

## REVIEW ARTICLE OPEN

## Quantum algorithms: an overview

Ashley Montanaro<sup>1</sup>

Quantum computers are designed to outperform standard computers by running quantum algorithms. Areas in which quantum algorithms can be applied include cryptography, search and optimisation, simulation of quantum systems and solving large systems of linear equations. Here we briefly survey some known quantum algorithms, with an emphasis on a broad overview of their applications rather than their technical details. We include a discussion of recent developments and near-term applications of quantum algorithms.

npj Quantum Information (2016) 2, 15023; doi:10.1038/npjqi.2015.23; published online 12 January 2016

## INTRODUCTION

A quantum computer is a machine designed to use quantum mechanics to do things which cannot be done by any machine based only on the laws of classical physics. Eventual applications of quantum computing range from breaking cryptographic systems to the design of new medicines. These applications are based on quantum algorithms—algorithms that run on a quantum computer and achieve a speedup, or other efficiency improvement, over any possible classical algorithm. Although large-scale general-purpose quantum computers do not yet exist, the theory of quantum algorithms has been an active area of study for over 20 years. Here we aim to give a broad overview of quantum algorithmics, focusing on algorithms with clear applications and rigorous performance bounds, and including recent progress in the field.

Contrary to a rather widespread popular belief that quantum computers have few applications, the field of quantum algorithms has developed into an area of study large enough that a brief survey such as this cannot hope to be remotely comprehensive. Indeed, at the time of writing the 'Quantum Algorithm Zoo' website cites 262 papers on quantum algorithms.<sup>1</sup> There are now a number of excellent surveys about quantum algorithms,<sup>2–5</sup> and we defer to these for details of the algorithms we cover here, and many more. In particular, we omit all discussion of how the quantum algorithms mentioned work. We will also not cover the important topics of how to actually build a quantum computer<sup>6</sup> (in theory or in practice) and quantum error-correction,<sup>7</sup> nor quantum communication complexity<sup>8</sup> or quantum Shannon theory.<sup>9</sup>

## Measuring quantum speedup

What does it mean to say that a quantum computer solves a problem more quickly than a classical computer? As is typical in computational complexity theory, we will generally consider asymptotic scaling of complexity measures such as runtime or space usage with problem size, rather than individual problems of a fixed size. In both the classical and quantum settings, we measure runtime by the number of elementary operations used by an algorithm. In the case of quantum computation, this can be measured using the quantum circuit model, where a quantum

circuit is a sequence of elementary quantum operations called quantum gates, each applied to a small number of qubits (quantum bits). To compare the performance of algorithms, we use computer science style notation  $O(f(n))$ , which should be interpreted as 'asymptotically upper-bounded by  $f(n)$ '.

We sometimes use basic ideas from computational complexity theory,<sup>10</sup> and in particular the notion of complexity classes, which are groupings of problems by difficulty. See Table 1 for informal descriptions of some important complexity classes. If a problem is said to be complete for a complexity class, then this means that it is one of the 'hardest' problems within that class: it is contained within that class, and every other problem within that class reduces to it.

## THE HIDDEN SUBGROUP PROBLEM AND APPLICATIONS TO CRYPTOGRAPHY

One of the first applications of quantum computers discovered was Shor's algorithm for integer factorisation.<sup>11</sup> In the factorisation problem, given an integer  $N=p \times q$  for some prime numbers  $p$  and  $q$ , our task is to determine  $p$  and  $q$ . The best classical algorithm known (the general number field sieve) runs in time  $\exp(O(\log N)^{1/3}(\log \log N)^{2/3}))$ <sup>12</sup> (in fact, this is a heuristic bound; the best rigorous bound is somewhat higher), while Shor's quantum algorithm solves this problem substantially faster, in time  $O(\log N)^3$ . This result might appear only of mathematical interest, were it not for the fact that the widely used RSA public-key cryptosystem<sup>13</sup> relies on the hardness of integer factorisation. Shor's efficient factorisation algorithm implies that this cryptosystem is insecure against attack by a large quantum computer.

As a more specific comparison than the above asymptotic runtimes, in 2010 Kleinjung *et al.*<sup>14</sup> reported classical factorisation of a 768-bit number, using hundreds of modern computers over a period of 2 years, with a total computational effort of  $\sim 10^{20}$  operations. A detailed analysis of one fault-tolerant quantum computing architecture,<sup>7</sup> making reasonable assumptions about the underlying hardware, suggests that a 2,000-bit number could be factorised by a quantum computer using  $\sim 3 \times 10^{11}$  quantum gates, and approximately a billion qubits, running for just over a

<sup>1</sup>School of Mathematics, University of Bristol, Bristol, UK.

Correspondence: A Montanaro (ashley.montanaro@bristol.ac.uk)

Received 18 August 2015; revised 2 October 2015; accepted 30 October 2015

**Table 1.** Some computational complexity classes of importance in quantum computation

Class	Informal definition
P	Can be solved by a deterministic classical computer in polynomial time
BPP	Can be solved by a probabilistic classical computer in polynomial time
BQP	Can be solved by a quantum computer in polynomial time
NP	Solution can be checked by a deterministic classical computer in polynomial time
QMA	Solution can be checked by a quantum computer in polynomial time

Abbreviation: QMA, Quantum Merlin–Arthur.

‘Polynomial time’ is short for ‘in time polynomial in the input size’.

day at a clock rate of 10 MHz. This is clearly beyond current technology, but does not seem unrealistic as a long-term goal.

Shor’s approach to integer factorisation is based on reducing the task to a special case of a mathematical problem known as the hidden subgroup problem (HSP)<sup>15,16</sup> then giving an efficient quantum algorithm for this problem. The HSP is parametrised by a group  $G$ , and Shor’s algorithm solves the case  $G=\mathbb{Z}$ . Efficient solutions to the HSP for other groups  $G$  turn out to imply efficient algorithms to break other cryptosystems; we summarise some important cases of the HSP and some of their corresponding cryptosystems in Table 2. Two particularly interesting cases of the HSP for which polynomial-time quantum algorithms are not currently known are the dihedral and symmetric groups. A polynomial-time quantum algorithm for the former case would give an efficient algorithm for finding shortest vectors in lattices;<sup>17</sup> an efficient quantum algorithm for the latter case would give an efficient test for isomorphism of graphs (equivalence under relabelling of vertices).

## SEARCH AND OPTIMISATION

One of the most basic problems in computer science is unstructured search. This problem can be formalised as follows:

**Unstructured search problem:** Given the ability to evaluate a function  $f:\{0, 1\}^n \rightarrow \{0, 1\}$ , find  $x$  such that  $f(x)=1$ , if such an  $x$  exists; otherwise, output ‘not found’.

It is easy to see that, with no prior information about  $f$ , any classical algorithm, which solves the unstructured search problem with certainty must evaluate  $f$   $N=2^n$  times in the worst case. Even if we seek a randomised algorithm which succeeds, say, with probability  $1/2$  in the worst case, then the number of evaluations required is of order  $N$ . However, remarkably, there is a quantum algorithm due to Grover,<sup>18</sup> which solves this problem using  $O(\sqrt{N})$  evaluations of  $f$  in the worst case (Grover’s original algorithm solved the special case where the solution is unique; the extension to multiple solutions came slightly later.<sup>19</sup>) The algorithm is bounded error; that is, it fails with probability  $\epsilon$ , for arbitrarily small (but fixed)  $\epsilon > 0$ . Although  $f$  may have some kind of internal structure, Grover’s algorithm does not use this at all; we say that  $f$  is used as an oracle or black box in the algorithm.

Grover’s algorithm can immediately be applied to any problem in the complexity class NP. This class encapsulates decision problems whose solutions can be checked efficiently, in the following sense: there exists an efficient classical checking algorithm  $\mathcal{A}$  such that, for any instance of the problem where the answer should be ‘yes’, there is a certificate that can be input to  $\mathcal{A}$  such that  $\mathcal{A}$  accepts the certificate. In other words, a certificate is a proof that the answer is ‘yes’, which can be checked by  $\mathcal{A}$ . On the other hand, for any instance where the answer should be ‘no’, there should be no certificate that can make  $\mathcal{A}$

accept it. The class NP encompasses many important problems involving optimisation and constraint satisfaction.

Given a problem in NP that has a certificate of length  $m$ , by applying Grover’s algorithm to  $\mathcal{A}$  and searching over all possible certificates, we obtain an algorithm which uses time  $O(2^{m/2}\text{poly}(m))$ , rather than the  $O(2^m\text{poly}(m))$  used by classical exhaustive search over all certificates. This (nearly) quadratic speedup is less marked than the super-polynomial speedup achieved by Shor’s algorithm, but can still be rather substantial. Indeed, if the quantum computer runs at approximately the same clock speed as the classical computer, then this implies that problem instances of approximately twice the size can be solved in a comparable amount of time.

As a prototypical example of this, consider the fundamental NP-complete circuit satisfiability problem (Circuit SAT), which is illustrated in Figure 1. An instance of this problem is a description of an electronic circuit comprising AND, OR and NOT gates which takes  $n$  bits as input and produces 1 bit of output. The task is to determine whether there exists an input to the circuit such that the output is 1. Algorithms for Circuit SAT can be used to solve a plethora of problems related to electronic circuits; examples include design automation, circuit equivalence and model checking.<sup>20</sup> The best classical algorithms known for Circuit SAT run in worst-case time of order  $2^n$  for  $n$  input variables, i.e., not significantly faster than exhaustive search.<sup>21</sup> By applying Grover’s algorithm to the function  $f(x)$  which evaluates the circuit on input  $x \in \{0, 1\}^n$ , we immediately obtain a runtime of  $O(2^{n/2}\text{poly}(n))$ , where the  $\text{poly}(n)$  comes from the time taken to evaluate the circuit on a given input.

## Amplitude amplification

Grover’s algorithm speeds up the naive classical algorithm for unstructured search. Quantum algorithms can also accelerate more complicated classical algorithms.

**Heuristic search problem:** Given the ability to execute a probabilistic ‘guessing’ algorithm  $\mathcal{A}$ , and a ‘checking’ function  $f$ , such that  $\Pr[\mathcal{A} \text{ outputs } w \text{ such that } f(w)=1] = \epsilon$ , output  $w$  such that  $f(w)=1$ .

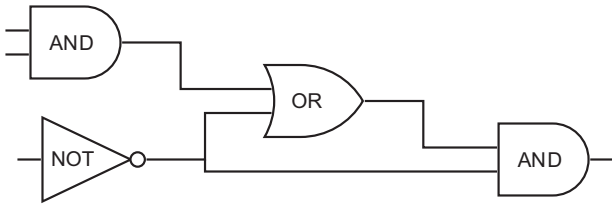
One way to solve the heuristic search problem classically is simply to repeatedly run  $\mathcal{A}$  and check the output each time using  $f$ , which would result in an average of  $O(1/\epsilon)$  evaluations of  $f$ . However, a quantum algorithm due to Brassard, Høyer, Mosca and Tapp<sup>22</sup> can find  $w$  such that  $f(w)=1$  with only  $O(1/\sqrt{\epsilon})$  uses of  $f$ , and failure probability arbitrarily close to 0, thus achieving a quadratic speedup. This algorithm is known as amplitude amplification, by analogy with classical probability amplification.

The unstructured search problem discussed above fits into this framework, by simply taking  $\mathcal{A}$  to be the algorithm, which outputs a uniformly random  $n$ -bit string. Further, if there are  $k$  inputs

**Table 2.** Some problems which can be expressed as hidden subgroup problems

Problem	Group	Complexity	Cryptosystem
Factorisation	$\mathbb{Z}$	Polynomial <sup>11</sup>	RSA
Discrete log	$\mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$	Polynomial <sup>11</sup>	Diffie-Hellman, DSA,...
Elliptic curve discrete log	Elliptic curve	Polynomial <sup>92</sup>	ECDH, ECDSA,...
Principal ideal	$\mathbb{R}$	Polynomial <sup>93</sup>	Buchmann-Williams
Shortest lattice vector	Dihedral group	Subexponential <sup>94,95</sup>	NTRU, Ajtai-Dwork,...
Graph isomorphism	Symmetric group	Exponential	—

The table lists the time complexity of the best quantum algorithms known for the HSPs and the cryptosystems that are (or would be) broken by polynomial-time algorithms.



**Figure 1.** An instance of the Circuit SAT problem. The answer should be ‘yes’ as there exists an input to the circuit such that the output is 1.

$w \in \{0, 1\}^n$  such that  $f(w) = 1$ , then

$$\Pr[\mathcal{A} \text{ outputs } w \text{ such that } f(w) = 1] = \frac{k}{N},$$

so we can find a  $w$  such that  $f(w) = 1$  with  $O(\sqrt{N/k})$  queries to  $f$ . However, we could imagine  $\mathcal{A}$  being a more complicated algorithm or heuristic targeted at a particular problem we would like to solve. For example, one of the most efficient classical algorithms known for the fundamental NP-complete constraint satisfaction problem 3-SAT is randomised and runs in time  $O((4/3)^n \text{poly}(n))$ .<sup>23</sup> Amplitude amplification can be applied to this algorithm to obtain a quantum algorithm with runtime  $O((4/3)^{n/2} \text{poly}(n))$ , illustrating that quantum computers can speedup non-trivial classical algorithms for NP-complete problems.

An interesting future direction for quantum algorithms is finding accurate approximate solutions to optimisation problems. Recent work of Farhi, Goldstone and Gutmann<sup>24</sup> gave the first quantum algorithm for a combinatorial task (simultaneously satisfying many linear equations of a certain form) which outperformed the best efficient classical algorithm known in terms of accuracy; in this case, measured by the fraction of equations satisfied. This inspired a more efficient classical algorithm for the same problem,<sup>25</sup> leaving the question open of whether quantum algorithms for optimisation problems can substantially outperform the accuracy of their classical counterparts.

#### Applications of Grover’s algorithm and amplitude amplification

Grover’s algorithm and amplitude amplification are powerful subroutines, which can be used as part of more complicated quantum algorithms, allowing quantum speedups to be obtained for many other problems. We list just a few of these speedups here.

1. Finding the minimum of an unsorted list of  $N$  integers (equivalently, finding the minimum of an arbitrary and initially unknown function  $f: \{0, 1\}^n \rightarrow \mathbb{Z}$ ). A quantum algorithm due to Dürr and Høyer<sup>26</sup> solves this problem with  $O(\sqrt{N})$  evaluations of  $f$ , giving a quadratic speedup over classical algorithms. Their algorithm is based on applying Grover’s algorithm to a function  $g: \{0, 1\}^n \rightarrow \{0, 1\}$  defined by  $g(x) = 1$ , if and only if  $f(x) < T$  for

some threshold  $T$ . This threshold is initially random, and then updated as inputs  $x$  are found such that  $f(x)$  is below the threshold.

2. Determining graph connectivity. To determine whether a graph on  $N$  vertices is connected requires time of order  $N^2$  classically in the worst case. Dürr, Heiligman, Høyer and Mhalla<sup>27</sup> give a quantum algorithm which solves this problem in time  $O(N^{3/2})$ , up to logarithmic factors, as well as efficient algorithms for some other graph-theoretic problems (strong connectivity, minimum spanning tree, shortest paths).
3. Pattern matching, a fundamental problem in text processing and bioinformatics. Here the task is to find a given pattern  $P$  of length  $M$  within a text  $T$  of length  $N$ , where the pattern and the text are strings over some alphabet. Ramesh and Vinay have given a quantum algorithm<sup>28</sup> which solves this problem in time  $O(\sqrt{N} + \sqrt{M})$ , up to logarithmic factors, as compared with the best possible classical complexity  $O(N+M)$ . These are both worst-case time bounds, but one could also consider an average-case setting where the text and pattern are both picked at random. Here the quantum speedup is more pronounced: there is a quantum algorithm which combines amplitude amplification with ideas from the dihedral hidden subgroup problem and runs in time  $O(\sqrt{N/M} 2^{O(\sqrt{\log M})})$  up to logarithmic factors, as compared with the best possible classical runtime  $O(N/M + \sqrt{N})$ .<sup>29</sup> This is a super-polynomial speedup when  $M$  is large.

#### Adiabatic optimisation

An alternative approach to quantum combinatorial optimisation is provided by the quantum adiabatic algorithm.<sup>30</sup> The adiabatic algorithm can be applied to any constraint satisfaction problem (CSP) where we are given a sequence of constraints applied to some input bits, and are asked to output an assignment to the input bits, which maximises the number of satisfied constraints. Many such problems are NP-complete and of significant practical interest. The basic idea behind the algorithm is physically motivated, and based around a correspondence between CSPs and physical systems. We start with a quantum state that is the uniform superposition over all possible solutions to the CSP. This is the ground (lowest energy) state of a Hamiltonian that can be prepared easily. This Hamiltonian is then gradually modified to give a new Hamiltonian whose ground state encodes the solution maximising the number of satisfied constraints. The quantum adiabatic theorem guarantees that if this process is carried out slowly enough, the system will remain in its ground-state throughout; in particular, the final state gives an optimal solution to the CSP. The key phrase here is ‘slowly enough’; for some instances of CSPs on  $n$  bits, the time required for this evolution might be exponential in  $n$ .

Unlike the algorithms described in the rest of this survey, the adiabatic algorithm lacks general, rigorous worst-case upper

bounds on its runtime. Although numerical experiments can be carried out to evaluate its performance on small instances,<sup>31</sup> this rapidly becomes infeasible for larger problems. One can construct problem instances on which the standard adiabatic algorithm provably takes exponential time;<sup>32,33</sup> however, changing the algorithm can evade some of these arguments.<sup>34,35</sup>

The adiabatic algorithm can be implemented on a universal quantum computer. However, it also lends itself to direct implementation on a physical system whose Hamiltonian can be varied smoothly between the desired initial and final Hamiltonians. The most prominent exponent of this approach is the company D-Wave Systems, which has built large machines designed to implement this algorithm,<sup>36</sup> with the most recent such machine ('D-Wave 2X') announced as having up to 1,152 qubits. For certain instances of CSPs, these machines have been demonstrated to outperform classical solvers running on a standard computer,<sup>37,38</sup> although the speedup (or otherwise) seems to have a rather subtle dependence on the problem instance, classical solver compared, and measure of comparison.<sup>38,39</sup>

As well as the theoretical challenges to the adiabatic algorithm mentioned above, there are also some significant practical challenges faced by the D-Wave system. In particular, these machines do not remain in their ground state throughout, but are in a thermal state above absolute zero. Because of this, the algorithm actually performed has some similarities to classical simulated annealing, and is hence known as 'quantum annealing'. It is unclear at present whether a quantum speedup predicted for the adiabatic algorithm would persist in this setting.

## QUANTUM SIMULATION

In the early days of classical computing, one of the main applications of computer technology was the simulation of physical systems (such applications arguably go back at least as far as the Antikythera mechanism from the 2nd century BC.). Similarly, the most important early application of quantum computers is likely to be the simulation of quantum systems.<sup>40–42</sup> Applications of quantum simulation include quantum chemistry, superconductivity, metamaterials and high-energy physics. Indeed, one might expect that quantum simulation would help us understand any system where quantum mechanics has a role.

The word 'simulation' can be used to describe a number of problems, but in quantum computation is often used to mean the problem of calculating the dynamical properties of a system. This can be stated more specifically as: given a Hamiltonian  $H$  describing a physical system, and a description of an initial state  $|\psi\rangle$  of that system, output some property of the state  $|\psi_t\rangle = e^{-iHt}|\psi\rangle$  corresponding to evolving the system according to that Hamiltonian for time  $t$ . As all quantum systems obey the Schrödinger equation, this is a fundamentally important task; however, the exponential complexity of completely describing general quantum states suggests that it should be impossible to

achieve efficiently classically, and indeed no efficient general classical algorithm for quantum simulation is known. This problem originally motivated Feynman to ask whether a quantum computer could efficiently simulate quantum mechanics.<sup>43</sup>

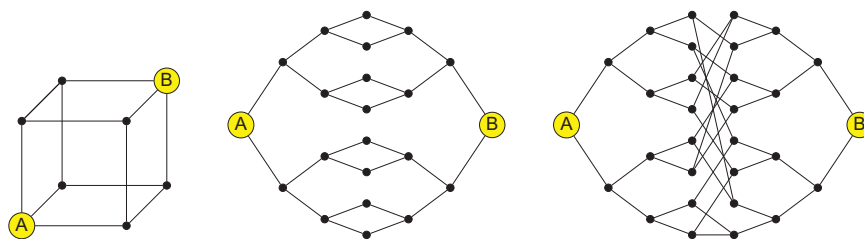
A general-purpose quantum computer can indeed efficiently simulate quantum mechanics in this sense for many physically realistic cases, such as systems with locality restrictions on their interactions.<sup>44</sup> Given a description of a quantum state  $|\psi\rangle$ , a description of  $H$ , and a time  $t$ , the quantum simulation algorithm produces an approximation to the state  $|\psi_t\rangle$ . Measurements can then be performed on this state to determine quantities of interest about it. The algorithm runs in time polynomial in the size of the system being simulated (the number of qubits) and the desired evolution time, giving an exponential speedup over the best general classical algorithms known. However, there is still room for improvement and quantum simulation remains a topic of active research. Examples include work on increasing the accuracy of quantum simulation while retaining a fast runtime;<sup>45</sup> optimising the algorithm for particular applications such as quantum chemistry;<sup>46</sup> and exploring applications to new areas such as quantum field theory.<sup>47</sup>

The above, very general, approach is sometimes termed digital quantum simulation: we assume we have a large-scale, general-purpose quantum computer and run the quantum simulation algorithm on it. By contrast, in analogue quantum simulation we mimic one physical system directly using another. That is, if we would like to simulate a system with some Hamiltonian  $H$ , then we build another system that can be described by a Hamiltonian approximating  $H$ . We have gained something by doing this if the second system is easier to build, to run or to extract information from than the first. For certain systems analogue quantum simulation may be significantly easier to implement than digital quantum simulation, at the expense of being less flexible. It is therefore expected that analogue simulators outperforming their classical counterparts will be implemented first.<sup>40</sup>

## QUANTUM WALKS

In classical computer science the concept of the random walk or Markov chain is a powerful algorithmic tool, and is often applied to search and sampling problems. Quantum walks provide a similarly powerful and general framework for designing fast quantum algorithms. Just as a random walk algorithm is based on the simulated motion of a particle moving randomly within some underlying graph structure, a quantum walk is based on the simulated coherent quantum evolution of a particle moving on a graph.

Quantum walk algorithms generally take advantage of one of two ways in which quantum walks outperform random walks: faster hitting (the time taken to find a target vertex from a source vertex), and faster mixing (the time taken to spread out over all vertices after starting from one source vertex). For some graphs, hitting time of quantum walks can be exponentially less than their classical counterparts.<sup>48,49</sup> The separation between quantum and



**Figure 2.** Three graphs for whose natural generalisations to  $N$  vertices a classical random walk requires exponentially more time than a quantum walk to reach the exit (B) from the entrance (A). However, on the first two graphs there exist efficient classical algorithms to find the exit which are not based on a random walk.



classical mixing time can be quadratic, but no more than this<sup>50</sup> (approximately). Nevertheless, fast mixing has proven to be a very useful tool for obtaining general speedups over classical algorithms.

Figure 2 illustrates special cases of three families of graphs for which quantum walks display faster hitting than random walks: the hypercube, the ‘glued trees’ graph, and the ‘glued trees’ graph with a random cycle added in the middle. This third example is of particular interest because quantum walks can be shown to outperform any classical algorithm for navigating the graph, even one not based on a random walk. A continuous-time quantum walk that starts at the entrance (on the left-hand side) and runs for time  $O(\log N)$  finds the exit (on the right-hand side) with probability at least  $1/\text{poly}(\log N)$ . However, any classical algorithm requires time of order  $N^{1/6}$  to find the exit.<sup>51</sup> Intuitively, the classical algorithm can progress quickly at first, but then gets ‘stuck’ in the random part in the middle of the graph. The coherence and symmetry of the quantum walk make it essentially blind to this randomness, and it efficiently progresses from the left to the right.

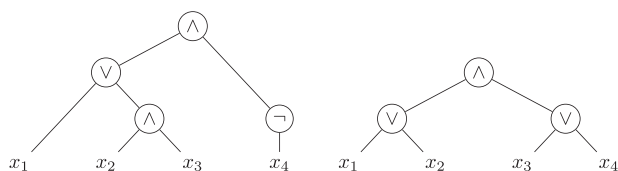
A possibly surprising application of quantum walks is fast evaluation of boolean formulae. A boolean formula on  $N$  binary inputs  $x_1, \dots, x_N$  is a tree whose internal vertices represent AND ( $\wedge$ ), OR ( $\vee$ ) or NOT ( $\neg$ ) gates applied to their child vertices, and whose  $N$  leaves are labelled with the bits  $x_1, \dots, x_N$ . Two such formulae are illustrated in Figure 3. There is a quantum algorithm which allows any such formula to be evaluated in slightly more than  $O(N^{1/2})$  operations,<sup>52</sup> while it is known that for a wide class of boolean formulae, any randomised classical algorithm requires time of order  $N^{0.753\dots}$  in the worst case.<sup>53</sup> The quantum algorithm is based around the use and analysis of a quantum walk on the tree graph corresponding to the formula’s structure. A particularly interesting special case of the formula evaluation problem which displays a quantum speedup is evaluating AND–OR trees, which corresponds to deciding the winner of certain two-player games.

Quantum walks can also be used to obtain a very general speedup over classical algorithms based on Markov chains. A discrete-time Markov chain is a stochastic linear map defined in terms of its transition matrix  $\mathbf{P}$ , where  $P_{xy}$  is the probability of transitioning from state  $x$  to state  $y$ . Many classical search algorithms can be expressed as simulating a Markov chain for a certain number of steps, and checking whether a transition is made to a ‘marked’ element for which we are searching. A key parameter that determines the efficiency of this classical algorithm is the spectral gap  $\delta$  of the Markov chain (i.e., the difference between the largest and second-largest eigenvalues of  $\mathbf{P}$ ).

There are analogous algorithms based on quantum walks, which improve the dependence on  $\delta$  quadratically, from  $1/\delta$  to  $1/\sqrt{\delta}$ .<sup>54–56</sup> This framework has been used to obtain quantum speedups for a variety of problems,<sup>4</sup> ranging from determining whether a list of integers are all distinct<sup>54</sup> to finding triangles in graphs.<sup>57</sup>

### SOLVING LINEAR EQUATIONS AND RELATED TASKS

A fundamental task in mathematics, engineering and many areas of science is solving systems of linear equations. We are given an



**Figure 3.** Two boolean formulae on 4 bits. For  $x_1 = 1, x_2 = x_3 = x_4 = 0$ , for example, the first formula evaluates to 1 and the second to 0. The second formula is an AND–OR tree.

$N \times N$  matrix  $\mathbf{A}$ , and a vector  $\mathbf{b} \in \mathbb{R}^N$ , and are asked to output  $x$  such that  $\mathbf{A}x = \mathbf{b}$ . This problem can be solved in time polynomial in  $N$  by straightforward linear-algebra methods such as Gaussian elimination. Can we do better than this? This appears difficult, because even to write down the answer  $x$  would require time of order  $N$ . The quantum algorithm of Harrow, Hassidim and Lloyd<sup>58</sup> (HHL) for solving systems of linear equations sidesteps this issue by ‘solving’ the equations in a peculiarly quantum sense: given the ability to create the quantum state  $|b\rangle = \sum_{i=1}^N b_i|i\rangle$ , and access to  $\mathbf{A}$ , the algorithm outputs a state approximately proportional to  $|x\rangle = \sum_{i=1}^N x_i|i\rangle$ . This is an  $N$ -dimensional quantum state, which can be stored in  $O(\log N)$  qubits.

The algorithm runs efficiently, assuming that the matrix  $\mathbf{A}$  satisfies some constraints. First, it should be sparse—each row should contain at most  $d$  elements, for some  $d \ll N$ . We should be given access to  $\mathbf{A}$  via an function to which we can pass a row number  $r$  and an index  $i$ , with  $1 \leq i \leq d$ , and which returns the  $i$ ’th nonzero element in the  $r$ ’th row. Also, the condition number  $\kappa = \|\mathbf{A}^{-1}\| \|\mathbf{A}\|$ , a parameter measuring the numerical instability of  $\mathbf{A}$ , should be small. Assuming these constraints,  $|x\rangle$  can be approximately produced in time polynomial in  $\log N$ ,  $d$  and  $\kappa$ .<sup>58,59</sup> If  $d$  and  $\kappa$  are small, then this is an exponential improvement on standard classical algorithms. Indeed, one can even show that achieving a similar runtime classically would imply that classical computers could efficiently simulate any polynomial-time quantum computation.<sup>58</sup>

Of course, rather than giving as output the entirety of  $x$ , the algorithm produces an  $N$ -dimensional quantum state  $|x\rangle$ ; to output the solution  $x$  itself would then involve making many measurements to completely characterise the state, requiring time of order  $N$  in general. However, we may not be interested in the entirety of the solution, but rather in some global property of it. Such properties can be determined by performing measurements on  $|x\rangle$ . For example, the HHL algorithm allows one to efficiently determine whether two sets of linear equations have the same solution,<sup>59</sup> as well as many other simple global properties.<sup>60</sup>

The HHL algorithm is likely to find applications in settings where the matrix  $\mathbf{A}$  and the vector  $\mathbf{b}$  are generated algorithmically, rather than being written down explicitly. One such setting is the finite element method (FEM) in engineering. Recent work by Clader, Jacobs and Sprouse has shown that the HHL algorithm, when combined with a preconditioner, can be used to solve an electromagnetic scattering problem via the FEM.<sup>60</sup> The same algorithm, or closely related ideas, can also be applied to problems beyond linear equations themselves. These include solving large systems of differential equations,<sup>61,62</sup> data fitting<sup>63</sup> and various tasks in machine learning.<sup>64</sup> It should be stressed that in all these cases the quantum algorithm ‘solves’ these problems in the same sense as the HHL algorithm solves them: it starts with a quantum state and produces a quantum state as output. Whether this is a reasonable definition of ‘solution’ depends on the application, and again may depend on whether the input is produced algorithmically or is provided explicitly as arbitrary data.<sup>65</sup>

### FEW-QUBIT APPLICATIONS AND EXPERIMENTAL IMPLEMENTATIONS

Although progress in experimental quantum computation has been rapid, there is still some way to go before we have a large-scale, general-purpose quantum computer, with current implementations consisting of only a few qubits. Any quantum computation operating on at most 20–30 qubits in the standard quantum circuit model can be readily simulated on a modern classical computer. Therefore, existing implementations of quantum algorithms should usually be seen as proofs of principle rather than demonstrating genuine speedups over the classical state of the art. In Table 3 we highlight some experimental

**Table 3.** Some proof-of-concept experimental implementations of quantum algorithms

Algorithm	Technology	Problem solved
Shor's algorithm	Bulk optics <sup>96</sup>	Factorisation of 21
Grover's algorithm	NMR <sup>97</sup>	Unstructured search, $N=8$
Quantum annealing	D-Wave 2X <sup>38</sup>	Ising model on a 'Chimera' graph with 1097 vertices
HHL algorithm	Bulk optics, <sup>98,99</sup> NMR <sup>100</sup>	$2 \times 2$ system of linear equations

Abbreviations: HHL, Harrow, Hassidim and Lloyd; NMR, nuclear magnetic resonance.

Table only includes some 'largest' problem instances solved thus far.

implementations of algorithms discussed here, focusing on the largest problem sizes considered thus far (although note that one has to be careful when using 'problem size' as a proxy for 'difficulty in solving on a quantum computer'.<sup>66</sup>).

An important algorithm omitted from this table is quantum simulation. This topic has been studied since the early days of quantum computation (with perhaps the first implementation dating from 1999<sup>67</sup>, and quantum simulations have now been implemented, in some form, on essentially every technological platform for quantum computing. One salient example is the use of a 6-qubit ion trap system<sup>68</sup> to implement general digital quantum simulation; we defer to survey papers<sup>40,42,69,70</sup> for many further references. It is arguable that quantum simulations, in the sense of measuring the properties of a controllable quantum system, have already been performed that are beyond the reach of current classical simulation techniques.<sup>71</sup>

One application of digital quantum simulation which is currently the object of intensive study is quantum chemistry.<sup>46,72,73</sup> Classical techniques for molecular simulation are currently limited to molecules with 50–70 spin orbitals.<sup>72</sup> As each spin orbital corresponds to a qubit in the quantum simulation algorithm, a quantum computer with as few as 100 logical qubits could perform calculations beyond the reach of classical computation. The challenge in this context is optimising the simulation time; although polynomial in the number of orbitals, this initially seemed prohibitively long,<sup>73</sup> but was rapidly improved via detailed analysis.<sup>72</sup>

The demonstration of quantum algorithms which outperform classical computation in the more immediate future is naturally of considerable interest. The Boson Sampling problem was designed specifically to address this.<sup>74</sup> Boson Sampling is the problem of sampling from the probability distribution obtained by feeding  $n$  photons through a linear-optical network on  $m$  modes, where  $m \gg n$ . This task is conjectured to be hard for a classical computer to solve.<sup>74</sup> However, Boson Sampling can be performed easily using linear optics, and indeed several small-scale experimental demonstrations with a few photons have already been carried out.<sup>75</sup> Although Boson Sampling was not originally designed with practical applications in mind, subsequent work has explored connections to molecular vibrations and vibronic spectra.<sup>76,77</sup>

One way in which quantum algorithms can be profitably applied for even very small-scale systems is 'quantum algorithmic thinking': applying ideas from the design of quantum algorithms to physical problems. An example of this from the field of quantum metrology is the development of high-precision quantum measurement schemes based on quantum phase estimation algorithms.<sup>78</sup>

## ZERO-QUBIT APPLICATIONS

We finally mention some ways in which quantum computing is useful now, without the need for an actual large-scale quantum computer. These can be summarised as the application of ideas from the theory of quantum computation to other scientific and mathematical fields.

First, the field of Hamiltonian complexity aims to characterise the complexity of computing quantities of interest about quantum-mechanical systems. A prototypical example, and a fundamental task in quantum chemistry and condensed-matter physics, is the problem of approximately calculating the ground-state energy of a physical system described by a local Hamiltonian. It is now known that this problem—along with many others—is Quantum Merlin–Arthur (QMA)-complete.<sup>79,80</sup> Problems in the class QMA are those which can be efficiently solved by a quantum computer given access to a quantum 'certificate'. We imagine that the certificate is produced by an all-powerful (yet untrustworthy) wizard Merlin, and given to a polynomial-time human Arthur to check; hence Quantum Merlin–Arthur. Classically, if a problem is proven NP-complete, then this is considered as good evidence that there is no efficient algorithm to solve it. Similarly, QMA-complete problems are considered unlikely to have efficient quantum (or classical) algorithms. One can even go further than this, and attempt to characterise for which families of physical systems calculating ground-state energies is hard, and for which the problem is easy.<sup>29,81</sup> Although this programme is not yet complete, it has already provided some formal justification for empirical observations in condensed-matter physics about relative hardness of these problems.

Second, using the model of quantum information as a mathematical tool can provide insight into other problems of a purely classical nature. For example, a strong lower bound on the classical communication complexity of the inner product function can be obtained based on quantum information-theoretic principles.<sup>82</sup> Ideas from quantum computing have also been used to prove new limitations on classical data structures, codes and formulae.<sup>83</sup>

## OUTLOOK

We have described a rather large number of quantum algorithms, solving a rather large number of problems. However, one might still ask why more algorithms are not known—and in particular, more exponential speedups?

One reason is that strong lower bounds have been proven on the power of quantum computation in the query complexity model, where one considers only the number of queries to the input as the measure of complexity. For example, the complexity achieved by Grover's algorithm cannot be improved by even one query while maintaining the same success probability.<sup>84</sup> More generally, in order to achieve an exponential speedup over classical computation in the query complexity model there has to be a promise on the input, i.e., some possible inputs must be disallowed.<sup>85</sup> This is one reason behind the success of quantum algorithms in cryptography: the existence of hidden problem structure that quantum computers can exploit in ways that classical computers cannot. Finding such hidden structure in other problems of practical interest remains an important open problem.

In addition, a cynical reader might point out that known quantum algorithms are mostly based on a rather small number of quantum primitives (such as the quantum Fourier transform and

quantum walks). An observation attributed to van Dam (see <http://dabacon.org/pontiff/?p=1291>) provides some justification for this. It is known that any quantum circuit can be approximated using only Toffoli and Hadamard quantum gates.<sup>86</sup> The first of these is a purely classical gate, and the second is equivalent to the Fourier transform over the group  $\mathbb{Z}_2$ . Thus any quantum algorithm whatsoever can be expressed as the use of quantum Fourier transforms interspersed with classical processing! However, the intuition behind the quantum algorithms described above is much more varied than this observation would suggest. The inspiration for other quantum algorithms, not discussed here, includes topological quantum field theory,<sup>87</sup> connections between quantum circuits and spin models,<sup>88</sup> the Elitzur–Vaidman quantum bomb tester,<sup>89</sup> and directly solving the semidefinite programming problem characterising quantum query complexity.<sup>90,91</sup>

As well as the development of new quantum algorithms, an important direction for future research seems to be the application of known quantum algorithms (and algorithmic primitives) to new problem areas. This is likely to require significant input from, and communication with, practitioners in other fields.

## ACKNOWLEDGEMENTS

This work was supported by the UK EPSRC under Early Career Fellowship EP/L021005/1.

## COMPETING INTERESTS

The author declares no conflict of interest.

## REFERENCES

- Jordan, S. The quantum algorithm zoo. Available at <http://math.nist.gov/quantum/zoo/>.
- Childs, A. & van Dam, W. Quantum algorithms for algebraic problems. *Rev. Mod. Phys.* **82**, 1–52 (2010).
- Mosca, M. in *Computational Complexity* 2303–2333 (Springer, 2012).
- Santha, M. Quantum walk based search algorithms. in *Theory Appl. Model. Comput.* **4978**, 31–46 (2008).
- Bacon, D. & van Dam, W. Recent progress in quantum algorithms. *Commun. ACM* **53**, 84–93 (2010).
- Ladd, T. et al. Quantum computing. *Nature* **464**, 45–53 (2010).
- Fowler, A., Mariantoni, M., Martinis, J. & Cleland, A. Surface codes: Towards practical large-scale quantum computation. *Phys. Rev. A* **86**, 032324 (2012).
- Buhrman, H., Cleve, R., Massar, S. & de Wolf, R. Non-locality and communication complexity. *Rev. Mod. Phys.* **82**, 665–698 (2010).
- Wilde, M. *Quantum Information Theory* (Cambridge Univ. Press, 2013).
- Papadimitriou, C. *Computational Complexity* (Addison-Wesley, 1994).
- Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26**, 1484–1509 (1997).
- Buhler, J. Jr., H. W. L. & Pomerance, C. Factoring integers with the number field sieve in *The Development Of The Number Field Sieve* Vol. 1554, 50–94 (Springer, 1993).
- Rivest, R., Shamir, A. & Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **21**, 120–126 (1978).
- Kleinjung, T. et al. in *Advances in Cryptology—CRYPTO 2010* Vol. 1554, 333–350 (2010).
- Boneh, D. & Lipton, R. in *Advances in Cryptology—CRYPTO’95*, 424–437 (1995).
- Brassard, G. & Høyer, P. in *Proceedings of the Fifth Israeli Symposium on Theory of Computing and Systems* 12–23 (Ramat Gan, Israel, 1997).
- Regev, O. Quantum computation and lattice problems. *SIAM J. Comput.* **33**, 738–760 (2004).
- Grover, L. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.* **79**, 325–328 (1997).
- Boyer, M., Brassard, G., Høyer, P. & Tapp, A. Tight bounds on quantum searching. *Fortschr. Phys.* **46**, 493–505 (1998).
- Prasad, M., Biere, A. & Gupta, A. A survey of recent advances in SAT-based formal verification. *Int. J. Softw. Tool. Technol. Transf.* **7**, 156–173 (2005).
- Williams, R. Improving exhaustive search implies superpolynomial lower bounds. *SIAM J. Comput.* **42**, 1218–1244 (2013).
- Brassard, G., Høyer, P., Mosca, M. & Tapp, A. Quantum amplitude amplification and estimation. in *Quantum Computation and Information* Vol. 305 of AMS Contemporary Mathematics Series (eds Lomonaco, S. J. & Brandt, H. E.), 53–74 (2002).
- Schöningh, U. in *Proceedings of 40th Annual Symposium on Foundations of Computer Science*, 410–414 (Washington DC, USA, 1999).
- Farhi, E., Goldstone, J. & Gutmann, S. A quantum approximate optimization algorithm applied to a bounded occurrence constraint problem. Preprint at [arXiv:1412.6062](https://arxiv.org/abs/1412.6062) (2014).
- Barak, B. et al. Beating the random assignment on constraint satisfaction problems of bounded degree. Preprint at [arXiv:1505.03424](https://arxiv.org/abs/1505.03424) (2015).
- Dürr, C. & Høyer, P. A quantum algorithm for finding the minimum. Preprint at [quant-ph/9607014](https://arxiv.org/abs/quant-ph/9607014) (1996).
- Dürr, C., Heiligman, M., Høyer, P. & Mhalla, M. in *Proceedings of 31st International Conference on Automata, Languages and Programming (ICALP’04)*, 481–493 (Turku, Finland, 2004).
- Ramesh, H. & Vinay, V. String matching in  $\tilde{O}(\sqrt{n} + \sqrt{m})$  quantum time. *J. Discrete Algorithms* **1**, 103–110 (2003).
- Montanaro, A. Quantum pattern matching fast on average. *Algorithmica* **1**–24 (2015).
- Farhi, E., Goldstone, J., Gutmann, S. & Sipser, M. Quantum computation by adiabatic evolution. *Tech. Rep.*, MIT-CTP-2936, MIT (2000).
- Farhi, E. et al. A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem. *Science* **292**, 472–475 (2001).
- van Dam, W., Mosca, M. & Vazirani, U. in *Proceedings of 42nd Annual Symposium on Foundations of Computer Science*, 279–287 (IEEE, 2001).
- Farhi, E., Goldstone, J., Gutmann, S. & Nagaj, D. How to make the quantum adiabatic algorithm fail. *Int. J. Quantum Inform.* **6**, 503 (2008).
- Farhi, E. et al. Quantum adiabatic algorithms, small gaps, and different paths. *Quantum Inf. Comput.* **11**, 0181–0214 (2011).
- Choi, V. Different adiabatic quantum optimization algorithms for the NP-complete exact cover and 3SAT problems. *Quantum Inf. Comput.* **11**, 0638–0648 (2011).
- Johnson, M. et al. Quantum annealing with manufactured spins. *Nature* **473**, 194–198 (2011).
- McGeoch, C. & Wang, C. in *Proceedings of ACM International Conference on Computing Frontiers (CF’13)*, 1–23 (Ischia, Italy, 2013).
- King, J., Yarkoni, S., Nevisi, M., Hilton, J. & McGeoch, C. Benchmarking a quantum annealing processor with the time-to-target metric. Preprint at [arXiv:1508.05087](https://arxiv.org/abs/1508.05087) (2015).
- Rønnow, T. et al. Defining and detecting quantum speedup. *Science* **345**, 420–424 (2014).
- Bulata, I. & Nori, F. Quantum simulators. *Science* **326**, 108–111 (2009).
- Brown, K., Munro, W. & Kendon, V. Using quantum computers for quantum simulation. *Entropy* **12**, 2268–2307 (2010).
- Georgescu, I., Ashhab, S. & Nori, F. Quantum simulation. *Rev. Mod. Phys.* **86**, 153 (2014).
- Feynman, R. Simulating physics with computers. *Int. J. Theor. Phys.* **21**, 467–488 (1982).
- Lloyd, S. Universal quantum simulators. *Science* **273**, 1073–1078 (1996).
- Berry, D., Childs, A. & Kothari, R. Hamiltonian simulation with nearly optimal dependence on all parameters. Preprint at [arXiv:1501.01715](https://arxiv.org/abs/1501.01715) (2015).
- Hastings, M., Wecker, D., Bauer, B. & Troyer, M. Improving quantum algorithms for quantum chemistry. *Quantum Inf. Comput.* **15**, 1–21 (2015).
- Jordan, S., Lee, K. & Preskill, J. Quantum algorithms for quantum field theories. *Science* **336**, 1130–1133 (2012).
- Childs, A., Farhi, E. & Gutmann, S. An example of the difference between quantum and classical random walks. *Quantum Inform. Process.* **1**, 35–43 (2002).
- Kempe, J. Quantum random walks hit exponentially faster. *Probab. Theory Rel. Fields* **133**, 215–235 (2005).
- Aharonov, D., Ambainis, A., Kempe, J. & Vazirani, U. Quantum walks on graphs. in *Proceedings of 33rd Annual ACM Symposium on Theory of Computing*, 50–59 (Heraklion, Crete, Greece, 2001).
- Childs, A. et al. Exponential algorithmic speedup by a quantum walk. in *Proceedings of 35th Annual ACM Symposium on Theory of Computing*, 59–68 (San Diego, CA, USA, 2003).
- Ambainis, A., Childs, A., Reichardt, B., Špalek, R. & Zhang, S. Any AND-OR formula of size  $n$  can be evaluated in time  $n^{1/2+o(1)}$  on a quantum computer. *SIAM J. Comput.* **39**, 2513–2530 (2010).
- Santha, M. On the Monte Carlo boolean decision tree complexity of read-once formulae. *Random. Struct. Algorithms* **6**, 75–87 (1995).
- Ambainis, A., Schulman, L. J., Ta-Shma, A., Vazirani, U. & Wigderson, A. The quantum communication complexity of sampling. *SIAM J. Comput.* **32**, 1570–1585 (2003).

55. Szegedy, M. in *Proceedings of 45th Annual Symposium on Foundations of Computer Science*, 32–41 (Rome, Italy, 2004).
56. Magniez, F., Nayak, A., Roland, J. & Santha, M. Search via quantum walk. *SIAM J. Comput.* **40**, 142–164 (2011).
57. Le Gall, F. in *Proceedings of 55th Annual Symposium on Foundations of Computer Science*, 216–225 (Philadelphia, USA, 2014).
58. Harrow, A., Hassidim, A. & Lloyd, S. Quantum algorithm for solving linear systems of equations. *Phys. Rev. Lett.* **15**, 150502 (2009).
59. Ambainis, A. in *Proceedings of 29th Annual Symposium on Theoretical Aspects of Computer Science*, 636–647 (Paris, France, 2012).
60. Clader, B., Jacobs, B. & Sprouse, C. Preconditioned quantum linear system algorithm. *Phys. Rev. Lett.* **110**, 250504 (2013).
61. Leyton, S. & Osborne, T. A quantum algorithm to solve nonlinear differential equations. Preprint at arXiv:0812.4423 (2008).
62. Berry, D. High-order quantum algorithm for solving linear differential equations. *J. Phys. A Math. Gen.* **47**, 105301 (2014).
63. Wiebe, N., Braun, D. & Lloyd, S. Quantum algorithm for data fitting. *Phys. Rev. Lett.* **109**, 050505 (2012).
64. Lloyd, S., Mohseni, M. & Rebentrost, P. Quantum algorithms for supervised and unsupervised machine learning. Preprint at arXiv:1307.0411 (2013).
65. Aaronson, S. Quantum machine learning algorithms: Read the fine print. *Nat. Phys.* **11**, 291–293 (2015).
66. Smolin, J., Smith, G. & Vargo, A. Oversimplifying quantum factoring. *Nature* **499**, 163–165 (2013).
67. Somaroo, S., Tseng, C., Havel, T., Laflamme, R. & Cory, D. Quantum simulations on a quantum computer. *Phys. Rev. Lett.* **82**, 5381 (1999).
68. Lanyon, B. *et al.* Universal digital quantum simulations with trapped ions. *Science* **334**, 57–61 (2011).
69. Blatt, R. & Roos, C. Quantum simulations with trapped ions. *Nat. Phys.* **8**, 277–284 (2012).
70. Aspuru-Guzik, A. & Walther, P. Photonic quantum simulators. *Nat. Phys.* **8**, 285–291 (2012).
71. Trotzky, S. *et al.* Probing the relaxation towards equilibrium in an isolated strongly correlated one-dimensional Bose gas. *Nat. Phys.* **8**, 325–330 (2012).
72. Poulin, D. *et al.* The Trotter step size required for accurate quantum simulation of quantum chemistry. *Quantum Inf. Comput.* **15**, 361–384 (2014).
73. Wecker, D., Bauer, B., Clark, B., Hastings, M. & Troyer, M. Gate count estimates for performing quantum chemistry on small quantum computers. *Phys. Rev. A* **90**, 022305 (2014).
74. Aaronson, S. & Arkhipov, A. The computational complexity of linear optics. *Theory Comput.* **9**, 143–252 (2013).
75. Ralph, T. Quantum computation: Boson sampling on a chip. *Nat. Photon.* **7**, 514–515 (2013).
76. Huh, J., Guerreschi, G., Peropadre, B., McClean, J. & Aspuru-Guzik, A. Boson sampling for molecular vibronic spectra. *Nat. Photon.* **9**, 615–620 (2015).
77. Martín-López, E. *et al.* Simulating molecular vibrations with photons (2015). in preparation.
78. Higgins, B., Berry, D., Bartlett, S., Wiseman, H. & Pryde, G. Entanglement-free Heisenberg-limited phase estimation. *Nature* **450**, 396–396 (2007).
79. Kitaev, A. Y., Shen, A. H. & Vyalı, M. N. *Classical and Quantum Computation* Vol. 47. (AMS, 2002).
80. Bookatz, A. QMA-complete problems. *Quantum Inform. Comput.* **14**, 361–383 (2014).
81. Schuch, N. & Verstraete, F. Computational complexity of interacting electrons and fundamental limitations of Density Functional Theory. *Nat. Phys.* **5**, 732–735 (2009).
82. Cleve, R., van Dam, W., Nielsen, M. & Tapp, A. in *Proceedings of the 1st NASA International Conference on Quantum Computing and Quantum Communications*, 61–74 (Palm Springs, CA, USA, 1998).
83. Drucker, A. & de Wolf, R. Quantum proofs for classical theorems. *Theory Comput. Grad. Surv.* **2**, 1–54 (2011).
84. Zalka, C. Grover's quantum searching algorithm is optimal. *Phys. Rev. A* **60**, 2746–2751 (1999).
85. Beals, R., Buhrman, H., Cleve, R., Mosca, M. & de Wolf, R. Quantum lower bounds by polynomials. *J. ACM* **48**, 778–797 (2001).
86. Shi, Y. Both Toffoli and controlled-NOT need little help to do universal quantum computing. *Quantum Inf. Comput.* **3**, 84–92 (2003).
87. Freedman, M., Larsen, M. & Wang, Z. A modular functor which is universal for quantum computation. *Commun. Math. Phys.* **227**, 605–622 (2002).
88. De las Cuevas, G., Dür, W., van den Nest, M. & Martin-Delgado, M. Quantum algorithms for classical lattice models. *New J. Phys.* **13**, 093021 (2011).
89. Lin, C. & Lin, H. in *Proceedings of 30th Annual IEEE Conference on Computational Complexity*, 537–566 (Portland, OR, USA, 2015).
90. Reichardt, B. in *Proceedings of 50th Annual Symposium on Foundations of Computer Science*, 544–551 (Atlanta, GA, USA, 2009).
91. Belovs, A. Quantum algorithms for learning symmetric juntas via adversary bound. in *Proceedings of 29th Annual IEEE Conference on Computational Complexity*, 22–31 (Vancouver, Canada, 2014).
92. Proos, J. & Zalka, C. Shor's discrete logarithm quantum algorithm for elliptic curves. *Quantum Inform. Comput.* **3**, 317–344 (2003).
93. Hallgren, S. Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem. *J. ACM* **54**, 4:1–4:19 (2007).
94. Kuperberg, G. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM J. Comput.* **35**, 170–188 (2005).
95. Regev, O. A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space. Preprint at quant-ph/0406151 (2004).
96. Martín-López, E. *et al.* Experimental realisation of Shor's quantum factoring algorithm using qubit recycling. *Nat. Photon.* **6**, 773–776 (2012).
97. Vandersypen, L. *et al.* Implementation of a three-quantum-bit search algorithm. *Appl. Phys. Lett.* **76**, 646–648 (2000).
98. Cai, X.-D. *et al.* Experimental quantum computing to solve systems of linear equations. *Phys. Rev. Lett.* **110**, 230501 (2013).
99. Barz, S. *et al.* Solving systems of linear equations on a quantum computer. *Sci. Rep.* **4**, 115 (2014).
100. Pan, J. *et al.* Experimental realization of quantum algorithm for solving linear systems of equations. *Phys. Rev. A* **89**, 022313 (2014).



This work is licensed under a Creative Commons Attribution 4.0 International License. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in the credit line; if the material is not included under the Creative Commons license, users will need to obtain permission from the license holder to reproduce the material. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>