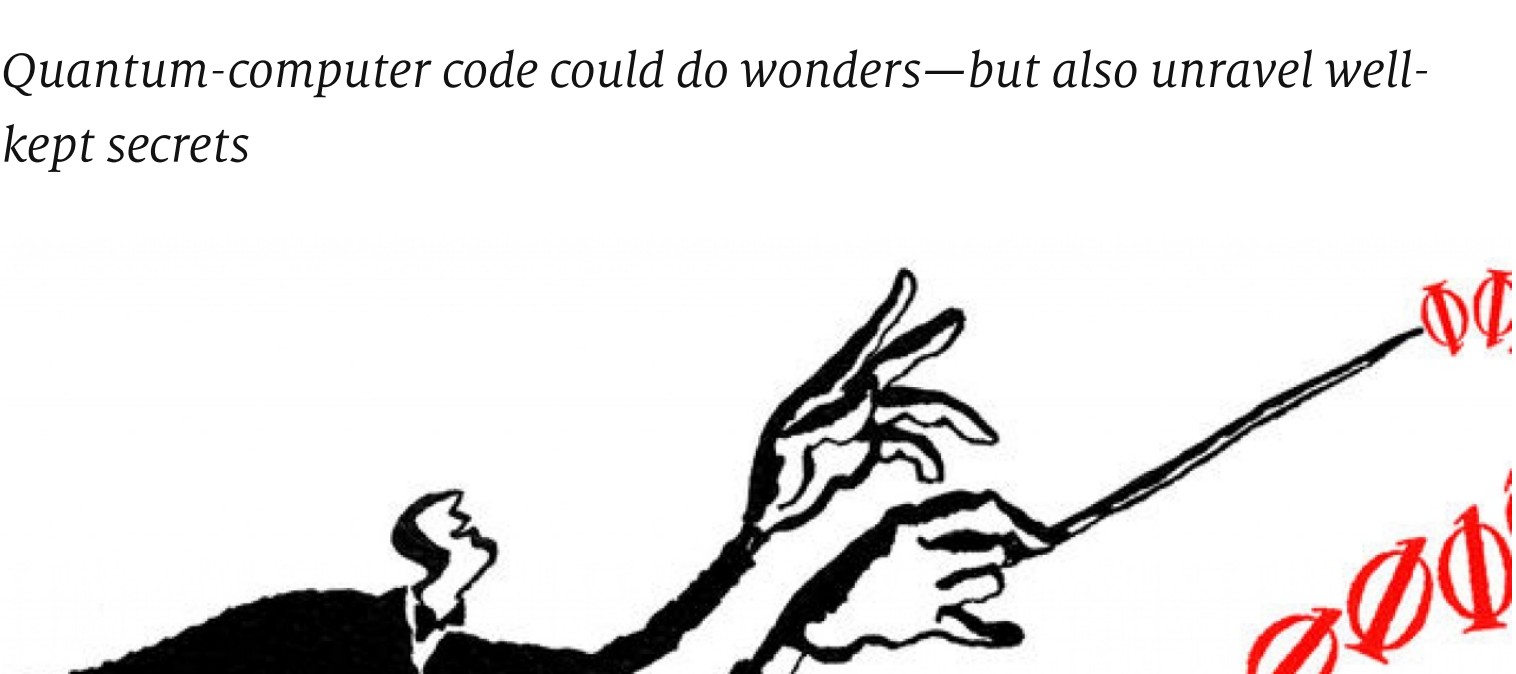
Program management

Quantum computers will require a whole new set of software

Quantum-computer code could do wonders—but also unravel well-kept secrets



Belle Mellor

Print edition | Technology Quarterly ›
Mar 9th 2017

IT DOESN'T help to have a quantum computer if no one knows how to program it," says Tim Polk, of the White House Office of Science and Technology Policy in Washington. Although academic efforts to build quantum-computer hardware have been going on for two decades, comparatively little has been done to develop the software needed to run the machines when they come.

That is changing, because in the past few years it has become clear that those machines are getting closer. Two parallel efforts are under way. One is to create software as generally understood—the graphical interfaces, programming languages and so on, a kind of "Windows for quantum". The other is to develop novel algorithms, step-by-step instructions that break down problems into discrete parts amenable to quantum computing.

Latest stories
A massacre in Pittsburgh illustrates America's disunity
DEMOCRACY IN AME... 10 HOURS AGO
Brazil's next president is likely to be Jair Bolsonaro
2 DAYS AGO
Petrostates must diversify to cope with fluctuating oil prices
2 DAYS AGO
"Bohemian Rhapsody" is more fantasy than real life
PROSPERO › 2 DAYS AGO
What is the INF treaty?
THE ECONOMIST EXPLA... 3 DAYS AGO
An Air India flight attendant falls out of an aircraft
GULLIVER › 3 DAYS AGO
See more ›

Innovation abounds in both camps, and among big tech firms as well as plucky startups. Some big players are working on both sides of the problem, and a growing ecosystem of quantum-friendly consultancies advises companies on what quantum computing might do for them.

"Machine" language for quantum computers, which actually tells the computer what to do, is fairly well understood. It is not so different from the logic gates of standard computing, except that it allows for "superpositions" of qubits in which they can be both 0 and 1 at the same time. But how to write computer code to interact with such a machine, or to simulate what it can do? Options are multiplying, including open-source software packages such as QuTip, funded by a number of research outfits in Asia. On March 6th IBM released the first commercial program for universal quantum computers (the general-purpose kind). And various startups have released their own quantum software.

One of the most ambitious, LIQUi|> (whose name plays on a symbol in quantum mechanics), comes from Microsoft. It aims to tackle the whole "software stack", from the user interface to code-compilers and ultimately to a machine language suitable for Microsoft's planned hardware, and that of others.

Krysta Svore, who leads Microsoft's quantum-software team, says that the group is also working on reducing the total number of qubits and operations required for quantum calculations, known as "overhead", and on making standard computers better at emulating quantum ones (the group recently hired a world expert in that field, Matthias Troyer). The team's full-scale simulation of a 32-qubit computer requires 32 gigabytes of memory, more than the average desktop can muster but still manageable.

Dr Svore and her colleagues are also making estimates of how many qubits, and minutes, would be needed to crack specific problems. She says the numbers are "down dramatically", thanks to recent improvements in keeping qubits under tighter control. For example, she reckons that a thorough analysis of the energy-intensive nitrogenase reaction to make fertiliser would take a 100-logical-qubit quantum computer hours or perhaps days, whereas a conventional supercomputer would need billions of years. The prize might be a cut of 1-2% in global natural-gas consumption.

But the key to getting the most out of quantum computers are the algorithms that these various software packages implement. The first of them, including the one by Peter Shor that showed how quantum computers could crack global encryption systems, tested the theoretical idea by aiming at the most intractable problems on the biggest notional machines.

Even deeper learning

These days, says Aram Harrow of the Massachusetts Institute of Technology, the focus has shifted to algorithms that smaller machines can make use of, because that kind of hardware will soon be widely available. "We're still interested in what you can do with a million or a billion qubits, but it's interesting to see if you can figure out what you can do with 100," he says.

A lot, it seems. One of the most promising areas is in machine learning and deep learning, two facets of artificial intelligence that have attracted much attention recently. Applications include searching through vast swathes of data to find patterns, such as in image recognition, cyber-security and, more prosaically, recommendation engines that suggest products consumers might like. But there are all manner of other algorithms, from those that crunch numbers to those that mimic atoms.

All these quantum recipes call for some means of cataloguing them. Stephen Jordan heads the Quantum Algorithm Zoo at the National Institute of Standards and Technology in Maryland, a comprehensive collection of known algorithms. He has devised a taxonomy of 59 mathematical families they fit into, each suited to particular kinds of problems or breaking down problems in a particular, quantum-friendly way.

Many such algorithms, when run on existing special-purpose machines or as emulations on standard computers, fail to beat their "classical" counterparts. Vlatko Vedral, of the National University of Singapore's Centre for Quantum Technologies, stresses that traditional techniques, particularly for quantum-chemistry problems like the nitrogenase reaction, are already quite sophisticated. The trouble is that no beefy general-purpose quantum computer exists as yet, so no one knows whether a given algorithm run on one would beat its classical counterpart. At the same time, astonishingly efficient algorithms suited to quantum computing are waiting to be discovered.

Those 59 families of algorithms, and ever-better emulators for eventual machines, are an excellent starting point for planning the quantum-computing future, and nowhere is interest greater than in finance. Commonwealth Bank of Australia is getting in early, collaborating closely with a research group led by Michelle Simmons at the University of New South Wales. D-Wave has partnered with 1Qbit, a startup, to develop "Quantum for Quants", a forum for the quantitative-finance industry. Its editors include Michael Sotiropoulos, head of global equities at Deutsche Bank. UBS, a big Swiss bank, is working with QxBranch, another startup, on using quantum algorithms in foreign-exchange trading and arbitrage. Hyder Jaffrey, head of Strategic Investments and Fintech Innovation at UBS, says he puts quantum computing in the same category as artificial intelligence and blockchains, "all stuff with the potential to change markets".

Banking on it

Companies such as QxBranch and 1Qbit play a new role of middleman between the quantum experts and industry, examining whether and how a given firm's business might be improved by quantum methods, for example optimising trading strategies or supply chains, or monitoring network activity to spot cyber-attacks. Landon Downs, a co-founder of 1Qbit, says that can lead to solutions which can already be put to use. "By taking the

The Economist
Subscribe
Welcome

algorithms," he says. "That's where lots of our successes come from."

The biggest benefit is expected to come from quantum-computing hardware once it arrives, so much of this business depends on simulating that hardware on standard machines as accurately as possible. Michael Brett, chief executive of QxBranch, says the idea is that "some Tuesday morning when one becomes available we just swap out our simulation for the real hardware."

Even as all these computer scientists and consultants are working on software for the quantum future, a handful of others are working on software to combat it. After all, what got researchers going in the first place was the fear that global encryption standards would crumble in the face of quantum computing. That remains a danger for the future, and retrospectively perhaps even for the present, if encrypted communications filed away now are analysed by powerful quantum computers later. That is the idea behind post-quantum cryptography, an effort to create ciphers that even future quantum computers will be unable to crack.

PQCRYPTO is a three-year, European-funded project to develop post-quantum ciphers. Its goal is not to find the most mathematically gnarly way of encrypting data, but rather to identify one that is sufficiently difficult to break without needing too much memory or computation to implement. RSA, a current global standard, could be made hard enough to break, but the cryptographic keys would have to be a terabyte long—an impracticable option. Keys for elliptic-curve cryptography, another current standard, are just 32 bytes long; any post-quantum solution needs to aim for a similar ratio of brevity to security.

Tanja Lange, who leads the project, says that post-quantum efforts are now attracting a lot of attention, particularly from nervous Silicon Valley outfits. In 2015 America's National Security Agency said it would be updating all its cryptography to make it quantum-computer-proof. Last year Google quietly ran its own post-quantum cryptography test in Chrome, its web browser. Some of its users' communications were protected both with elliptic-curve encryption and New Hope, a post-quantum protocol developed as part of PQCRYPTO. The median delay added to those communications turned out to be just a millisecond.

"The power of quantum computing is rediscovering all the problems that computers cannot solve, and having a path to solving them," says Dario Gil, vice-president of science and solutions at IBM. "It's a reorientation of what we think about computers." But a device capable of solving big problems will create new ones if it can unravel protocols that have protected secrets for decades.

This article appeared in the Technology Quarterly section of the print edition under the headline "Program management"

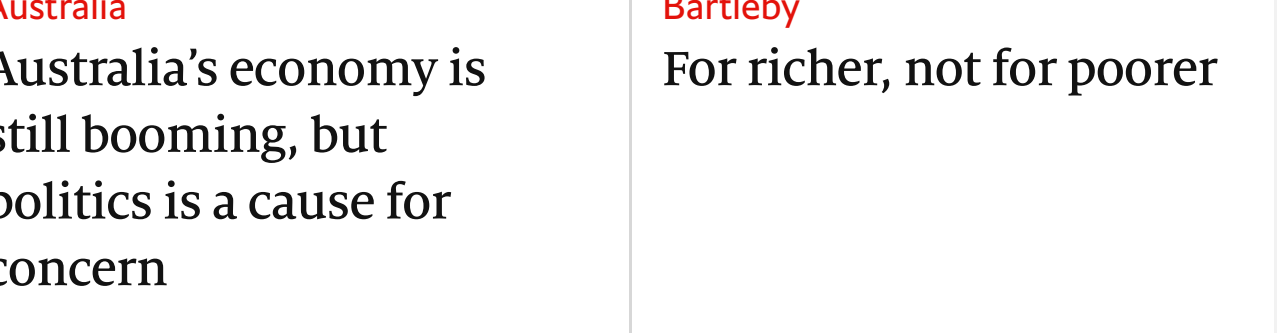
€20
for 12 weeks' access.

The Economist
SUBSCRIBE NOW ›

Print edition | Technology Quarterl

Subscribe: 12 weeks for €20
Get full access to *The Economist* via print, online and our apps.
Subscribe: 12 weeks for €20

provide moral leadership
DEMOCRACY IN AMERICA ›



AFP

Brazil's elections
Containing Jair Bolsonaro

Australia
Australia's economy is still booming, but politics is a cause for concern

Bartleby
For richer, not for poorer

Tell us what you think of Economist.com
Leave feedback
Need assistance with your subscription?
Contact us

Classified ads

Subscribe | Group subscriptions | Contact us | Help

Keep updated

Sign up to get more from *The Economist*
Get 3 free articles per week, daily newsletters and more.
Email address
Sign up

About *The Economist*
Advertise | Reprints | Careers | Media Centre
Terms of Use | Privacy | Cookie Policy | Manage Cookies
Accessibility | Modern Slavery Statement

Copyright © The Economist Newspaper Limited 2018. All rights reserved.