OUTWARD BOUNDS

Creating new tools for quantum computing and probing its theoretical limits

Chris Quirk

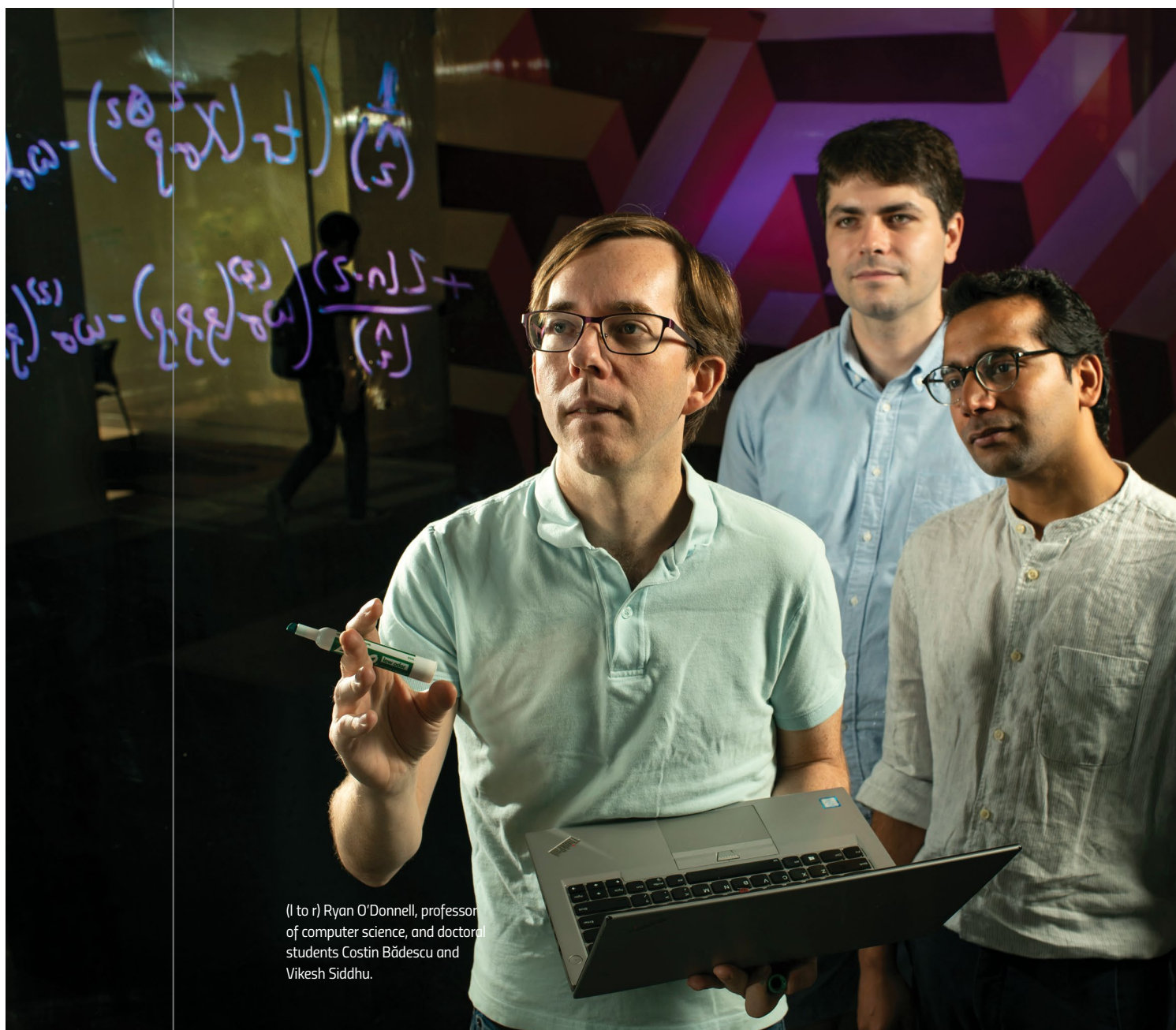
It's almost impossible to scan the science news without quickly coming across bold claims for the prospects of quantum computing, like speeding the development of life-saving drugs and radically enhancing machine learning. Governments and massive technology firms like Google, Microsoft and IBM are pouring billions into quantum computing research and development, with reports of new breakthroughs happening all the time. An era of virtually unlimited computational power feels imminent.

As experimentalists develop new ways to corral and control the wayward particles that are the meat and potatoes of quantum computers, researchers across Carnegie Mellon are creating tools that could aid their endeavors, while exploring the computational limits of what might be achieved. And though the overall outlook for quantum computing is upbeat, much remains unknown about its potential limitations, both theoretical and physical.

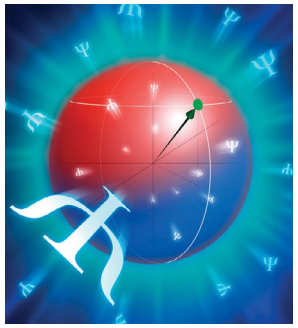
Ryan O'Donnell, professor of computer science, has devoted much of his recent research efforts to quantum information theory. "I'm inherently enthused about the nature of computation and what it means to compute things," he said. "Now it seems like there's this whole new method of computing. It's amazing, and it's incumbent on scientists to discover the power and limits of it that are allowed by the physical universe."

"Now it seems like there's this whole new method of computing. It's amazing, and it's incumbent on scientists to discover the power and limits of it that are allowed by the physical universe."

—Ryan O'Donnell



(l to r) Ryan O'Donnell, professor of computer science, and doctoral students Costin Bădescu and Vikesh Siddhu.



DEFINING QUANTUM COMPUTING

The difference between classical and quantum computing is the vastly expanded computational power that comes from taking advantage of the quantum states of atoms, particles or photons, which can serve as quantum bits (or qubits). Two important quantum characteristics integral to quantum computing are superposition and entanglement.

For a particle in superposition, its precise state remains unknown. For instance, one characteristic of an electron, spin, will always resolve to a value of 1 or 0 when measured, but prior to measurement you can't know its value — it's a combination of both 1 and 0 simultaneously. Compared to a classical bit, which will have a value of 1 or 0, the amount of information you can embed in a quantum system will be exponentially greater. If two particles are entangled — even if the particles are miles apart — when you measure one particle, the other immediately comes out of superposition, as if it had been measured, too.

Under the hood, a quantum computer will take an initial state of a set of qubits and perform a series of gate operations in a manner not dissimilar to classical computers. The difference is instead of sending charges into a circuit, the qubits are physically manipulated or rotated in a kind of synchronized dance, altering their quantum states and producing a result when the system is measured. It may sound like a tidy process, but the reality of quantum computing is full of engineering, software and theoretical obstacles.

O'Donnell, along with his former doctoral student John Wright (CS 2016), who is now a postdoc at the California Institute of Technology, has been examining possibilities for quantum tomography, a method for understanding the states of quantum particles. "Suppose you run an experiment, and at the end you get a quantum system of particles," Wright said. "The particles end up in a certain state, and you want to understand if that's the state they're supposed to be in. It's a fundamental fact about quantum mechanics that you can't learn the complete state of a particle — for instance, you can't simultaneously learn its position and velocity. But if you had identical particles, you could learn the position from one and the velocity from another." The problem is, what is the minimum number of particles required to do that?

It turns out that for an array of qubits, the number of proxy particles you need to verify the states of the original particles escalates rapidly. "A physical system can be assigned a dimension, which in the case of a quantum computer grows exponentially with the number of qubits available," said Costin Bădescu, a doctoral student in computer science working with O'Donnell. "The minimum number of copies you need scales linearly with regard to the dimension of the system."

QUANTUM INFORMATION THEORY

O'Donnell and Wright's analysis determined how to find the lower bound on that number. Their work could markedly increase the efficiency for calibrating a quantum computer. "Almost every quantum experimentalist is going to want to do a validation at the close of their experiment," O'Donnell said. Using an array of identical particles, experimentalists could check the gates on a quantum computer.

In a scenario where time is limited, efficiency is critical. O'Donnell described a recent quantum teleportation experiment, where the characteristics of one qubit are transmitted to a distant qubit. "In this case it was between a qubit on Earth and one on a satellite," O'Donnell said. "They had to check how close the state on the qubit on the satellite was to the qubit on Earth, but they only had about six minutes a day to do it because of interference from light from the moon and such. So in that case, you are really motivated to use as few copies as possible."

"Ryan and John are pretty much at the top of the game on the theoretical aspects of this," said Vikesh Siddhu, a doctoral student in physics. "One of the basic tenets of quantum computing, laid down by

> "We have to be cognizant of how quantum information science and this technology is moving in a multidimensional way."
>
> —Jason Larkin (E 2013)

David DiVincenzo [in the DiVincenzo Criteria as they are known, published in 2000 and positing the minimum requirements for quantum computing], is that you must be able to initialize your computer in a simple state and then change that state as necessary. Quantum tomography can tell if you have achieved what you intended."

Part of quantum information theory is circumscribing the domain of the possible, Siddhu said. "We study theoretical limits that give upper and lower bounds on how well one can send information using quantum states." Siddhu's recent work looks at noisy quantum channels, whose ability to send information is not well understood. The problem here involves determining the capacities of quantum information transfers given the inherent instability of quantum elements. "Any channel that sends quantum information can be noisy. Knowing the limits of these channels would be vital for quantum computers and quantum memories," Siddhu said.

PUSHING BOUNDARIES

The theoretical work O'Donnell, his team and others are pursuing seems rarified at times, but is part and parcel of creating a foundation of knowledge that experimentalists and software developers can use as quantum computing becomes more viable, according to Siddhu. "We are creating some tools and studying the theoretical limits of what a quantum computer and a quantum communication device can do," he said.

"All these sorts of things come into play when we do our research," said Jason Larkin (E 2013), a researcher at the Software Engineering Institute's Emerging Technology Center who works with quantum computing. "We have to be cognizant of how quantum information science and this technology is moving in a multidimensional way. Ryan's work is looking far ahead and thinking about the ultimate scaling of things. Finding the bounds on the optimal, and answering questions like, 'Can you get me to 99% of the optimal, or 96% rather than the 93% of a classical computer?' can have huge consequences if you are looking at something like large-scale logistics."

It is generally accepted that if quantum computers obtain the functionality foreseen for them, the computational increase over classical computers will be astronomical for some tasks. But hype aside, quantum computers created thus far are limited in their abilities, typically sporting qubits numbering only in the dozens. No small feat, but nowhere near able to fulfill the more extravagant of quantum computing's promises. There are also questions about the kinds of problems quantum computing might legitimately be able to tackle.

On this note, O'Donnell remains ambivalent. "While I'm not an expert on the experimental side of things, I do think they will be able to build large-scale quantum computers in 10-20 years. It's like building a space station on Mars. It would be very hard — requiring tremendous theoretical and engineering efforts — and a lot of money, but I believe it could be done.

"I'm less bullish on whether quantum computers will change the way we eat, sleep and play," he said. "It's expected there will be applications for things like quantum chemistry, but from a theory point of view, people have been thinking about what you can do with quantum computers for 25 years, and beyond things like Shor's or Grover's algorithms, we don't have a lot more examples. So while I'm cautious about whether they will revolutionize everything, I'm very interested in setting up the mathematical framework for what can be accomplished." ■