News & Views
Quantum algorithms: Equation solving by simulation

Andrew M. Childs*

is in the Department of Combinatorics & Optimization and Institute for Quantum Computing, University of Waterloo, 200 University Avenue West, Waterloo, Ontario N2L 3G1, Canada

Quantum computers can outperform classical ones at some tasks, but the full scope of their power is unclear. A recent quantum algorithm suggests the possibility of far-reaching applications.

Quantum mechanical computers have the potential to quickly perform calculations that are infeasible with current technology. There are fast quantum algorithms to simulate the dynamics of quantum systems[1] and to decompose integers into their prime factors,[2] problems thought to be intractable for classical computers. But quantum computation is not a magic bullet—some problems cannot be solved dramatically faster by quantum computers than by classical ones. So is a quantum computer fundamentally a special-purpose device, suitable only for number-theoretic calculations or problems that are inherently quantum? In a recent article in Physical Review Letters,[3] Aram Harrow, Avinatan Hassidim, and Seth Lloyd describe how quantum computers can extract information about the solutions to linear equations, a fundamental task with broad applications.

The basic problem of finding a vector $\vec{x}$ satisfying $A\vec{x} = \vec{b}$ for some given matrix A and vector $\vec{b}$ arises throughout science and engineering. For example, signal processing, convex optimization, and finite element analysis all rely on solving linear equations. Due to the importance of linear systems, considerable effort has been spent on finding fast algorithms for solving them. One simple approach, the method of Gaussian elimination, was already known in ancient China, and today is standard fare in linear algebra courses. Alternative methods offer improved speed and better numerical stability, and some can take advantage of special properties like sparsity. However, if A is an $N \times N$ matrix (or a rectangular matrix with larger dimension N), all of these methods use a number of operations at least proportional to N.

Harrow, Hassidim, and Lloyd suggest approaching this problem using quantum simulation. Given an $N \times N$ sparse Hermitian matrix A, a quantum state $|b\rangle$, and a time t, quantum simulation provides a method of preparing the quantum state $e^{-iAt}|b\rangle$ using a number of operations that is only polynomial in $\log N$.[4] In the approach of Harrow et al., the vector $\vec{b}$ is first encoded into a quantum state $|b\rangle$. Then, by a well-known technique called phase estimation,[5] the ability to produce $e^{-iAt}|b\rangle$ is leveraged to produce a quantum state $|x\rangle$ proportional to $A^{-1}|b\rangle$. (A similar approach can be applied when the matrix A is non-Hermitian, or even when A is non-square.) The result is a solution to the system of linear equations encoded as the quantum state $|x\rangle$.

By itself, producing a quantum state proportional to $A^{-1}|b\rangle$ does not solve the task at hand. To extract information from a quantum state, one must perform a measurement. Learning all N amplitudes of an N-dimensional state requires a number of measurements at least proportional to N. Thus, if our goal is to completely reconstruct a solution $\vec{x}$, the quantum algorithm cannot hope to have a significant advantage over classical methods. However, for some problems one may not

*amchilds@uwaterloo.ca

be interested in the entire vector $\vec{x}$, but rather, in some special feature of it, such as an expectation value. Then a quantum computer may be able to solve the problem rapidly.

In addition to readout, the approach suffers from other significant limitations. The vector $\vec{b}$ must be given in a way that allows quickly preparing the quantum state $|b\rangle$. While methods are available for doing this if $\vec{b}$ has a suitable implicit description, the approach is useless if $\vec{b}$ is given by explicit classical data. Furthermore, as in classical methods for solving linear equations, the performance depends crucially on the condition number κ, a measure of how close A is to singular. The running time of the quantum algorithm is polynomial in $\log N$ and in κ, so the quantum advantage is only significant when κ is not too large.

Having lowered the bar for the sense in which we hope to solve a system of linear equations, one might wonder whether the quantum algorithm offers any real advantage over classical computing. To address this concern, in perhaps the most interesting aspect of their work, Harrow, Hassidim, and Lloyd prove that the problem they solve is as hard as anything a quantum computer can do. In particular, they show that any quantum computation can be encoded into an instance of solving linear equations, even with the restrictions required for their quantum solver to be efficient. Thus, either ordinary classical computers can efficiently simulate quantum ones—a highly unlikely proposition—or the quantum algorithm for solving linear equations performs a task that is beyond the reach of classical computation.

Proving hardness results of this kind is a widely-used strategy for establishing the nontriviality of quantum algorithms. Similar constructions are known for problems such as finding ground states by adiabatic evolution,[6] computing invariants of knots,[7] estimating entries of powers of matrices,[8] and contracting tensor networks,[9] among others. But what sets linear equations apart is their ubiquity in scientific computing and engineering applications.

Will the quantum solution of linear equations turn out to be an invaluable tool, or are its limitations too great for the technique to be of practical significance? Unfortunately, no concrete task has yet been proposed for which the quantum algorithm provides a clear advantage. But it will be exciting to explore the impact of this and related applications of quantum computing, especially as quantum information processing devices become a reality.

References

[1] R. P. Feynman, *Int. J. Theor. Phys.* **21**, 467–488 (1982).

[2] P. W. Shor, *SIAM J. Comput.* **26**, 1484–1509 (1997).

[3] A. W. Harrow, A. Hassidim, and S. Lloyd, *Phys. Rev. Lett.* **103**, 150502 (2009).

[4] D. Aharonov and A. Ta-Shma, *Proc. 35th ACM STOC*, pages 20–29, 2003.

[5] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, *Proc. Roy. Soc. London A* **454**, 339–354 (1998).

[6] D. Aharonov et al., *Proc. 45th IEEE FOCS*, 42–51 (2004).

[7] M. Bordewich, M. Freedman, L. Lovász, and D. Welsh, *Comb. Probab. Comput.* **14**, 737–754 (2005).

[8] D. Janzing and P. Wocjan, *Theory of Computing* **3**, 61–79 (2007).

[9] I. Arad and Z. Landau, arXiv:0805.0040.