Quantum Computing Reading Group at KAUST

Organizational Meeting

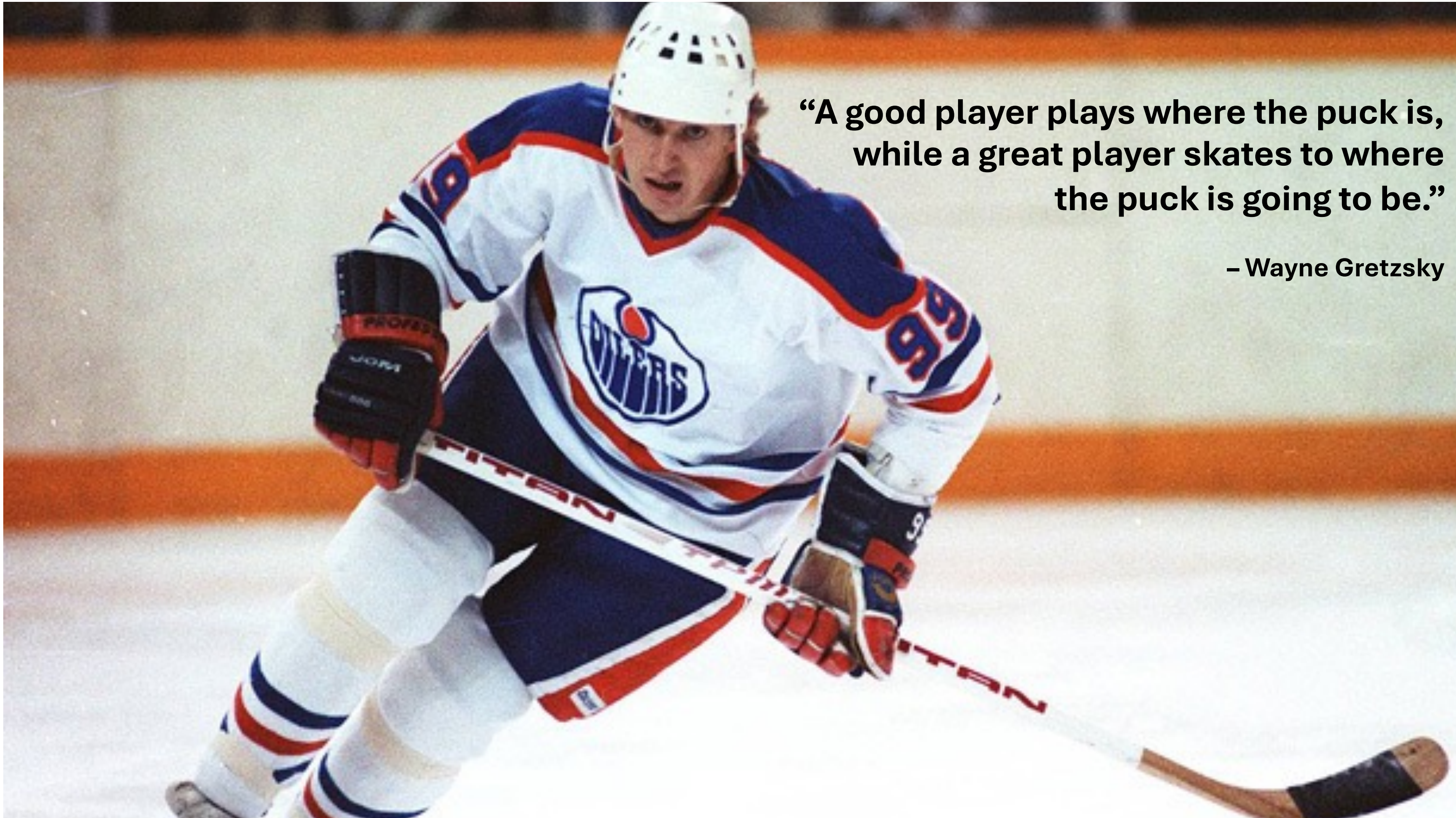
17 July 2024

Welcome to the Qommunity!

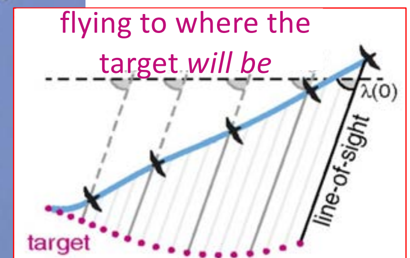
Quantum computing is here today.
Quantum advantage (over classical) is *not*… yet.

The “space race” of this decade is the search for the best qubit device for both reliability and scaling. Once “quantum Moore’s Law” appears, watch out.

A pessimist complains about the wind.
An optimist expects it to change.
A realist adjusts the sails.


"A good player plays where the puck is,
while a great player skates to where
the puck is going to be."
– Wayne Gretzsky

A falcon flies to where the prey will be...



C. H. Brighton, et al., PNAS (2017)

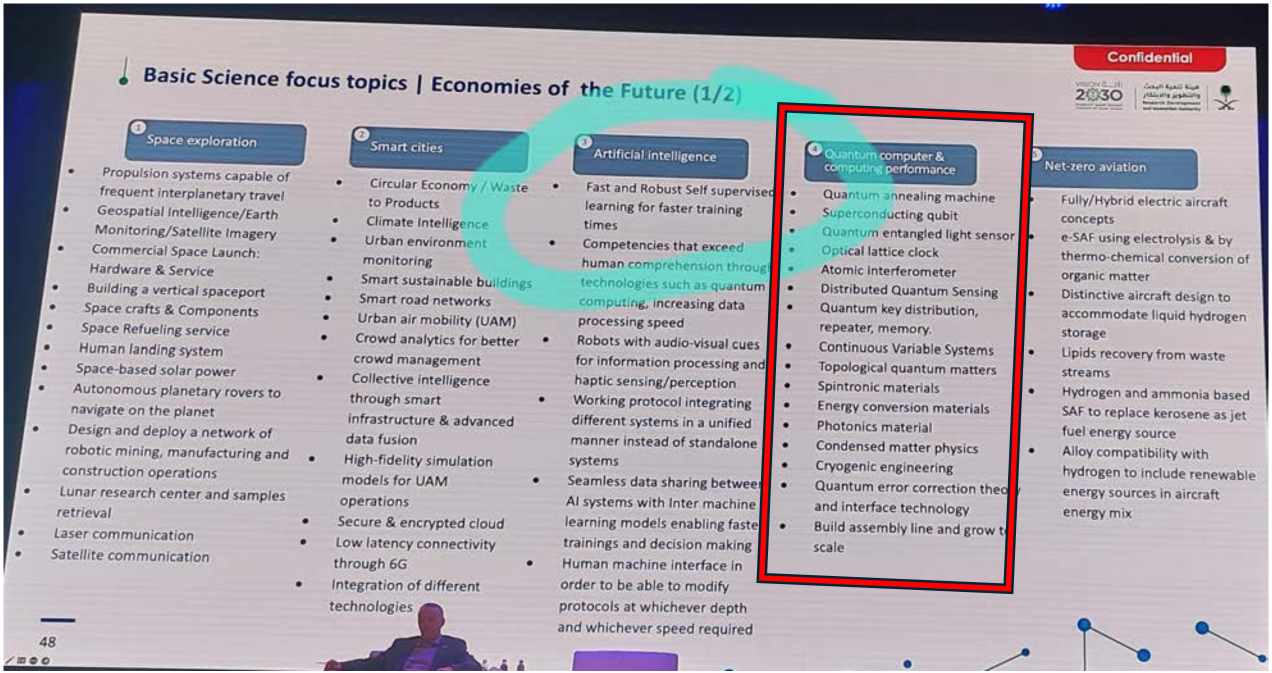
... rather than where it is

Our modest goal: to get used to quantum

“[In quantum] you don’t understand things; you just get used to them.”

In 1926 (at age 23!) Von Neumann mathematized the new physics of quantum mechanics by recognizing that quantum observables (e.g., energy, momentum, angular momentum, spin, etc.) can be represented as linear operators acting on a quantum state vector or on a wave function in an infinite-dimensional Hilbert space.

Our motivation: KSA plans a "quantum economy"



Quantum computing

- One of the three primary technologies of the “Quantum Information Sciences” (QIS)
  - Along with Quantum Sensing and Quantum Communication
- Quantum Algorithms are *mathematics*
  - Operations on ideal qubits
  - A two-state system in arbitrary superposition until read as |0> or |1>
- Quantum Hardware is *physics*
  - Qubits can be built from a variety of physical devices that are sufficiently small and protected from “noise”
- Quantum computing applies quantum algorithms on physical qubits or emulates them in classical computer hardware

Quantum

noun: **quantum**; *plural noun:* **quanta**

1. a discrete quantity of energy proportional in magnitude to the frequency of the radiation (Planck's constant, $h \sim 6.6 \times 10^{-34}$ Joule-seconds)
2. a discrete amount of any other physical quantity, such as momentum or electric charge
3. a required or allowed amount
4. a share or portion

adjective: **quantum**

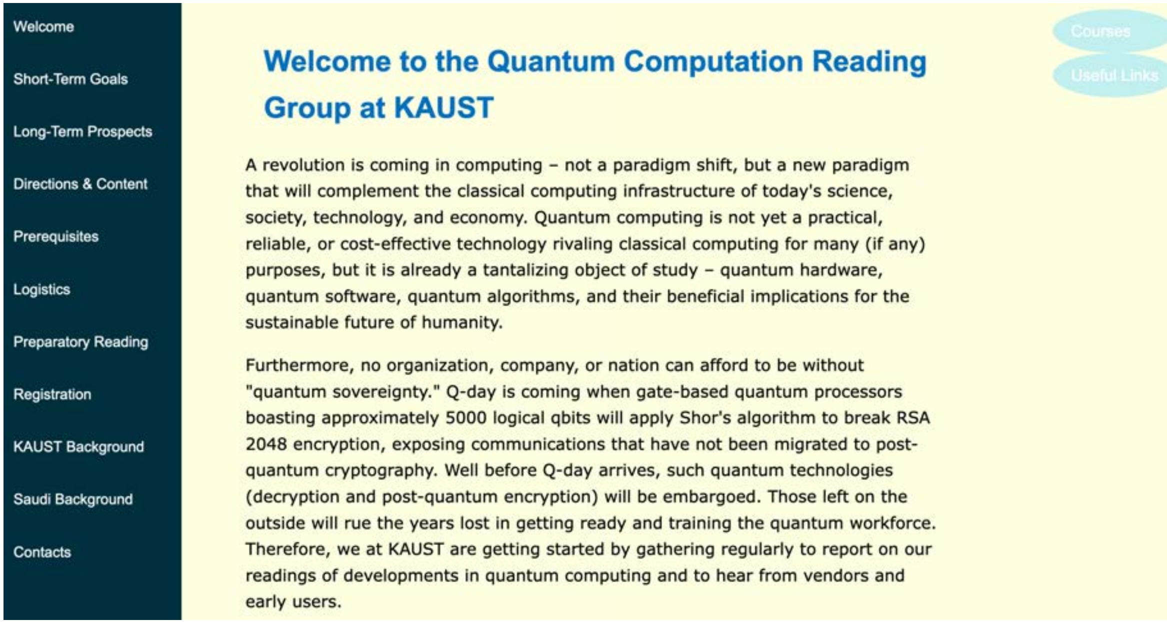
1. subject to discrete quantization (as opposed to "continuous" or "infinitesimal")

From Latin: **quantus**; *related to English:* **quantity** *or* **quantized**

Organizational meeting agenda

- a roundtable on the objectives of all who are participating in the first meeting
- a short introductory lecture by one of our students sketching the state of quantum computing
- a short update from me on Saudi Arabia's initiative in quantum computing with the World Economic Forum
- a discussion from Samar on upcoming educational offerings from vendors
- selection of a reading for discussion at our next meeting
- organizational details & some diverse resources
- a ceremonial reading of a quantum computing-themed poem "Quantum Dynamics"

Quantum Computing Reading Group (QCRG)



Welcome
Short-Term Goals
Long-Term Prospects
Directions & Content
Prerequisites
Logistics
Preparatory Reading
Registration
KAUST Background
Saudi Background
Contacts

Courses
Useful Links

Welcome to the Quantum Computation Reading Group at KAUST

A revolution is coming in computing – not a paradigm shift, but a new paradigm that will complement the classical computing infrastructure of today's science, society, technology, and economy. Quantum computing is not yet a practical, reliable, or cost-effective technology rivaling classical computing for many (if any) purposes, but it is already a tantalizing object of study – quantum hardware, quantum software, quantum algorithms, and their beneficial implications for the sustainable future of humanity.

Furthermore, no organization, company, or nation can afford to be without "quantum sovereignty." Q-day is coming when gate-based quantum processors boasting approximately 5000 logical qbits will apply Shor's algorithm to break RSA 2048 encryption, exposing communications that have not been migrated to post-quantum cryptography. Well before Q-day arrives, such quantum technologies (decryption and post-quantum encryption) will be embargoed. Those left on the outside will rue the years lost in getting ready and training the quantum workforce. Therefore, we at KAUST are getting started by gathering regularly to report on our readings of developments in quantum computing and to hear from vendors and early users.

(See https://qcrg.kaust.edu.sa)

Our Short-Term Goals

- Identify thrusts in the KAUST research mission that may benefit currently or in the future from quantum computation
- Place KAUST on the "on-ramp" for a significant thrust of the Economies of the Future RDIA pillar, which is likely to become a Saudi national initiative in 2025
- Propose a "wish list" of speakers for visits to KAUST, potentially as a part of a workshop on quantum computation to be offered Kingdom-wide in 2025
- Prepare the KAUST community to make early use of quantum hardware acquired by NEOM (ORCA) and Aramco (Pasqal), as well as quantum computing systems available remotely for free or low-cost exploration in research clouds abroad
- Burst the hype bubble of quantum computing and come to a realistic appraisal of its evolving implications for advancing science and engineering

(See https://qcrg.kaust.edu.sa)

Long-Term Prospects

- Spawn additional specialty groups, as appropriate, to go deeper into aspects of quantum computation relevant to particular areas but requiring more background in physics, mathematics, or computer science than the group has a whole possesses, such as quantum computing and materials discovery, quantum computing and optimization, quantum computing and machine learning, quantum computing and cybersecurity, etc.
- Arrive at a syllabus for a three-credit KAUST graduate course in quantum computation to be proposed first locally then, after refinement, on-line
- Evaluate the prospects of a quantum attached processor (quantum processing unit, or QPU) for a classical computing system in the KAUST Supercomputing Laboratory, possibly Shaheen3

(See https://qcrg.kaust.edu.sa)

Directions & Content

- Participant-led presentations of research papers on quantum computation, such as the 435 papers describing the 65 algorithms in the Quantum Algorithm Zoo
- Presentations from the major academic quantum computing research centers
- Presentations from the quantum software, hardware, and services vendor community, such as the 79 quantum computing companies listed at The Quantum Insider
- Hands-on exercises using quantum frameworks such as (to name a few) cuQuantum, PennyLane, Qisket, Cirq, etc.

(See https://qcrg.kaust.edu.sa)

Prerequisites

- Willingness to confront the unknown and the mysterious and perhaps to be removed from familiar foundations
- Commitment to be patient with what may appear at times to be a too slow or a too fast pace for the group as a whole

(See https://qcrg.kaust.edu.sa)

Preparatory Reading

- Olivier Ezratty, *Understanding Quantum Technologies*, 2023
- Alexander Dalzell et al., *Quantum Algorithms*, 2023
- Torsten Hoefler et al., *Disentangling Hype from Practicality: On Realistically Achieving Quantum Advantage*, 2023
- Hyperion, *4th Annual Global QC Market: Robust and on the Rise*, 2024
- World Economic Forum, *State of Quantum Computing: Building a Quantum Economy*, 2022
- Saudi Center for the Fourth Industrial Revolution, *Quantum Economy Project, First Workshop*, 2024

Courtesy of Dr. Samar Aseeri, who will co-organize the group, these readings are available at https://github.com/samaraseeri/project_downloads. They include descriptions of high-level Saudi expectations, a global market analysis, an assessment of the crossover point of classical to quantum advantage, an introduction to quantum computing technologies, and introductions to numerous topics from the quantum computing perspective in physics, chemistry, optimization, cryptanalysis, finance, and machine learning.

(See https://qcrg.kaust.edu.sa)

KAUST Background

In October 2023, three commercial quantum computing companies ran orientation sessions at KAUST, in person or by teleconference, and several other such companies have recently expressed interest in helping to develop the KAUST quantum computing ecosystem. These sessions were well received, but probably failed to reach some interested members of the community. The Quantum Computation Reading Group (QCRG) will provide a nucleus for publicity of future such sessions.

KAUST's Shaheen-3 is a hardware platform that will be able to emulate up to an estimated 50 reliable qbits for quantum algorithm development.

(See https://qcrg.kaust.edu.sa)

Saudi Background

Many quantum technologies, including quantum computing, are listed in the Saudi Arabia's Research, Development and Innovation Authority (RDIA) "Economies of the Future" Pillar.

Saudi Arabia is a member of the World Economic Forum's Quantum Economy Hub. According to https://www.weforum.org/agenda/2024/04/towards-saudi-blueprint-robust-quantum-economy/, Saudi Arabia's Vision 2030 is a national strategic plan that aims to diversify the country's economy beyond oil and transform its society into a vibrant, ambitious society. While still in its early stages, the field of quantum technologies holds immense potential to contribute significantly to these ambitious goals.

Quantum technologies and applications hold tremendous potential to revolutionize various sectors, such as finance and logistics, healthcare, Artificial Intelligence (AI), cybersecurity, and energy.

(See https://qcrg.kaust.edu.sa)

Majlis roundtable

(See UNESCO video @ https://www.youtube.com/watch?v=59KQbS1DMpQ)

Introduction to Quantum Computing

by Karim Saifullin, PhD candidate, ECE

Quantum Computing Initiatives in the KSA

by David Keyes, CEMSE Professor,
Advisory Board of the Center for the Fourth Industrial Revolution (C4IR), KSA

FOURTH INDUSTRIAL REVOLUTION

Towards a Saudi blueprint for a robust quantum economy

Apr 28, 2024

The Forum's Quantum Economy Blueprint provides a roadmap to building and enabling quantum ecosystems equitably. Image: REUTERS/Mohammed Benmansour

FORUM INSTITUTIONAL

The world is heading for a 'quantum divide': here's why it matters

Jan 18, 2023

Quantum technology will exponentially accelerate the Fourth Industrial Revolution. But more than 150 countries do not yet have a quantum strategy.

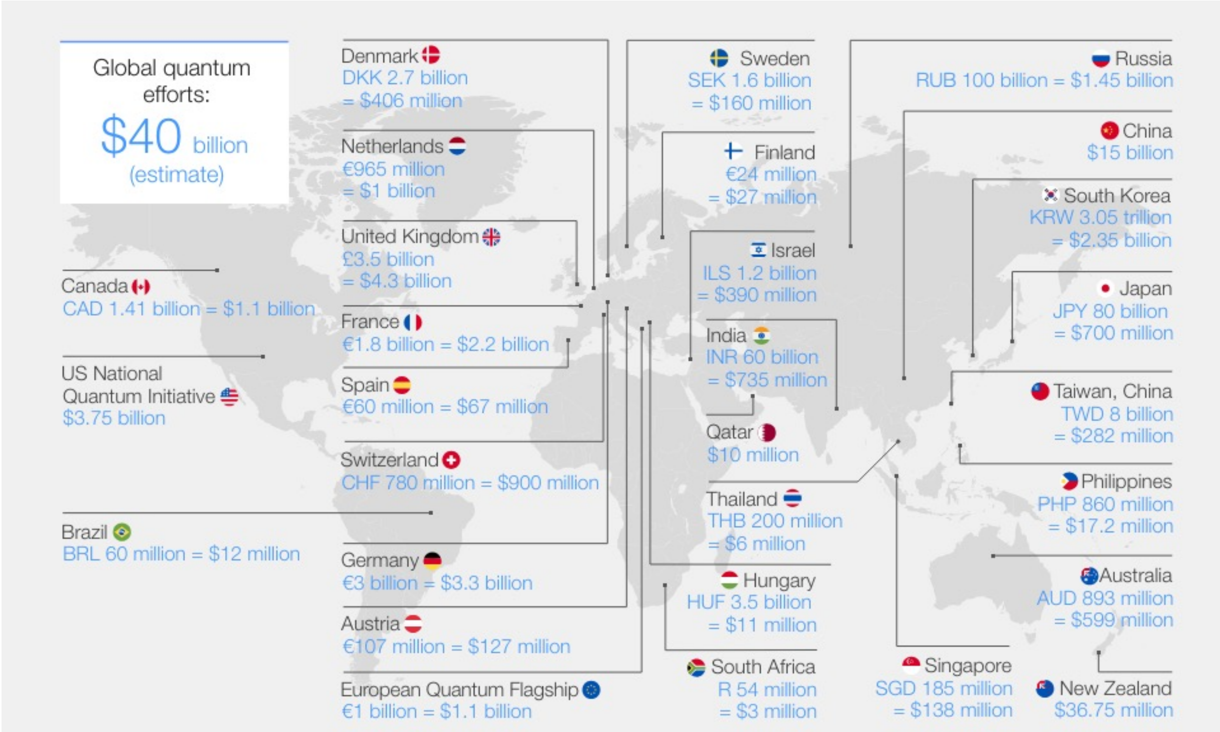
Image: Getty Images/iStockphoto

Saudi Quantum Economy Workshop, 6 Feb 2024

- In attendance: 8 from PIF, plus Aramco, SABIC, STC, SAMA, NEOM-Oxagon, KACST, KFUPM, KSU, WEF, C4IR
- Sessions led by: KACST and KFUPM
- Discussions w/ ORCA, Xanadu, Pasqal & Quantinuum

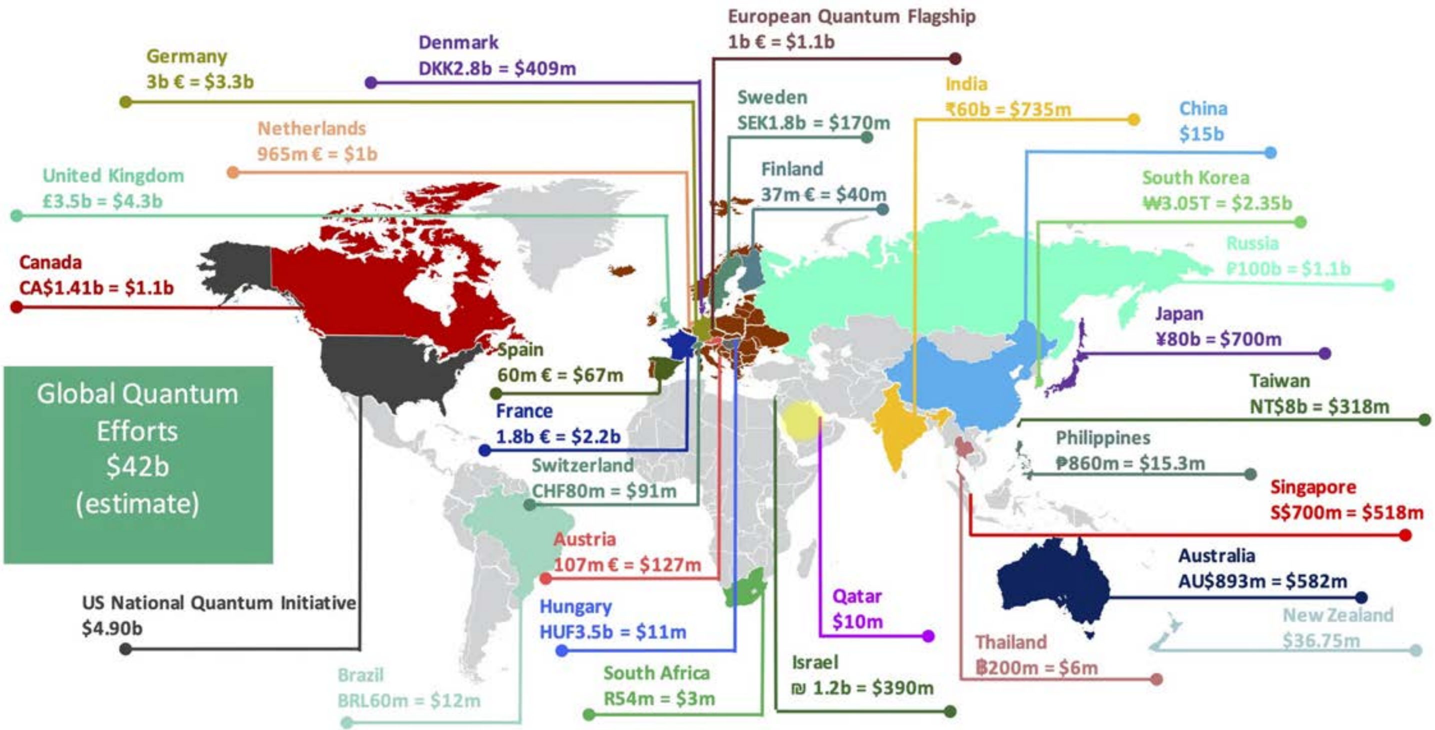
Takeaways re: Saudi Quantum Economy

- Main motivations for jump-starting the Saudi Quantum Economy
  - cybersecurity, the $1B motivation of G20 economies (FOMO)
  - to make everything “run 1000x faster”
  - to save energy devoted to computation
- The first one is justified; the latter two are not for now
- Schor’s algorithm offers superpolynomial to exponential speedup factoring large primes and thus cracking RSA encryption
  - RSA == Rivest, Shamir, Adleman, founded in 1982
  - Early decryptors get access to troves of stored encrypted data on their rivals
- Quantum-generated encryption keys offer protection again quantum decryption



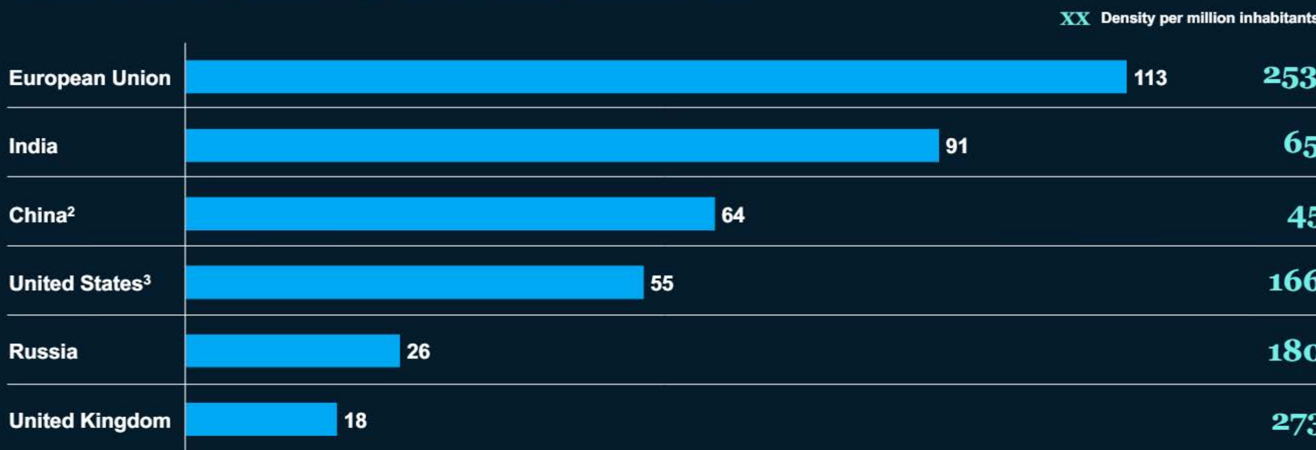
Note: Not exhaustive; timelines for funding vary by country.

Sources: "Overview of Quantum Initiatives Worldwide 2023", *QURECA*, 19 July 2023, https://qureca.com/overview-of-quantum-initiatives-worldwide-2023/; Department of Industry, Science and Resources, Australia; ETH Domain (ETH Zurich, EPFL, PSI).


Global Quantum Efforts
$42b
(estimate)
European Quantum Flagship
1b € = $1.1b
Denmark
DKK2.8b = $409m
Germany
3b € = $3.3b
Sweden
SEK1.8b = $170m
India
₹60b = $735m
China
$15b
Netherlands
965m € = $1b
Finland
37m € = $40m
United Kingdom
£3.5b = $4.3b
South Korea
₩3.05T = $2.35b
Russia
₽100b = $1.1b
Canada
CA$1.41b = $1.1b
Japan
¥80b = $700m
Spain
60m € = $67m
Taiwan
NT$8b = $318m
France
1.8b € = $2.2b
Philippines
₱860m = $15.3m
Switzerland
CHF80m = $91m
Singapore
S$700m = $518m
Austria
107m € = $127m
Australia
AU$893m = $582m
US National Quantum Initiative
$4.90b
Hungary
HUF3.5b = $11m
Qatar
$10m
New Zealand
$36.75m
Thailand
฿200m = $6m
Israel
₪ 1.2b = $390m
Brazil
BRL60m = $12m
South Africa
R54m = $3m

The European Union has the highest number and concentration of QT talent.

Absolute number of graduates in QT-relevant fields (thousands),[1] 2021



~ 367k Number of graduates in QT-relevant fields[3]

[1]Graduates of master's level or equivalent in 2021 in biochemistry, chemistry, electronics and chemical engineering, information and communications technology, mathematics and statistics, and physics.
[2]High-level estimates.
[3]The actual talent pool for the United States may be larger, as bachelor programs are longer and master's programs are less common.

Source: National government websites; OECD

KSA and the WEF C4IR'S Quantum Economy Project

The emergence of quantum technologies presents a new global divide, where unequal access leads to serious geopolitical and economic consequences. Saudi Arabia needs a national quantum technology strategy that focus on developing and sustaining different focus areas namely: R&D, workforce, industry growth, socio-economic impact and international collaboration. The quantum economy project provides a clear and detailed roadmap for: R&D, workforce development, industry growth, socio-economic translation, and international collaboration.

Impact:

1- Create a roadmap across academia, industry, and government to help countries develop, support and commercialize their quantum technology initiatives

2- Aid policy makers and government institutions, industry and academia with a blueprint for developing and growing a national quantum ecosystem

Goals:

1- Initiate necessary analysis, with stakeholders, to implement and develop a national quantum strategy

2- Cultivate collaborative frameworks and knowledge sharing within the quantum technology stakeholder community, leading to a more informed and efficient approach to governance

3- Promote the importance of quantum technologies to public and decision makers.

WEF's Quantum Hub & KSA's Quantum Economy Project

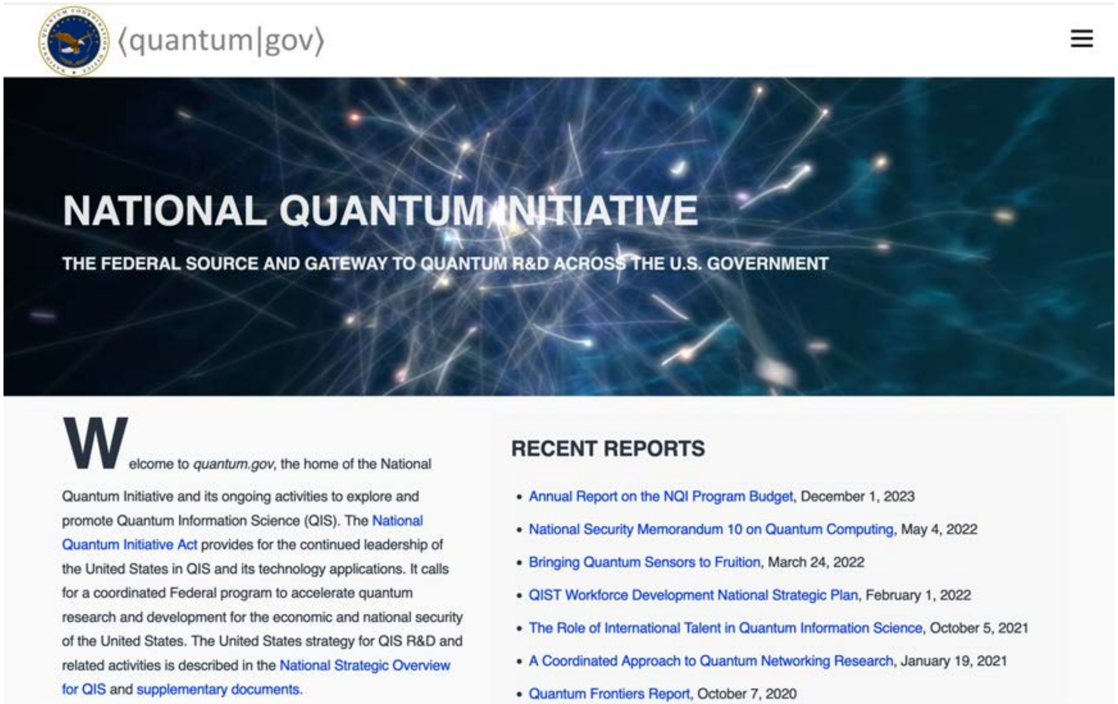
- Bartschi et al LANL Quantum use cases.pdf
- Hoefler et al Disentangling Hype 2023.pdf
- Quantum Algorithms Alexander Dalzell 2023...
- Quantum Computing in Chemistry 2024.pdf
- Rieffel et al NASA Quantum use cases.pdf
- ✓ Saudi C4IR Quantum Economy 2nd Worksho...
- ✓ Saudi C4IR Quantum Economy Project 2024...
- Sorensen Quantum Markets Hyperion 2024....
- Understanding Quantum Technologies Olivie...
- ✓ WEF State of Quantum Computing 2022.pdf

(in the QCRG repo)

Aramco signs agreement with Pasqal to deploy first quantum computer in the Kingdom of Saudi Arabia

20 May 2024

quantum.gov



⟨quantum|gov⟩

NATIONAL QUANTUM INITIATIVE

THE FEDERAL SOURCE AND GATEWAY TO QUANTUM R&D ACROSS THE U.S. GOVERNMENT

Welcome to *quantum.gov*, the home of the National Quantum Initiative and its ongoing activities to explore and promote Quantum Information Science (QIS). The National Quantum Initiative Act provides for the continued leadership of the United States in QIS and its technology applications. It calls for a coordinated Federal program to accelerate quantum research and development for the economic and national security of the United States. The United States strategy for QIS R&D and related activities is described in the National Strategic Overview for QIS and supplementary documents.

RECENT REPORTS

- Annual Report on the NQI Program Budget, December 1, 2023
- National Security Memorandum 10 on Quantum Computing, May 4, 2022
- Bringing Quantum Sensors to Fruition, March 24, 2022
- QIST Workforce Development National Strategic Plan, February 1, 2022
- The Role of International Talent in Quantum Information Science, October 5, 2021
- A Coordinated Approach to Quantum Networking Research, January 19, 2021
- Quantum Frontiers Report, October 7, 2020

quantum.gov.sa

Hmm. We're having trouble finding that site.

We can't connect to the server at quantum.gov.sa.

If you entered the right address, you can:

- Try again later
- Check your network connection
- Check that Firefox has permission to access the web (you might be connected but behind a firewall)

Try Again

Introduction to Educational Opporunities from Quantum Vendors

by Samar Aseeri, Research Scientist, CEMSE

Quantum algorithms

https://quantumalgorithmzoo.org

re on the bookmarks toolbar. Manage bookmarks...

Quantum Algorithm Zoo

This is a comprehensive catalog of quantum algorithms. If you notice any errors or omissions, please email me at spj.jordan@gmail.com. (Alternatively, you may submit a pull request to the repository on github.) Although I cannot guarantee a prompt response, your help is appreciated and will be acknowledged.

Algebraic and Number Theoretic Algorithms

Algorithm: Factoring
Speedup: Superpolynomial
Implementation: Classiq
Description: Given an n-bit integer, find the prime factorization. The quantum algorithm of Peter Shor solves this in $\widetilde{O}(n^3)$ time [82,125]. The fastest known classical algorithm for integer factorization is the general number field sieve, which is believed to run in time $2^{\widetilde{O}(n^{1/3})}$. The best rigorously proven upper bound on the classical complexity of factoring is $O(2^{n/4+o(1)})$ via the Pollard-Strassen algorithm [252, 362]. Shor's factoring algorithm breaks RSA public-key encryption and the closely related quantum algorithms for discrete logarithms break the DSA and ECDSA digital signature schemes and the Diffie-Hellman key-exchange protocol. A quantum algorithm even faster than Shor's for the special case of factoring "semiprimes", which are widely used in cryptography, is given in [271]. If small factors exist, Shor's algorithm can be beaten by a quantum algorithm using Grover search to speed up the elliptic curve factorization method [366]. Additional optimized versions of Shor's algorithm are given in [384, 386, 431]. There are proposed classical public-key cryptosystems not believed to be broken by quantum algorithms, *cf.* [248]. At the core of Shor's factoring algorithm is order finding, which can be reduced to the Abelian hidden subgroup problem, which is solved using the quantum Fourier transform. A number of other problems are known to reduce to integer factorization including the membership problem for matrix groups over fields of odd order [253], and certain diophantine problems relevant to the synthesis of quantum circuits [254].

Algorithm: Discrete-log
Speedup: Superpolynomial
Description: We are given three n-bit numbers a, b, and N, with the promise that $b = a^s \mod N$

Navigation

- Algebraic & Number Theoretic
- Oracular
- Approximation and Simulation
- Optimization, Numerics, & Machine Learning
- Acknowledgments
- References

Translations

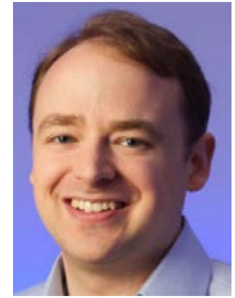
This page has been translated into:
Japanese

Other Surveys

For overviews of quantum algorithms I recommend:

- Nielsen and Chuang
- Childs
- Preskill
- Mosca
- Childs and van Dam
- van Dam and Sasaki
- Bacon and van Dam
- Montanaro
- Hidary

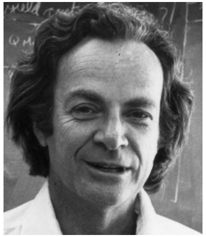
Survey of 435 papers (1982-2021)
60 Algorithms



c/o Stephen Jordan
PhD Physics, 2008, MIT

Currently:
- Google's Quantum AI

Previously:
- Computing and Communications
- Theory Group, NIST
- Institute
- for Quantum Information, Caltech



Int. J. Theor. Phys. **21**:467-488, 1982

Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

1. INTRODUCTION

On the program it says this is a keynote speech—and I don't know what a keynote speech is. I do not intend in any way to suggest what should be in this meeting as a keynote of the subjects or anything like that. I have my own things to say and to talk about and there's no implication that anybody needs to talk about the same thing or anything like it. So what I want to talk about is what Mike Dertouzos suggested that nobody would talk about. I want to talk about the problem of simulating physics with computers and I mean that in a specific way which I am going to explain. The reason for doing this is something that I learned about from Ed Fredkin, and my entire interest in the subject has been inspired by him. It has to do with learning something about the possibilities of computers, and also something about possibilities in physics. If we suppose that we know all the physical laws perfectly, of course we don't have to pay any attention to computers. It's interesting anyway to entertain oneself with the idea that we've got something to learn about physical laws; and if I take a relaxed view here (after all I'm here and not at home) I'll admit that we don't understand everything.

SIAM J. COMPUT.
Vol. 26, No. 5, pp. 1484–1509, October 1997

POLYNOMIAL-TIME ALGORITHMS FOR PRIME FACTORIZATION AND DISCRETE LOGARITHMS ON A QUANTUM COMPUTER*

PETER W. SHOR†

Abstract. A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

Key words. algorithmic number theory, prime factorization, discrete logarithms, Church's thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transforms

AMS subject classifications. 81P10, 11Y05, 68Q10, 03D10

PII. S0097539795293172

1. Introduction. One of the first results in the mathematics of computation, which underlies the subsequent development of much of theoretical computer science, was the distinction between computable and noncomputable functions shown in papers of Church [1936], Post [1936], and Turing [1936]. The observation that several apparently different definitions of what it meant for a function to be computable yielded the same set of computable functions led to the proposal of Church's thesis, which says that all computing devices can be simulated by a Turing machine.

From *Automata Studies*, Claude Shannon, ed., Princeton University Press, 1956

PROBABILISTIC LOGICS AND THE SYNTHESIS OF RELIABLE ORGANISMS FROM UNRELIABLE COMPONENTS

J. von Neumann

1. INTRODUCTION

The paper that follows is based on notes taken by Dr. R. S. Pierce on five lectures given by the author at the California Institute of Technology in January 1952. They have been revised by the author but they reflect, apart from minor changes, the lectures as they were delivered.

The subject-matter, as the title suggests, is the role of error in logics, or in the physical implementation of logics — in automata-synthesis. Error is viewed, therefore, not as an extraneous and misdirected or misdirecting accident, but as an essential part of the process under consideration — its importance in the synthesis of automata being fully comparable to that of the factor which is normally considered, the intended and correct logical structure.

Zoo of quantum algorithms (1/6)

Factorization (Shor, 1997), superpolynomial

Discrete-log (Shor, 1997), superpolynomial

Pell's Equation (Halgren, 2002), superpolynomial

Principal Ideal (Halgren, 2002), superpolynomial

Unit Group (Halgren, 2005), superpolynomial

Class Group (Halgren, 2005), superpolynomial

Gauss Sums (van Dam et al., 2002), superpolynomial

Exponential Congruences (van Dam et al., 2008), polynomial

Matrix Elements of Group Representation (Beals, 1997), polynomial

Verifying Matrix Products (Ambainis, 2002), polynomial

Zoo of quantum algorithms (2/6)

Subset-sum (Bernstein et al., 2013), polynomial

Decoding (Grice, 2014), varies

Constraint Satisfaction (Ambainis, 2004), polynomial

Quantum Cryptanalysis (Shor, 1997), various

Searching (Grover, 1997), polynomial

Abelian Hidden Subgroups (Boneh et al., 1995), superpolynomial

Non-Abelian Hidden Subgroups (Ettinger et al., 2004), superpoly.

Bernstein-Vazirani (Bernstein et al., 1993), superpolynomial

Deutsch-Jozsa (Deutsch, 1985), exponential

Formula Evaluation (Reichardt, 2011), polynomial

Zoo of quantum algorithms (3/6)

Gradients, Structured Search (Jordan, 2005), polynomial

Hidden Shift (van Dam et al., 2006), superpolynomial

Polynomial Interpolation (Boneh et al., 2013), constant factor

Pattern Matching (Bennett et al., 1997), superpolynomial

Linear Systems* (Harrow et al., 2009), superpolynomial

Ordered Search (Farhi et al., 1999), constant factor

Graph Properties, Adjacency Matrix (Durr et al., 1996), polynomial

Graph Properties, Adjacency List (Ambainis et al., 1996), polynomial

Welded Tree (Childs et al., 2011), superpolynomial

Collision Finding (Brassard et al., 1997), polynomial

* not what we usually mean, but finding expectation values of *f*(***A***)***b*,** for various *f*

Zoo of quantum algorithms (4/6)

Graph Collision (Magniez et al., 2007), polynomial

Matrix Commutativity (Itakura, 2005), polynomial

Group Commutativity (Magniez et al., 2005), polynomial

Hidden Nonlinear Structures (Childs et al., 2007), superpolynomial

Center of Radial Function (Liu, 2009), polynomial

Group Order and Membership (Mosca, 1999), superpolynomial

Group Isomorphism (Cheung et al., 2001), superpolynomial

Statistical Difference (Bravyi et al., 2011), polynomial

Finite Rings and Ideals (Arvind et al., 2006), superpolynomial

Counterfeit Coins (Terhal et al., 1998), polynomial

Zoo of quantum algorithms (5/6)

Matrix Rank (Reichardt, 2009), polynomial

Matrix Multiplication over Semi-rings (Le Gall et al., 2005), poly.

Subset Finding (Ambainis, 2007), polynomial

Search with Wildcards (Ambainis et al., 2012), polynomial

Network Flows (Ambainis et al., 2007), polynomial

Electrical Resistance (Wang, 2017), exponential

Machine Learning (Lloyd et al., 2013), varies

Finite Rings and Ideals (Arvind et al., 2006), superpolynomial

Junta and Group Testing (Ambainis et al., 1998), polynomial

Quantum Simulation (Childs, 2004), superpolynomial

Zoo of quantum algorithms (6/6)

Knot Invariants (Freedman et al., 2002), superpolynomial

Three-manifold Invariants (Alagic et al., 2010), superpolynomial

Adiabatic Algorithms (Jansen et al., 2007), unknown

Quantum Approximate Optimization (Farhi et al., 2014), superpoly.

Semidefinite Programming (Brandao et al., 2016), polynomial

Zeta Functions (Kedlaya, 2006), superpolynomial

Weight Enumerators (Knill et al., 2001), superpolynomial

Simulated Annealing (Szegedy, 2004), polynomial

String Rewriting (Janzing et al., 2010), superpolynomial

Matrix Powers (Janzing et al., 2007), superpolynomial

Suggested reading for next meeting

DOI:10.1145/3571725

What are the promising applications to realize quantum advantage?

BY TORSTEN HOEFLER, THOMAS HÄNER, AND MATTHIAS TROYER

Disentangling Hype from Practicality: On Realistically Achieving Quantum Advantage

There is a maze of hard problems that have been suggested to profit from quantum acceleration: from cryptanalysis, chemistry and materials science, to optimization, big data, machine learning, database search, drug design and protein folding, fluid dynamics and weather prediction. But which of these applications realistically offer a potential quantum advantage in practice? For this, we cannot only rely on asymptotic speedups but must consider the constants involved. Being optimistic in our outlook for quantum computers, we identify clear guidelines for quantum practicality and use them to classify which of the many proposed applications for quantum computing show promise and which ones would require significant algorithmic improvements to become practical and relevant.

To establish reliable guidelines, or lower bounds for the required speedup of a quantum computer, we err on the side of being optimistic for quantum and overly pessimistic for clas-

Key insights from Hoefler *et al*.

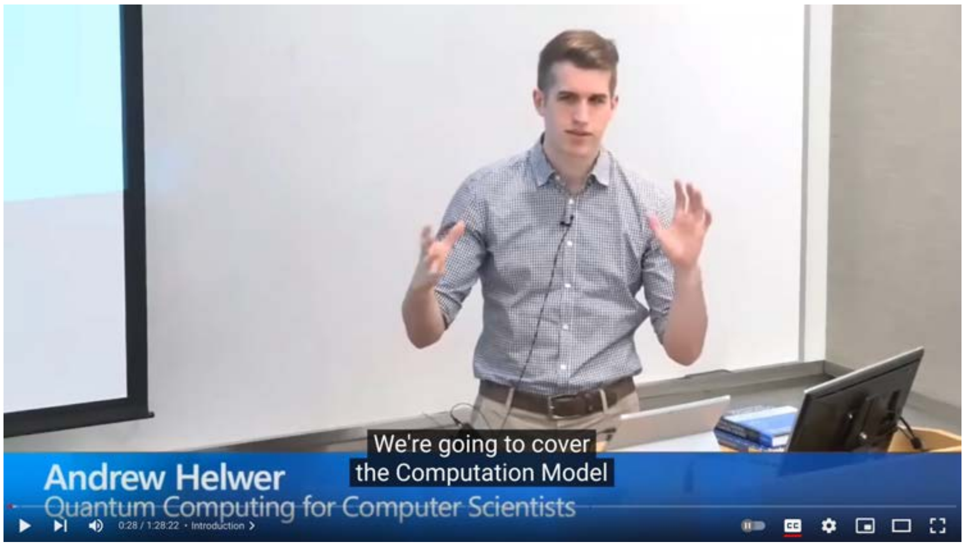
- Most of today’s quantum algorithms may not achieve practical speedups over classical counterparts on every-improving classical computers
- Material sciences and chemistry have a huge potential and we hope more practical algorithms will be invented based on our guidelines
- Due to limitations of input and output bandwidth, quantum computers will be practical for “big compute” problems on small data, not big data problems.
- Quadratic speedups delivered by algorithms such as Grover’s search are insufficient for practical quantum advantage without significant improvements across the entire software/hardware stack.

Resources for Hoefler *et al.*

- DOI:10.1145/3571725
- https://vimeo.com/811415204

A 90-minute video with “meat” for geeks

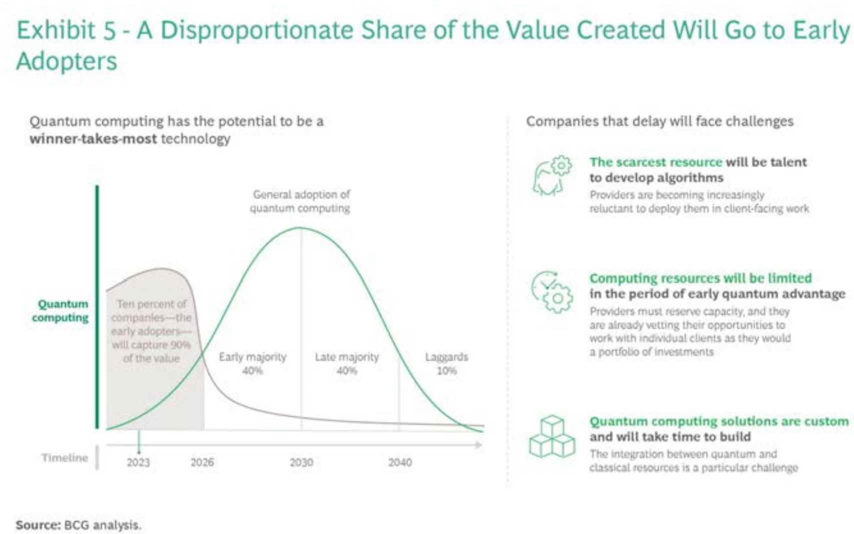
- *Quantum Computing for Computer Scientists*
- https://www.youtube.com/watch?v=F_Riqjdh2oM



Microsoft Research

A short article for corporate planners

- *Quantum Computing is Becoming Business Ready*
- https://www.bcg.com/publications/2023/enterprise-grade-quantum-computing-almost-ready



BOSTON CONSULTING GROUP

A directory for getting started in the cloud

TABLE 15-1 Public Cloud Providers and Quantum Computer Manufacturers

Company	Technology	Amazon Braket	Azure Quantum	Google Quantum AI	Access Providers*
D-Wave	Quantum annealing				x
Google	Superconducting			x**	
IBM	Superconducting				x
IonQ	Trapped ion	x	x	x	x
OQC	Superconducting	x			x
Pasqal	Neutral atom		x		x
Quantum Circuits, Inc.	Superconducting		x		x
QuEra	Cold atoms	x			x
Quantinuum	Trapped ion		x		x
Rigetti	Superconducting	x	x		x
Xanadu	Photonic				x
Total		4	5	2	10

**This specific list of quantum computers is for Strangeworks; others have somewhat different lineups.*

***Google's quantum computers are available only to selected applicants using the Google Quantum AI platform.*

Quantum Dynamics

We are getting used to you!
Like Von Neumann, so we, too.
Feynman[1] took a careful look
And since that day, we've all been hooked.
In most of life, large size takes all
But your potential's in the small,
O Quantum.

Entanglement defies belief;
Of all your miracles, it is chief!
Superposition reigns supreme:
At once, all values – what a dream!
But decoherence complicates;
We trust solutions lie in wait…
O Quantum.

To stay ahead in crypto wars
We are studying Peter Schor[2].
For large-scale search, we'll ask Lev Grover[3] –
In square root time, the search is over!
To optimize, we have a feeling
We can't do better than annealing,
O Quantum.

Qisket, Q-sharp, Silq, or Cirq –
Which language will streamline our work?
Photonic networks, neutral atoms,
Trapped ions, quantum dots,
Tunnel junctions, diamond defects …
For devices, we will take our shots,
O Quantum.

Science is but half your story;
Mystery adds to your glory.
Into our thoughts deterministic
You inject a touch artistic.
We celebrate the great expanse
Opened by your world of "chance",
O Quantum.

Watching's fun, but we want more;
Thus, we're swarming at your door.
Older souls may skip this race;
Let the younger set the pace!
Nations that in you invest
Anticipate a future blessed,
O Quantum.

You are not for the fainthearted
But we are ready to get started.
We know we have lots to learn
But bargain on a large return!
Early though your hour is
We gather where your power is,
O Quantum.

1 R. Feynman, 1982, *Simulating Physics with Computers,* Int. J. Theoretical Physics, **21**, No. 6/7.
2 P. Shor, 1997, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Computing, **26**, 1484-1509.
3 L. Grover, 1996, *A fast quantum mechanical algorithm for database search*, 28th ACM Symp. Theory Comput, pp. 212-219.

Word pairs to disambiguate

- Quantum vs. classical / traditional / conventional
  - *Best not to say "quantum vs. digital" because digital has meanings within both classical and quantum*
- Digital vs. analog
  - *Within classical, "digital" refers to discretely representable values, e.g., floats or ints, and analog to continuously representable values, e.g., voltages or currents*
  - *Within quantum, digital may refer to gate-based and analog to adiabatic systems*
- Simulation vs. emulation
  - *Within classical, "simulation" refers to approaches based on first principles laws and "emulation" to statistical or learned approaches*
  - *Within quantum, "simulation" refers to mimicking a physical quantum system, as in chemistry, and "emulation" to carrying out a quantum algorithm on a classical computer*