# Quantum Computers for Exponentially Hard Problems

PETER D. DRUMMOND AND MARGARET D. REID CENTRE FOR QUANTUM AND OPTICAL SCIENCE SWINBURNE UNIVERSITY OF TECHNOLOGY

## ABSTRACT

A new generation of application specific quantum computers has shown great promise in solving exponentially hard problems that are inaccessible to classical computers, by employing innovative designs that do not utilize traditional gate-based architectures. The real world problems that can be treated range from issues important to industry, to the most challenging problems in cosmology. This article will explain these novel approaches being investigated at Swinburne University and elsewhere, with experiments and theory planned or underway in Australia, Japan, Europe and the USA.

## INTRODUCTION

The search for quantum computers designed to outperform classical computers is driven by the quantum advantages potentially obtainable [1]. Moore's law – the doubling of transistor counts every year – served the computer industry well for the last fifty years. Today, computer speeds have reached a plateau, and transistor count increases are also slowing down. Circuit sizes have reached the point that silicon devices are hard to shrink further without adverse effects.

Yet the demand for increasing computer power to process large quantities of data is expanding. This uses increasing amounts of energy, which is not environmentally sustainable. One way to solve this problem is the quantum computer. A new generation of quantum computers is now under development, with the goal of trying to solve exponentially hard problems that are central to areas like optimization and quantum dynamics. If solved, these would have numerous applications in almost every field that analyses data and then applies the data to complex, realistic problems, as well as consequences to fundamental science.

Scalability is all-important to computing. The most insoluble problems of modern computing are exponentially complex [2]: the required time is an exponential function of the problem size. Classical universal computers are generally unable to overcome this, except through approximations, although a rigorous proof that this is true is an unsolved grand challenge [3].

An encouraging sign that quantum dominated behaviour is feasible is shown by recent Nobel awards in quantum science [4,5], which demonstrate that extreme quantum behaviour is indeed obtainable in experiments. More recent work includes the successful observation of quantum opto-mechanical entanglement [6,7], which is in excellent agreement with quantum phase-space calculations [8,9]. Other quantum science experiments involve ultracold Bose-Einstein condensates [10] and related polariton experiments [11,12], as well as superconducting quantum circuits [13].

The difficulty in creating any quantum computer is decoherence, causing the loss of the quantum character of the device. This can be eliminated either through quantum error-correction, which has proved difficult to implement, or else by means of careful design to reduce quantum errors at the earliest stage possible.

The development of modern integrated circuit and computer chip designs was expedited with the use of a computational toolbox for electronic design, SPICE, which had an enormous impact on this field. It is safe to say that all existing industrial integrated circuit designs and roadmaps could not exist without SPICE or its successors that are used today. There are at present no comparable simulation tools for quantum technologies. This is a very significant issue, since without general purpose design tools it is hard to develop new devices.

For quantum computers, the problem is that most theoretical methods are either limited to small devices or else use uncontrolled approximations. For example, the mean-field approximation simply removes much important quantum behaviour, rendering it useless. Other methods generally don't scale to large sizes.

The Centre for Quantum and Optical Science at Swinburne University is developing a quantum design computational toolbox [14], which is applicable to quantum technologies, to determine how to predict performance, and estimate the effects of decoherence. Such tools are proven by comparison to experiment.

One of the methods employed in this stochastic toolbox, which is readily scalable to large size, is the generalized P-representation phase-space method [15]. This is not restricted to small devices. It has already been applied to simulate very large and highly non-classical quantum systems, including entanglement in parametric down-conversion [16], quantum soliton propagation and quantum collisions of Bose-Einstein condensates [17], quantum decoherence in 60 qubit ion traps [18], and 100 mode quantum photonic interferometers [19].

The hardware strategy of the new generation of quantum computers can be summarised in one word: *simplicity*. What is the simplest process that can be employed to solve one specific exponentially complex problem? Simplified design makes for reduced decoherence. Such devices are not universal, but they can provide answers to vital questions that occur repeatedly in important areas of industry and science. Modern computers have many specialised circuits for specific problems, like arithmetic. Even the brain itself has different structures for different purposes, so why not a quantum computer?

To understand these different approaches, its best to consider the problems they are designed to solve.

# SEMIPRIME FACTORIZATION

The earliest attempts to build quantum computers tried to reconstruct classical universal computers, following traditional architectures: but with quantum gates, memory and communications. Such experiments provided information on decoherence, but were not easy to scale to large size. Although not just restricted to only one problem, these were often targeted at factorization.

Perhaps the most famous problem for a quantum computer, factorization has a very long history. Once just of interest to number theorists, it is now central to the Internet. It provides the lock and key for secure online transactions. Tools for factorization are of great interest to any organisation that wishes to decode secret communications, for many obvious reasons.

The role of the quantum computer comes from the discovery that certain types of quantum Fourier transform can be used to efficiently factorise large integers. For these, no fast classical algorithm currently exists. In the long term this hardware could benefit governments, but unfortunately there are ethical issues: criminals also have an interest in hacking!

The time-scale involved when this will become important can be estimated from current sizes of ion-trap quantum computers [20]. This shows that universal quantum computer sizes have been growing linearly at a rate of approximately one qubit per year since the first gates were developed, which is like a quantum Moore's law.

However, a published estimate for the required size of a gate-based quantum computer that can factorize a 1024 bit integer is  $4.54 \times 10^8$  physical qubits [21], including overheads and error-correction. Even if this can be reduced, it is not surprising that there is now a search for alternative architectures to solve hard problems.

# THE TRAVELING SALESMAN PROBLEM

While not as newsworthy as cryptography, the traveling salesman problem is one of the most well known hard problems in computer science [2]. It sounds trivial: despite this, the traveling salesman problem is of great universal significance in computer science.

Such problems are NP complete, which means that if one can solve them, a large range of similar exponentially

hard problems will become soluble. The potential applications range from DNA sequencing to circuit design, efficient power transmission and transport routes that consume less energy, all of great benefit to society.

The tantalizing motivation for the quantum computer scientist is that solutions to NP complete problems have a much larger range of uses than factorization. These challenges have many real-world applications. Classical computers are already being used to solve these problems approximately, so the potential benefits to humanity are simply enormous.

This means that there is every reason to design computers whose only purpose is to solve routing and optimization problems, just as there is a long history of classical computer circuits whose only purpose is, for example, carrying out floating point arithmetic. While not universal, this approach may have more immediate benefit if the computers are more easily built.

The Canadian company, D-wave, chose this class of problem as the target of their large-scale, commercial quantum computers. These operate on the principle of adiabatic passage. The idea is that a quantum ground state can be used to encode the optimal solution, which can be reached adiabatically from a known starting point.

The D-wave computer was criticised initially on the basis that it may not be truly operating in the quantum regime [22]. What is worth noting is that these computers are in fact solving nontrivial problems. This is something that traditional quantum computer designs have not yet been able to do, owing to size limitations.

Other promising approaches include trapped-ion quantum simulators [23], and the Ising machine [24], under development at Stanford and Tokyo. This targets the same problems, but with a different approach. Rather than use a ground state, the Ising machine models optimization problems as the steady state of a non-equilibrium parametric system, driven with lasers.

Such an approach has many advantages. It can operate at room temperature, rather than cryogenically, making for lower cost operation and greater portability, at least in principle. The use of a non-equilibrium steady state may allow for greater speed in reaching the solution. In addition, larger size problems appear practical. But can it really outperform classical computers at NPhard optimization? This is still very much open to debate, since the existing Ising machines can also be modelled semiclassically. However, even if not yet fully quantum in operation, like the D-wave computer they already solve difficult optimization problems, an achievement in itself.

An alternative hardware model is the `XY' machine, which uses a different type of photonic interaction. These solve a different class of problem, similar to the planar ground state problems made well known by the 2016 Nobel Prize. Experiments on these types of device are underway at the Weizmann Institute in Israel.

It is well known from quantum optics that photonic parametric devices can operate in fully quantum regimes. Closely related parametric models are under investigation at Swinburne University of Technology, using phasespace methods from quantum optics [25]. A long-term goal is to include quantum-tunnelling effects – which have no classical explanation – to see if this can be employed to speed these devices up, to the point that they overcome the known classical speed limitations.

# **BOSON SAMPLING**

The effort to develop computers with unambiguous quantum advantages has recently led to a very surprising conclusion. Theoretical research at MIT [26] has resulted in the conjecture that even a linear, photonic network can have an output whose statistics cannot be replicated with a classical computer in less than exponential time.

This is made more plausible by the fact that simply calculating the output statistical moments of such quantum photonic devices - if fed a single-photon input into a subset of channels – would already be exponentially hard. The reason for this is that computing such output moments requires knowledge of matrix permanents, which are exponentially hard to find.

Permanents are mathematical objects similar to determinants. They are the sum of all distinct n-fold products of matrix elements of an  $n \times n$  matrix. Since the number of such products is factorial (n), their difficulty grows exponentially with n. This calculation is known as a **#**P hard problem in computer science. The difficulty of such problems is shown by the fact that the largest permanent calculated exactly was for a  $50 \times 50$  matrix – and it required the world's fastest supercomputer [27].

It is important to have quantum computers with both computational advantages and verifiable results. Photonic networks are examples of this, with numerous recent experiments demonstrating quantum properties [28] and operation using boson sampling [29-31].

Using phase-space theory, we have developed both a quantum simulation of a boson sampling quantum computer, and analytic results [19]. Surprisingly, we can simulate the experimental correlations much faster and with less error than in the experiments. This does not solve a **#P** hard problem – but gives signatures that can verify the computational output.

The important point about these machines is that their quantum behaviour is easily understood, and is completely different to their classical counterparts: making the identification of a quantum speed-up a simpler task than with many other approaches.

The boson sampler also has an unexpected spin-off. Two boson sampling computers, working together, can measure field gradients with a quantum-limited precision far beyond what is classically possible [32].

# EARLY UNIVERSE SIMULATOR

The emulation of the quantum decay of a relativistic scalar field from a metastable state ("false vacuum decay") is a fundamental idea in quantum field theory and cosmology, but is also one of the most exponentially complex problems imaginable – and has no exact solution. It is the current standard model in cosmology for the Big Bang event that started the universe.

We propose that this can be simulated using an ultracold spinor Bose gas [33,34]. This will demonstrate that an exponentially complex, high energy theoretical model can be solved on a table-top quantum computer, even with energies far higher than any future CERN LHC, under conditions impossible to achieve in terrestrial experiments. While the experiment is still in the planning stages, a potassium isotope with a suitably engineered coupling has already been identified.

The physics involved is to use two ground states of a suitable potassium isotope, coupled with a microwave field at nanokelvin temperatures. Under these conditions, the relative phase between the two Bose-Einstein condensates - akin to the Josephson phase in a superconducting junction – behaves as a relativistic quantum field in one, two or three dimensions. This is the type of quantum field believed to exist in the early universe, whose decay from a metastable vacuum to a true vacuum triggered the Big Bang.

While approximate theories exist, there is no currently known exact solution of these quantum equations, due to exponential complexity. Such experiments would therefore provide us with a way to construct a quantum computer for the early universe, and to test current cosmological pictures against this computer.

Importantly, this would be first experimental demonstration of metastable vacuum decay.



**Fig. 1:** Early universe simulator: computer predictions of formation of true vacuum 'bubbles' in a metastable false vacuum region, modeling the origin of the Big Bang.

Acknowledgements: Grateful acknowledgements are given to funding from the Australian Research Council, and to discussions with many valued colleagues including: A. Sidorov, L. Rosales-Zarate, B. Opanchuk, S. Kiesewetter, R. Polkinghorne, K. Dechoum, S. Chaturvedi, P. J. Forrester, J. Brand and O. Fialko.

#### References

- [1] R. P. Feynman, Int. J. Th. Phys. 21, 467 (1982).
- [2] Sanjeev Arora and Boaz Barak, Computational Complexity: A Modern Approach (Cambridge, 2009).
- [3] A. M. Jaffe, The Millennium Grand Challenge in Mathematics, Notices of the AMS 53.6 (2006).
- [4] S. Haroche, Annalen der Physik 525, 753 (2013).
- [5] D. J. Wineland, Annalen der Physik 525, 739 (2013).
- [6] M. R. Vanner et. al., PNAS 108, 16182, (2011).
- [7] T. A. Palomaki, J. D. Teufel, R. W. Simmonds, and K. W. Lehnert, Science 342, 710 (2013).
- [8] S. Kiesewetter, Q. Y. He, P. D. Drummond, and M. D. Reid, Phys. Rev. A 90, 043805 (2014).
- [9] P. D. Drummond and M. Hillery, The Quantum Theory of Nonlinear Optics (Cambridge University Press, 2014).
- [10] S. Bose, Zeitschrift fur Physik 26, 178 (1924); A. Einstein, Sitz. der Preuss. Akad. der Wissenschaften 3, 18 (1925); M. H. Anderson et al, Science 269, 198 (1995); K.B. Davis et al., Phys. Rev. Lett. 75, 3969 (1995).
- [11] Hui Deng, Hartmut Haug, and Yoshihisa Yamamoto, Rev. Mod. Phys. 82, 1489 (2010).
- [12] Karol Winkler et al, New Journal of Physics 17 023001 (2015).

- [13] M. H. Devoret and R. J. Schoelkopf, Science 339, 1169 (2013).
- [14] S. Kiesewetter et. al., SoftwareX, March (2016).
- [15] P. D. Drummond and S. Chaturvedi, Physica Scripta 91, 073007 (2016).
- [16] M. D. Reid and P. D. Drummond, Phys. Rev. Lett. 60, 2731 (1988); M. D. Reid and L. Krippner Phys. Rev. A 47, 552 (1993); K. Dechoum, P. D.
- Drummond, S. Chaturvedi, M. D. Reid, Phys. Rev. A 70, 053807 (2004). [17] J. F. Corney et. al., Phys. Rev. A. 78, 023831 (2008); R. Dong, et. al., Optics Lett. 33, 116 (2008); P. Deuar and P. D. Drummond, Phys. Rev. Lett. 98, 120402 (2007).
- [18] M. D. Reid et. al, Phys. Rev. A 90, 012111 (2014); L. Rosales-Zárate, et. al., Phys. Rev. A 90, 022109 (2014).
- [19] P. D. Drummond et. al, Phys. Rev. A 94, 042339 (2016); B. Opanchuk et. al, arXiv:1609.05614v1 (2016);
- [20] B. Lanyon, et. al., Science 334, 57 (2011).
- [21] N. Cody Jones, et. al., Phys.Rev. X 2, 031007 (2012).
- [22] Troels F. Ronnow et. al., Science 345, 420 (2014).
- [23] K. Kim et. al., Nature 465, 590 (2010); J. W. Britton, et al, Nature 484, 489 (2012).
- [24] Alireza Marandi et. al., Nat. Photonics 8, 937 (2014).
- [25] P. D. Drummond and K. Dechoum, Phys. Rev. Lett. 95, 083601 (2005); K. Dechoum et. al., J. Opt. Soc. Am. B 33, 871-883 (2016).
- [26] S. Aaronson, Proc. Roy. Soc. A 467, 3393 (2011).
- [27] J. Wu et. al., arXiv:1606.05836v1.
- [28] M. A. Broome et. al., Science 339, 794 (2013); S. Armstrong et al., Nature Physics 11, 167 (2015).
- [29] A. Crespi et al., Nat. Photon. 7, 545 (2013).
- [30] M. Tillmann et al., Nat. Photon. 7, 540 (2013).
- [31] J. B. Spring et al., Science 339, 798 (2013).
- [32] K. R. Motes et al., Phys. Rev. Lett. 114, 170802 (2015).
- [33] B. Opanchuk et al, Annalen der Physik 525, 866 (2013).
- [34] O. Fialko et. al, Europhysics Lett. 110, 56001 (2015); arXiv:1607.01460.



**Peter Drummond** is the science director of the Center for Quantum and Optical Science at Swinburne University of Technology, researching ultra cold atomic physics and quantum information. He has a master's from Harvard University and a PhD from Waikato University, supervised by New Zealand's Dirac Medallist, Dan Walls. He has worked at Rochester, Auckland, Erlangen and Queensland Universities, at IBM Laboratories in San Jose, and NTT Laboratories in Tokyo. He has won the AIP Boas and Massey medals for research, the German Humboldt award, and is a fellow of the Australian Academy of Science, the AIP and the American Physical Society.