TATA CONSULTANCY SERVICES

Preparing for Quantum Computing

Insights from TCS research partner TIFR

R Jaikumar,
R Vijayraghavan

TCS has established a partnership with Tata Institute of Fundamental Research (TIFR), one of the prime research institutes in India to collaborate and cocreate new solutions on the quantum computing platform. TIFR has successfully built the first superconducting circuit-based quantum computer in India with 3 qubits. TIFR is on course to build a 7-qubit quantum computer and TCS has partnered with TIFR to enable cloud access to this quantum computer. This interview reinforces some quantum computing facts, enriched by TIFR team's experimentation.

What gives quantum computing some unique capabilities?

Dr. R Vijayaraghavan: A classical computer uses a bit as the fundamental unit for storage and processing. It can take one of the two possible states at any time, that is, 0 or 1. On the other hand, a quantum computer uses a quantum bit or qubit as the building block. The laws of quantum mechanics allow the system to use a combination of both states, that is, 0 and 1. When extended to many qubits, the number of possible states that can exist simultaneously becomes enormous and gives a quantum computer some unique capabilities.

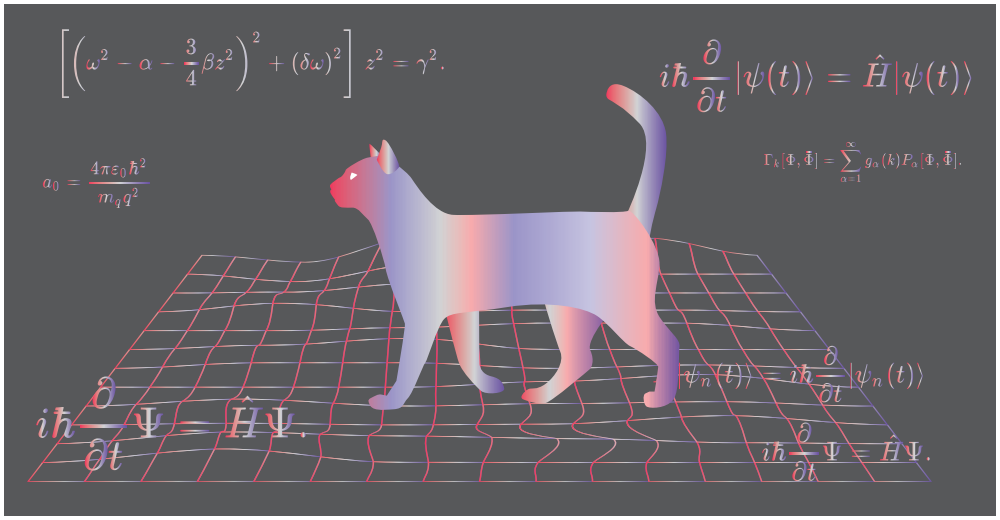
Dr. Jaikumar: In quantum computation, the state of the computer at any point is modeled as a superposition of basis states $|0\rangle$ and $|1\rangle$. The superposition assigns to each basis state a complex amplitude α and β, respectively, which behaves roughly as the square root of the probability. The subsequent evolution of the state is modeled as unitary operations (for example, rotations, reflections, etc.) on the state, which preserve the sum of the squares of the amplitudes ($|\alpha|^2 + |\beta|^2 = 1$) associated with the basis states. Unitary operations allow for cancellation of amplitudes, which gives quantum computation its additional power.

For example, in classical computation, the state of a bit is a probability distribution over the set {0, 1}, so it is determined by a probability vector of the form (p_0, p_1) where $p_0 + p_1 = 1$. A typical evolution might replace the bit by a random bit if it is 1, and leave it as it is if it is 0. This would modify the state (p_0, p_1) to $(p_0 + p_1/2, p_1/2)$. This operation corresponds to the application of the stochastic matrix:

$$\begin{pmatrix} 1 & 0.5 \\ 0 & 0.5 \end{pmatrix}$$

In quantum computation, the state of a qubit is described by a unit vector of the form $\alpha|0\rangle + \beta|1\rangle$, with complex amplitudes α and β such

Unitary operations allow for cancellation of amplitudes, which gives quantum computation its additional power.



© Shutterstock

Figure 1 : *Illustration of Erwin Schrödinger's cat explaining a state known as quantum superposition.*

that $|\alpha|^2 + |\beta|^2 = 1$. For example, a unitary operation can change this to $((\alpha+\beta)/\sqrt{2}, (\alpha-\beta)/\sqrt{2})$, which corresponds to the unitary matrix:

$$1/\sqrt{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

This matrix corresponds to the single-qubit Hadamard gate.

Can quantum computing (QC) perform search functions more efficiently?

Dr. J: If we are given access to a table with "n" entries and are required to locate where a particular item "x" is, a quantum algorithm namely Grover's algorithm would (with high probability) locate the element in about sqrt{n} steps. Whereas, it can be shown that every classical algorithm would need around "n" queries for this problem.

One must, however, be cautious in interpreting this claim. For Grover's quantum algorithm to work, we must have the ability to probe the table with qubits in superposition. We cannot just build the quantum algorithm over the current implementations of Relational Database Management System (RDBMS). The quantum algorithm promises a reduction in the number of queries made to the database. Between two queries, there is some quantum processing that is done in the algorithm. In an ideal quantum computer, this will account for algorithmic overhead.

If the RDBMS allows quantum access, then in principle, one can locate an element in a table of 4 elements using just one query, assuming each entry appears only once. The exact number of queries needed for table with "n" elements is complicated, but it grows as (pi/4) sqrt{n}. So for a table of 100 entries, one would need about 8 quantum queries.

How can teams build and operate their own quantum computers? What are the difficulties?

Dr. V: There are several competing quantum hardware platforms, leveraging trapped ions, superconducting circuits, or others. Each has its own

> Understanding of linear algebra and some basic probability is usually sufficient to work in the area of quantum algorithms

challenges. However, the most important challenge is to build sufficient number of coherent qubits with high fidelity, that is qubits, and quantum gates with low error rates, implement error correction, and build a computer with enough qubits to have access to a large enough computational space (as "n"-qubit Hilbert space). The problem is that quantum systems are fragile and very difficult to control, manipulate, and measure.

Is there a simple way to understand some basic concepts of quantum computing, such as superposition and entanglement, without resorting to mathematics?

Dr. J: It is possible to compare superposition and entanglement with classical notions of random variables and dependence, respectively. Such qualitative understanding however has its limitations. Some use of basic linear algebra is unavoidable to properly appreciate the significance of superposition and entanglement.

What difference will a software engineer experience when writing programs for a quantum computer?

Dr. J: Quantum computation has not developed sufficiently where one can write a program in a high-level language. It is difficult to predict the precise form quantum computers will take.

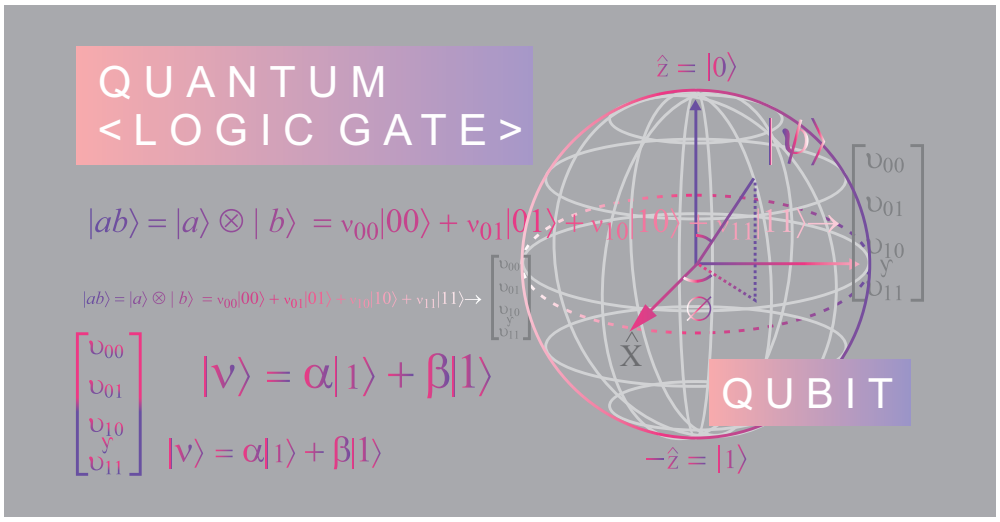
For a general programmer, access to quantum computers might well be provided in the form of libraries. When a call is made to a subroutine responsible for some specialized task, perhaps the task will be delegated to the quantum hardware to accomplish, and the results will be conveyed to the classical program. If quantum computers do develop, most software engineers will use quantum computing through such an interface, without having to deal with quantum nitty-gritties.

Is the knowledge of quantum mechanics essential to design algorithms for the quantum computer?

Dr. V: Yes, a basic knowledge of quantum mechanics is needed but the necessary rules are easy and straightforward to grasp. The tricky part is to figure out how to exploit these new rules to solve a particular problem.

Dr. J: The basic algorithms in quantum computing, as they are approached by theoretical computer scientists, are based on a small number of principles. Understanding of linear algebra and some basic probability is usually sufficient to work in the area of quantum algorithms. Knowing quantum mechanics helps in many ways. Many of the computations involved in quantum algorithms can be seen as discrete manifestations of physical phenomena: for example, the two-slit experiment and the Deutsch–Jozsa algorithm. Furthermore, understanding advanced ideas, such as quantum random walks, shed light on what might be possible using quantum algorithms. Conversely, narrowing the study to the discrete setting often allows one to understand quantum phenomena in a simple way, that otherwise appear rather inaccessible to an average computer scientist.

Quantum computation has not developed sufficiently where one can write a program in a high-level language.



Can we write a program in C or Python and expect it to run on a quantum computer, assuming there is a reliable one with 10000 qubits?

Dr. J: A quantum computer when deployed in a regular computer is likely to serve only as an accelerator for some specialized tasks (just as a GPU). 10000 qubits might well be able to speed up some tasks by a large factor, but one must account for the additional time taken in interfacing with quantum hardware, etc.

Dr. V: The exact programming language doesn't matter in the sense that the high-level language could be anything. However, the software environment would need to have some compiler which would take the code and convert it into instructions that can be executed on a quantum processor. If C or Python developers don't include the relevant functions in their software platforms, then one cannot write a program for a quantum computer. If the question is whether a regular classical program written in C/ Python would run on a quantum computer, the answer is no; only quantum algorithms should run on a quantum computer.

Are there any limits on the length of a quantum program? How long can a quantum program run today? Do I have to run a program many times or will a one-time run suffice?

Dr. V: In principle, there is no limit to the length of a quantum program. However, today's quantum computers do not use error correction and hence are prone to errors. The longer the program, the higher the chances of an error. Qubits with superconducting processors have coherence times of about 100 microseconds. Any algorithm which takes significantly longer than that time will be prone to errors. Running a program once or many times will depend on the nature of the algorithm.

Many cryptographic algorithms based on number theoretic functions often have an underlying periodic structure. By learning this periodic structure, one can mount and attack such cryptographic protocols. QFT can unravel this periodic structure rather efficiently.

What would one not be likely to use a quantum computer for?

Dr. V: Well not for most of the things! Not every problem can be solved faster using a quantum computer. For example, I can't imagine needing a quantum computer for sending e-mails or word processing.

In what ways does quantum computing influence cryptography?

Dr. J: Cryptography, especially the kind based on public keys, often relies on assumptions that certain mapping that can be computed efficiently cannot be inverted. It might appear that since quantum algorithms are capable of inverting more efficiently than classical algorithms, such assumptions are violated if the adversary is in possession of a quantum computer. This is true only to a small extent and is misleading. General-purpose inversion algorithms (for example, Grover's algorithm) provide only minor improvements over classical algorithms, and do not pose a threat to cryptography.

The real threat emanates from the remarkable tool of Quantum Fourier Transform (QFT). Many cryptographic algorithms based on number theoretic functions often have an underlying periodic structure. By learning this periodic structure, one can mount and attack such cryptographic protocols. QFT can unravel this periodic structure rather efficiently. So, if a quantum algorithm for factoring numbers is implemented, we will no longer be able to use the Rivest–Shamir–Adleman (RSA) algorithm.

Anticipating such threats, several new proposals exist for basing cryptography on functions and tasks that are expected to be hard even for quantum algorithms.

Why is it that quantum chemistry is touted to be the application most likely to be speeded up by early quantum computers?

Dr. V: One of the earliest applications envisaged for quantum computers was to solve problems in quantum mechanics which are very inefficient to solve on regular computers. Quantum chemistry involves solving the Schrodinger equation to understand the properties of molecules. Scientists have figured out various ways to map problems in quantum chemistry to quantum computers. We are still far away from solving quantum chemistry problems of practical relevance, but the progress is promising.

Quantum
– *Here and Now*

While hardware development has been impeded by the challenges of qubit coherence and errors, there is much that can be done today.

Algorithms: Several new quantum algorithms have been discovered. These algorithms have been validated, thanks to the availability of quantum simulators (on classical computers) which can simulate systems as large as 49 qubits.

Today, there is a need to study and evaluate the current quantum algorithms and conceive an architecture on which the available QC platforms will fit in to solve existing or near future applications. It is then necessary to estimate the number of qubits and the error rates required to solve the problems of industry scale with quantum supremacy. This could help project the likely year when quantum computing could be a business value proposition.

Quantum on the cloud: Given the costs of owning and maintaining a quantum computer, it is very likely that most enterprises will prefer to use a quantum computer on the cloud. Enterprises could just start using cloud services to create value for themselves and their customers.

But how can we validate the results returned by the quantum computer on the cloud? These computations will be difficult to compute with classical servers. There have been some recent breakthroughs in this regard. One solution involves computing something similar to a hash which can be computed only by a quantum computer. The correctness of the hash can be verified easily by a classical computing platform.

While a reliable and practical quantum hardware will take many years to come, many alternative solutions are coming up. Examples: mem-compute [1], hardware-based spiking neural networks [2], coherent Ising machines [3], and digital annealers [4], especially when one looks at applications like optimization and its closely related fields like machine learning. More such technologies are expected to evolve soon.

As we write this, we know that not all quantum computing applications will be able to run efficiently from day one. Nevertheless, there is a tremendous opportunity for IP creation and thereafter exploitation in the search of newer quantum algorithms and use cases. However, this will require heavy investment and therefore needs careful evaluation.

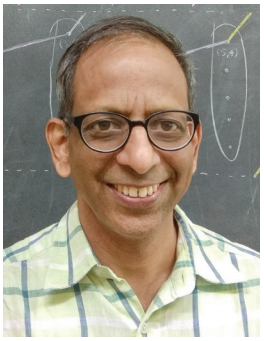
Manoj Nambiar

[1] https://www.memcpu.com/

[2] https://en.wikipedia.org/wiki/Spiking_neural_network

[3] https://www.nature.com/articles/s41534-017-0048-9

[4] https://spectrum.ieee.org/tech-talk/computing/hardware/fujitsus-cmos-digital-annealer-produces-quantum-computer-speeds



Jaikumar Radhakrishnan

Jaikumar Radhakrishnan is a Senior Professor with the School of Technology and Computer Science, Tata Institute of Fundamental Research, Mumbai. He obtained his B.Tech. (Computer Science and Engineering) from IIT Kharagpur in 1985, and his Ph.D. (Computer Science) from Rutgers University in 1991.

His research interests include randomness and computation, combinatorial and algebraic methods in complexity theory, information theory and quantum computing.

Rajamani Vijayraghavan

Rajamani Vijayaraghavan is an Associate Professor in the Dept of Condensed Matter Physics and Materials Science at TIFR, Mumbai, since December 2012. He received his Ph.D. in Applied Physics from Yale University and carried out postdoctoral research at the University of California, Berkeley. His research group at TIFR called The Quantum Measurement and Control Laboratory (QuMaC) investigates quantum phenomena in superconducting circuits. Some key highlights of the group's work include the development of a broadband ultralow noise amplifier for quantum measurements and a novel multi-qubit processor design for applications in quantum computing.

Glossary

Coherence — The merit of a particular quantum computer is determined not only by its qubit counts but also by the "coherence" of these qubits, which means how long these qubits stay in their superposition states to process information, before being decohered by external (quantum) noise. The decoherence time is usually very small, in orders of microseconds (quantum dots) to milliseconds (in electron spin qubits).

Entanglement — Entanglement is a quantum mechanical phenomenon in which the quantum states of two or more objects have to be described with reference to each other, even though the individual objects may be spatially separated

Hilbert space — Hilbert space is an abstract vector space possessing the structure of an inner product that allows length and angle to be measured

QFT — Quantum Fourier Transform (QFT) is the mathematical and conceptual framework for contemporary elementary particle physics

RSA algorithm — RSA (Rivest–Shamir–Adleman) is an algorithm used by modern computers to encrypt and decrypt messages

Superposition — Superposition is the ability of a quantum system to be in multiple states at the same time until it is measured