of all computational-basis states:

$$ |\psi(t = 0)\rangle = \frac{1}{\sqrt{2^n}} \sum_{w \in \{0,1\}^n} |w \rangle \otimes |+\rangle = |+\rangle \otimes |+\rangle. \quad (15) $$

- Step 2: Evolve the system using a constant-rate adiabatic evolution for a fixed ($i.e.$, an $n$-independent) amount of time $T$. The Hamiltonians $\hat{H}_w$ are each an uncoupled system of $n$-spins. It should therefore be clear that the wave functions of the $n$-spins will evolve simultaneously and independently into the ground state of the problem Hamiltonian for every $w$ (for an appropriately chosen $T$), yielding $|\psi(t = T)\rangle_w = |g(w)\rangle$. The final state of the entire system will therefore be

$$ |\psi(t = T)\rangle = \frac{1}{\sqrt{2^n}} \sum_{w \in \{0,1\}^n} |w \rangle \otimes |g(w)\rangle = \frac{1}{\sqrt{2^n}} \sum_{w \in \{0,1\}^n} \left( |w\rangle + |w \oplus a\rangle \right) \otimes |g(w)\rangle. \quad (16) $$

- Step 3: A $z$-basis measurement of the second subsystem will collapse the wave function into a state

$$ |\psi_w\rangle = \frac{1}{\sqrt{2}} \left( |w\rangle + |w \oplus a\rangle \right) \otimes |g(w)\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{x \in \{0,1\}^{n-1}} (-1)^{w \cdot x} \left[ 1 + (-1)^{f(x)} \right] |x\rangle \otimes |g(w)\rangle, \quad (17) $$

where $w_*$ is a random bit configuration, $f(\cdot)$ is the BV function, eq. (1), and $|x\rangle$ are $x$-basis states. A subsequent $x$-basis measurement of the first subsystem will, similarly to the circuit-based algorithm, yield a state $|x_\ast\rangle$ whose bit representation is orthogonal to that of $a$ (modulo 2), namely, obeying $f(x) = 0$.

- Step 4: As in the circuit-based model, each time Steps 1 through 3 are repeated, with high probability, a different state $|x\rangle$ that is orthogonal to $a$ will be obtained [31]. The different runs will thus produce $(n-1)$ linear equations in the bits of $a$ that are highly likely to be independent of one another. Solving the resultant system of equations will produce the bits of $a$. The total query complexity of the entire process is therefore $O(n)$, similarly to the circuit-based case.

There is an exponentially small probability that the $(n-1)$ equations will be linearly dependent. In this case, more runs will be needed. Altogether, $n + 20$ runs will normally be sufficient [31].
Summary and conclusions. – We have outlined two quantum-adiabatic algorithms to solve the HSPs proposed by Bernstein and Vazirani [30] and the “period-finding” problem devised by Simon [28]. For the BV problem, an algorithm with an $O(1)$ complexity has been found (in contrast to its $O(n)$ classical counterpart), whereas for Simon’s problem we have devised an efficient $O(n)$ algorithm which is to be contrasted with the exponentially slow classical algorithm. The complexities of both algorithms have been found to be the same as the analogous circuit-based results.

The importance of the algorithm constructions given above, lies in the fact that these do not use the (suboptimal) polynomial-equivalence prescription of “translating” circuit-based algorithms to quantum-adiabatic ones [12]. The adiabatic Simon’s algorithm given here is therefore one of very few “genuine” quantum-adiabatic algorithms that provide an exponential speedup over probabilistic classical algorithms, and with no complexity overhead, thereby exhibiting the full potential power encompassed in AQC.

In addition, along with other recent results comparing circuit-based and adiabatic algorithms [22,25], this study provides further corroboration to a conjecture that suitably constructed quantum-adiabatic algorithms have the same complexities as their circuit-based counterparts. This claim is a stronger statement than the theorem establishing a (weaker) polynomial equivalence [12,13] between the two computing paradigms, and still awaits for practical implications both in the field of quantum computing and well beyond it.

***

We thank Peter Young, Siddharth M. Krishnan, David Gosset and Mohammad Amin for useful comments and discussions.

REFERENCES

[1] Schlosshauer M., Rev. Mod. Phys., 76 (2004) 1267.
[2] Amin M., Averin D. V. and Nesteroff J. A., Phys. Rev. A, 79 (2009) 022107 (arXiv:0708.0384).
[3] Amin M., Trunck C. J. S. and Averin D. V., Phys. Rev. A, 80 (2009) 022303.
[4] Childs A. M., Farhi E. and Preskill J., Phys. Rev. A, 65 (2001) 012322.
[5] McGeoch C. C. and Wang C., Experimental evaluation of an adiabatic quantum system for combinatorial optimization, in Proceedings of the 2013 ACM Conference on Computing Frontiers (ACM) 2013.
[6] Berkley A. J. et al., Phys. Rev. B, 87 (2013) 020502(R).
[7] Johnson M. W. et al., Nature, 473 (2011) 194.
[8] Farhi E., Goldstone J., Gutmann S., Lapan J., Lundgren A. and Preda D., Science, 292 (2001) 472. A longer version of the paper appeared in arXiv:quant-ph/0104129.
[9] Kato T., J. Phys. Soc. Jap., 5 (1951) 435.
[10] Messiah A., Quantum Mechanics (North-Holland, Amsterdam) 1962.
[11] Jansen S., Ruskai M. B. and Selier R., J. Math. Phys., 47 (2007) 102111.
[12] Aharonov D., van Dam W., Kempe J., Landau Z., Lloyd S. and Regev O., SIAM J. Comput., 37 (2007) 166.
[13] Mizel A., Lidar D. A. and Mitchell M., Phys. Rev. Lett., 99 (2007) 070502.
[14] Hogg T., Phys. Rev. A, 67 (2003) 022314.
[15] Farhi E., Goldstone J. and Gutmann S., Quantum adiabatic algorithms versus simulated annealing, arXiv:quant-ph/0201031 (2002).
[16] Farhi E., Goldstone J., Gutmann S. and Nagaj D., Int. J. Quantum Inf., 6 (2008) 503 (arXiv:quant-ph/0512159).
[17] Altshuler B., Krovi H. and Roland J., Adiabatic quantum optimization fails for random instances of NP-complete problems, arXiv:0908.2782v2 (2009).
[18] Young A. P., Knysh S. and Smelyanskiy V. N., Phys. Rev. Lett., 104 (2010) 020502.
[19] Hen I. and Young A. P., Phys. Rev. E, 84 (2011) 061152.
[20] Hen I., Phys. Rev. E, 85 (2012) 036705.
[21] Roland J. and Cerf N. J., Phys. Rev. A, 65 (2002) 042308.
[22] Hen I., How fast can quantum annealers count?, arXiv:1301.4956 (2013).
[23] Lomont C., The hidden subgroup problem - review and open problems, arXiv:quant-ph/0411037 (2004).
[24] Deutsch D. and Josza R., Proc. R. Soc. Lond. A, 439 (1992) 553.
[25] Hen I., J. Phys. A: Math. Theor., 47 (2014) 045305.
[26] Sarandy M. S. and Lidar D. A., Phys. Rev. Lett., 95 (2005) 250503.
[27] Panduranga Rao M. V., Phys. Rev. A, 67 (2003) 052306.
[28] Simon D. R., On the power of quantum computation, in Proceedings of the 35th Annual Symposium on Foundations of Computer Science, edited by Goldwasser S. (IEEE) 1994, pp. 116–123.
[29] Shor P. W., Algorithms for quantum computing: discrete logarithms and factoring, in Proceedings of the 35th Symposium on Foundations of Computer Science, edited by Goldwasser S. (IEEE) 1994, pp. 124–134.
[30] Bernstein E. and Vazirani U., SIAM J. Comput., 26 (1997) 1411.
[31] Mermin N. D., Quantum Computer Science: An Introduction (Cambridge University Press, Cambridge, UK) 2007.