Title: The argument against quantum computers

Speakers: Gil Kalai

Series: Colloquium

Date: December 14, 2022 - 2:00 PM

URL: https://pirsa.org/22120066

Abstract: A quantum computer is a new type of computer based on quantum physics. When it comes to certain computational objectives, the computational ability of quantum computers is much stronger than that of the familiar digital computers, and their construction will enable us to factor large integers and to break most of the current cryptosystems.

The question of whether quantum computation is possible is one of the fascinating clear-cut open scientific questions of our time. In my lecture I will explain theoretical discoveries from the 1990s that suggested that quantum computation is possible and present my theory as to why quantum computation is nevertheless impossible.

At the crux of the matter is the study of noisy intermediate scale quantum (NISQ) computers. Based on the mathematical notions of "noise sensitivity vs noise stability" (Benjamini, Kalai, and Schramm 1999, Kalai and Kindler 2014), we identify the inherent noise sensitivity of probability distributions arising from NISQ computers. This leads to a very low complexity class of probability distributions that can be robustly described by such quantum computers; consequently, NISQ computers will not allow good-quality quantum error-correction which are the necessary building blocks for larger quantum computers.

The lecture will be self-contained and will start with a gentle explanation of some basic notions about computation, and quantum computers.

Zoom link: https://pitp.zoom.us/j/93847236670?pwd=T2Z2emZ5ZExaZTVYcTNCdU1FNkxOdz09

The Argument against Quantum Computers

Gil Kalai

Einstein Institute of Mathematics
Hebrew University of Jerusalem

Efi Arazi School of Computer
Science, Reichman University

December 14, 2022

Perimeter Institute Colloquium

Overview

It is a serious possibility that quantum computers are not possible. This is what I expect, and I have been studying this possibility since 2005.

The argument for in-principle failure of quantum computers is connected to the mathematical theory of noise stability and sensitivity, and it may have a variety of consequences to physics.

Recent claims about "quantum supremacy," starting with Google's 2019 announcement, are in tension with my theory. We need to carefully study these claims.

"A fundamental problem is to reconcile external control with isolation and reversibility."

(Daniel Friedan, 2005.)

My message: It is fundamentally impossible to reconcile external control with isolation and reversibility. (Few caveats apply.)

This is a physical law (not a mathematical theorem).

Overview (cont.): The argument against Quantum Computers

Noisy intermediate scale quantum systems (NISQ systems) represent a low-level computational ability that will not allow using them for building quantum error-correcting codes that are needed for quantum computation.

The laws of physics and computations

The extended Church Turing thesis

ECTT

Falsified by quantum computers

The quantum extended Church Turing thesis

QECTT

Widely accepted

NISQ = LDP

Implied by my theory.

Part I: Background

Computers! (Boolean circuits)

The basic memory component in classical computing is a bit, which can be in two states, “0” or “1”.

A computer (or circuit) has n bits, and it can perform certain logical operations on them. The **NOT gate**, acting on a single bit, and the **AND gate**, acting on two bits, suffice for the full power of classical computing.

Efficient computation

There are certain computational tasks that are very easy to formulate (and even to check whether a suggested answer to them is correct), but which are nonetheless impossible to perform because they require too many computational steps.

Efficient computation requires that the number of computational steps (gates) is polynomial in the number n of input bits.

Probabilistic bits and random computation

A single bit has two possible values, “zero” and “one,” and it is possible to extend the Boolean circuit model by allowing the bit to have the value “zero” with probability p and the value “one” with probability $1 - p$.

In this way, the classical computer equipped with probabilistic bits can describe a sample from a probability space of sequences of zeros and ones.

Quantum circuits: qubits

Qubits are unit vectors in $\mathbb{C}^2$: A qubit is a piece of quantum memory. The state of a qubit is a unit vector in a 2-dimensional complex Hilbert space **H** = $\mathbb{C}^2$.

There are two basic states for the qubit and we denote them by $|0\rangle$ and $|1\rangle$, (they are called ket 0 and ket 1) while the general state of the qubit is a "superposition" of these two basic states, namely, the general state of a qubit is a linear combination of the form

$$z_1|0\rangle + z_2|1\rangle,$$

where z_1 and z_2 are complex numbers satisfying

$$|z_1|^2 + |z_2|^2 = 1.$$

Quantum gates

Gates are unitary transformations: We can put one or two qubits through gates representing unitary transformations acting on the corresponding two- or four-dimensional Hilbert spaces, and as for classical computers, there is a small list of gates sufficient for the full power of quantum computing.

Quantum circuits

The memory of a quantum computer (quantum circuit) consists of n qubits and the state of the computer is a unit vector in $(\mathbb{C}^2)^{\otimes n}$. We can put one or two qubits through gates representing unitary transformations acting on the corresponding two- or four-dimensional Hilbert spaces, tensored with the identity operator on all other qubits.

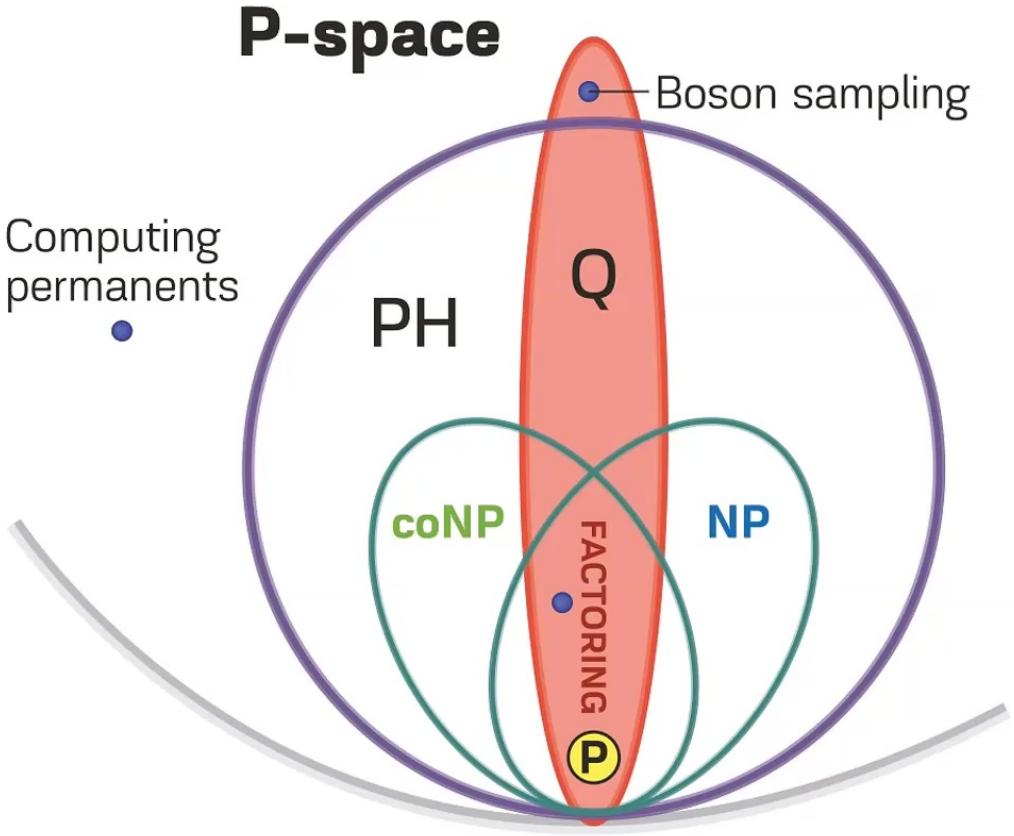
Measuring the state of k qubits leads to a probability distribution on 0–1 vectors of length k.

Shor's and Grover's algorithms

In the 1990s, Peter Shor discovered that quantum computers would allow the execution of certain computational tasks hundreds of orders of magnitude faster than regular computers and would enable us to break most current cryptosystems. Shor's algorithm is an efficient (polynomial time) quantum algorithm to factor an n-digit number.

Another important quantum algorithm from that time is Grover's algorithm.

Efficient computation and Computational complexity



Noisy quantum circuits

The term “noise” refers to a deviation of the computer from the planned program, and in the case of a quantum computer any unwanted interaction or leakage of information leads to such a deviation.

Noisy quantum circuits have the property that there exists a certain level of noise for qubits and gates.

Noisy intermediate-scale quantum (NISQ) computers: These are simply noisy quantum circuits with at most 200 (say) qubits.

NISQ devices - near term tasks

Goal 1: Demonstrate quantum supremacy on random circuits (namely, circuits that are based on randomly choosing the computation process, in advance), with 50–100 qubits. (proposed in 2015, 2016)

Goal 2: Demonstrate quantum supremacy via systems of non-interacting bosons. (proposed in 2012)

Goal 3: Create distance-5 surface codes on NISQ circuits that require a little over 100 qubits. (proposed in 2000 - 2010)

My predictions (2018)

Goal 1: Demonstrate quantum supremacy on random circuits (namely, circuits that are based on randomly choosing the computation process, in advance), with 50–100 qubits.

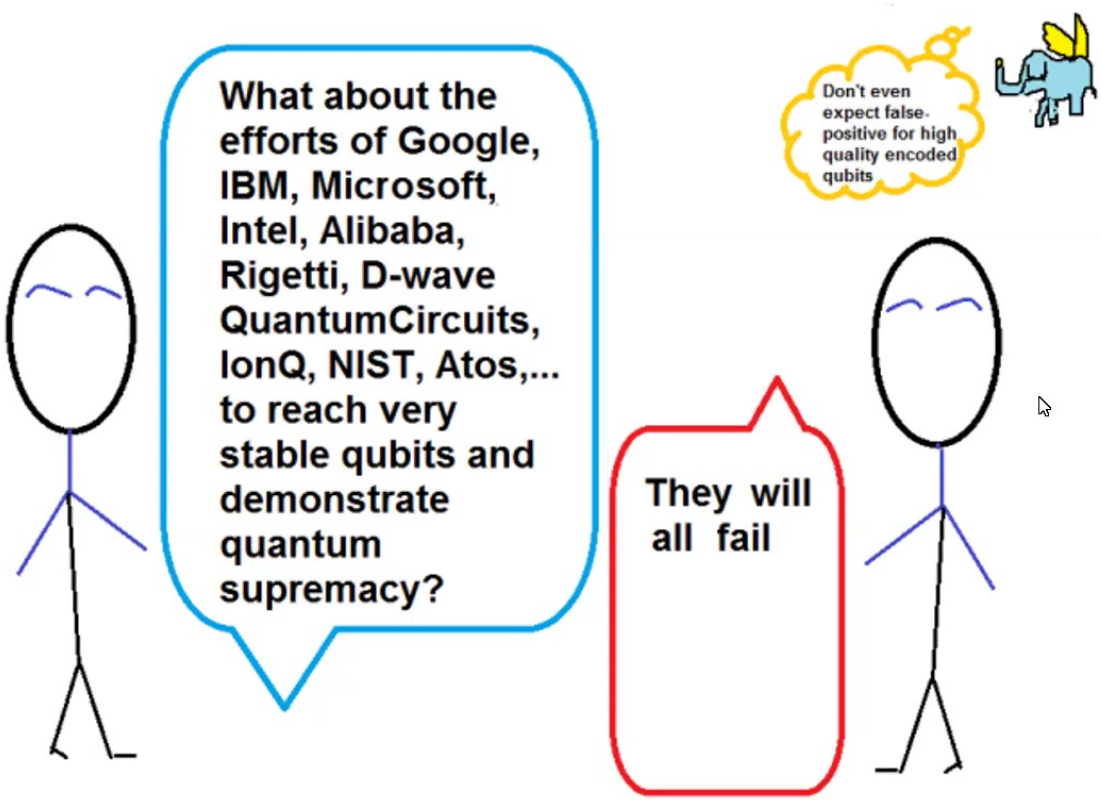
My prediction: impossible!

Goal 2: Demonstrate quantum supremacy via systems of non-interacting bosons

My prediction: impossible!

Goal 3: Create distance-5 surface codes on NISQ circuits that require a little over 100 qubits.

My prediction: impossible!



(A cartoon from 2017)

nature

Search Login

Content About Publish

NEWS | 23 October 2019

Hello quantum world! Google publishes landmark quantum supremacy claim

The company says that its quantum computer is the first to perform a calculation that would be practically impossible for a classical machine.

Elizabeth Gibney

Science

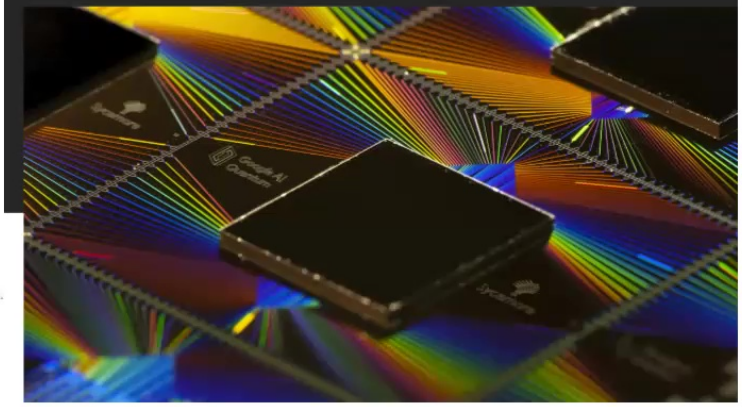
HOME > NEWS > ALL NEWS > ORDINARY COMPUTERS CAN BEAT GOOGLE'S QUANTUM...

NEWS | PHYSICS

Ordinary computers can beat Google's quantum computer after all

Superfast algorithm put crimp in 2019 claim that Google's machine had achieved "quantum supremacy"

2 AUG 2022 · 5:05 PM · BY ADRIAN CHO



Part II: The Argument Against Quantum Computers

The three ingredients of the argument against quantum computers

Noise levels for NISQ computers are inherently high and therefore:

a) Such systems cannot demonstrate significant quantum computational advantage.
b) Such systems cannot be used for the creation of quantum error-correcting codes.
c) Such systems lead to non-stationary and even chaotic probability distributions.

The reason NISQ computers cannot support quantum supremacy

NISQ computers cannot support quantum supremacy because when we use computational complexity tools to understand the computational power of NISQ computers, we discover that they describe a very low-level computational class. This low-level computational class does not allow for any complicated computations, much less computational supremacy.

The reason NISQ computers cannot support good-quality quantum error correcting codes

It is impossible to build good-quality quantum error-correcting codes because it requires an even lower noise level than that required for demonstrating quantum supremacy.

$$\alpha < \beta < \gamma < \delta$$

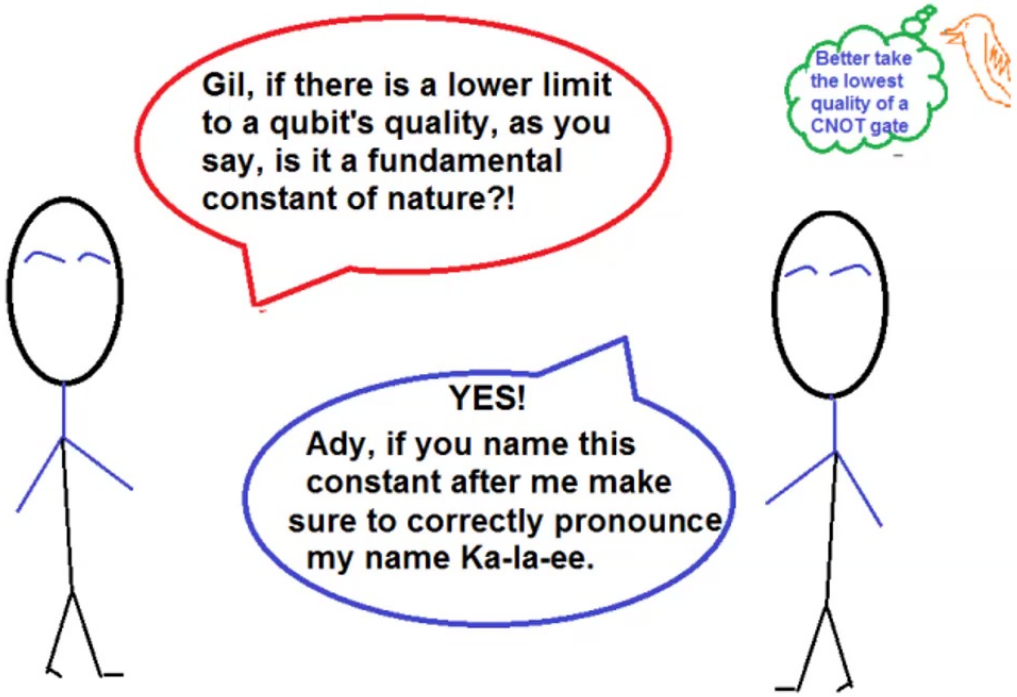
α – The rate of noise required by large quantum computers

β – The rate of noise required for good quality quantum error correcting codes. (E.g., distance 5 surface code)

γ – The rate of noise required to demonstrate “quantum supremacy”

δ – The lowest realistic rate of noise for quantum circuits in nature

$$\alpha < \beta < \gamma < \delta$$



The chaotic/noise-sensitive nature of NISQ samples

Analysis of the intermediate-scale quantum computer model points to chaotic behavior across a broad range of noise levels. Here we use the term “chaotic” in the following strong sense: it will not be possible, even probabilistically, to predict the behavior of the computer, namely the distribution of the samples it produces.

This chaotic behavior is caused by high amount of noise sensitivity of the quantum computer samples, namely, small fluctuations in the parameters describing the noise will have a big effect on the distribution of the samples produced by the computer.

The crux of the debate

I argue that from the point of view of computational complexity, NISQ devices are, in fact, low-level classical computing devices, and I regard it as strong evidence that engineers will not be able to reach the level of noise required for quantum supremacy and good-quality quantum error correcting codes.

Others argue that the existence of low-level simulation (in the NISQ regime) for every fixed level of noise does not have any bearing on the engineering question of reducing the level of noise.

These sharply different views will be tested in the next few years.

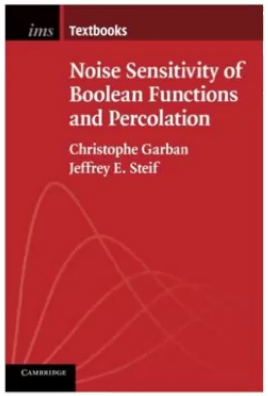
Part III: Noise Stability and sensitivity for boson sampling

"Mathematical physics is a two-way street: problems in physics can precipitate new mathematics to solve them, while new mathematics opens doors to understanding the physical universe."

(Latham Boyle's home page)

Add the theory of computing to get a wonderful three-way street!

The mathematical theory of noise sensitivity and stability



The meaning of noise-sensitivity as I see it

There are quantum systems (like Googles Sycamore computer with 12 qubits or certain systems of non interacting photons) for which it is impossible, *as a matter of principle*, to describe their future behavior (samples) *even probabilistically.*

Boson Sampling
(non interacting bosons)

Troyansky-Tishby (1996), Aaronson-Arkhipov (2010, 2013):

Given a complex *n* by *m* matrix *X* with orthonormal rows. Sample subsets of columns (with repetitions) according to the **absolute value-squared** of permanents.

This task is referred to as **Boson Sampling.**

Quantum computers can perform Boson Sampling on the nose. There is a good theoretical argument by Aaronson-Arkhipov (2010) that these tasks are beyond reach for classical computers.

$$\begin{array}{ccc} 1 & 2 & 3 \\ \left(\begin{array}{ccc} 1/\sqrt{3} & i/\sqrt{3} & 1/\sqrt{3} \\ 0 & 1/\sqrt{2} & i/\sqrt{2} \end{array} \right) & & \end{array}$$

Input matrix

Boson Sampling (permanents):

{1,1} – 0 {1,2} – 1/6 {1,3} – 1/6

{2,2} – 2/6 {2,3} – 0 {3,3} – 2/6

Fermion Sampling (determinants):

{1,2} – 1/6 {1,3} – 1/6 {2,3} – 4/6

Noisy Boson Sampling

(Kalai-Kindler 2014) Let **G** be a complex Gaussian n x m noise matrix (normalized so that the expected row norms is 1). Given an input matrix **A**, we average the Boson Sampling distributions over $(1-t)^{1/2}$ **A** + $t^{1/2}$ **G**.

t is the rate of noise.

Now, expand the outcomes in terms of Hermite polynomials. The effect of the noise is exponential decay in terms of the Hermite degree.

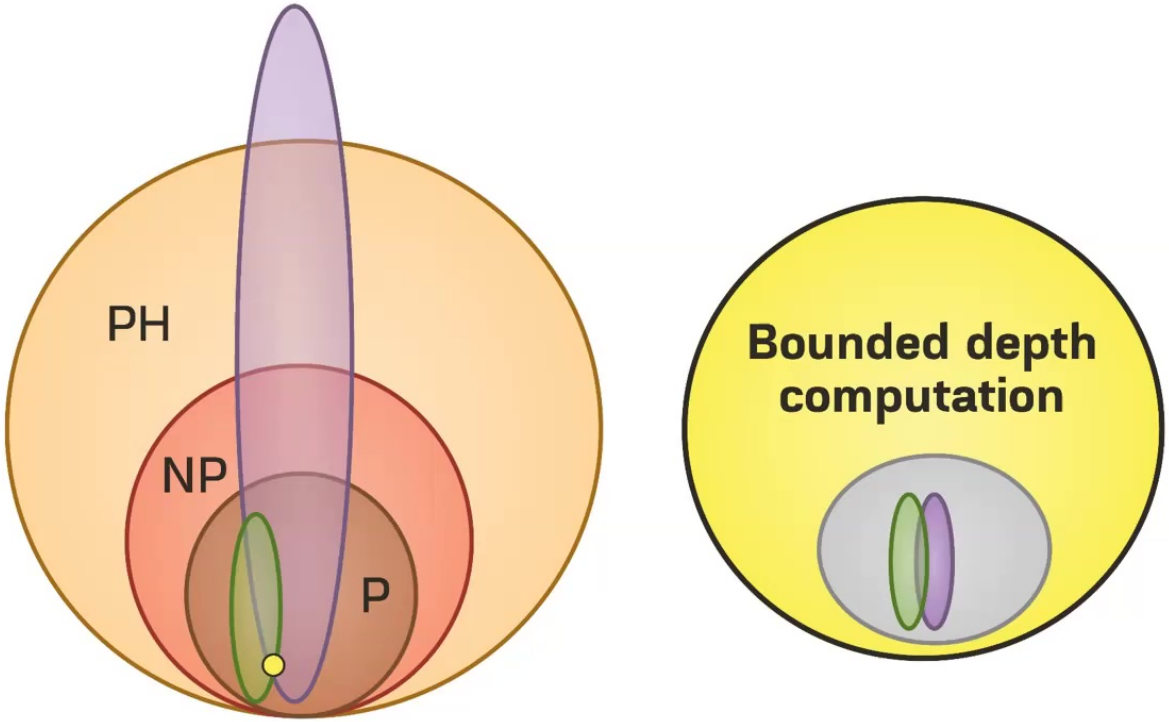
The Fourier-Hermite expansion for the Boson Sampling model is beautiful and very simple!

Noise stability/sensitivity of Boson Sampling

Boson sampling is technically and conceptually simpler than the circuit model and it allows definite and clear-cut insights that extend to more general models and more complicated situations.

Theorem 1 (Kalai-Kindler, 2014): When the noise level is constant, distributions given by noisy Boson Sampling are well approximated by their low-degree Fourier-Hermite expansion. (Consequently, these distributions can be approximated by bounded-depth polynomial-size circuits.)

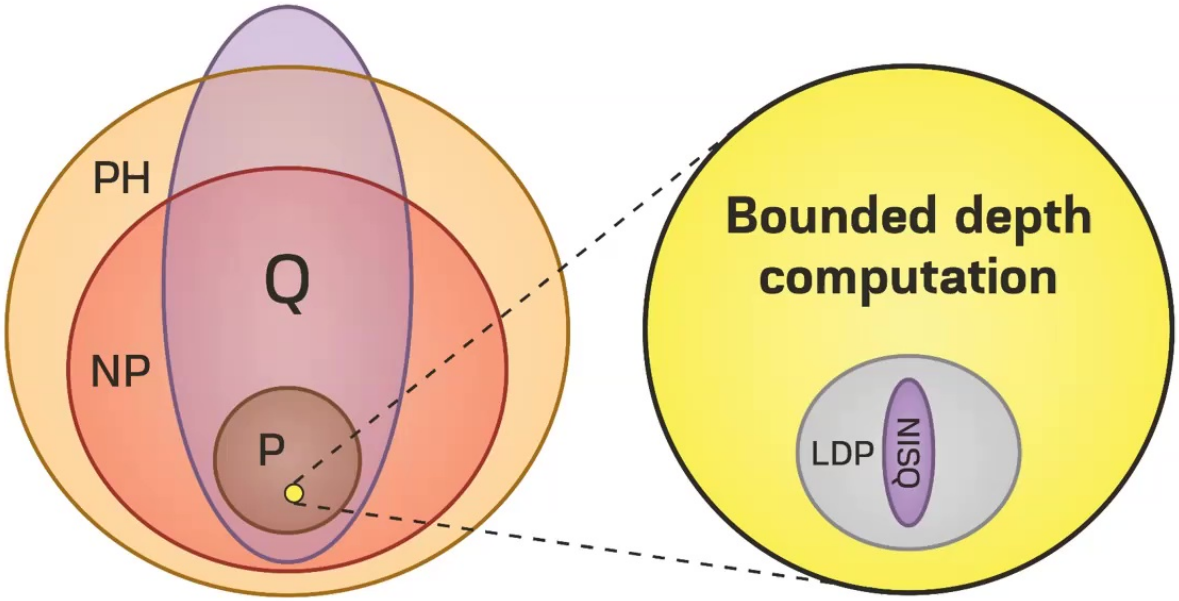
Theorem 2 (Kalai-Kindler, 2014): When the noise level is larger than $1/n$, noisy boson sampling is very sensitive to noise, with a vanishing correlation between the noisy distribution and the ideal distribution.



The huge computational gap (left) between Boson Sampling (purple) and Fermion Sampling (green) vanishes in the noisy version.

The computational power of NISQ systems

NISQ-circuits are computationally very weak, unlikely to allow quantum codes needed for quantum computers.



Physics and computations – the laws

ECCT: The extended Church Turing thesis

Every computation in nature (in the large scale) can be described by an efficient Boolean circuit.

QECCT: The quantum extended Church Turing thesis

Every computation in nature (in the large scale) can be described by an efficient Boolean circuit.

NISQ=LDP: NISQ computers represent bounded degree polynomials (plus chaos)

Every quantum computation in nature (in the small scale) can be represented by low degree polynomials

Weiner chaos and Lorenz chaos

When I speak here of chaotic behavior I refer to a system (either deterministic, probabilistic, or quantum) that is so sensitive to its defining parameters that its behavior (or a large component of its behavior) cannot be determined, not even probabilistically. This notion is related to the mathematical theory of "noise sensitivity" (Benjamini, Kalai, and Schramm 1999) that we mentioned before, and to the related mathematical theory of "black noise" (Tsirelson and Vershik 1998). Both these theories have their early roots in **Weiner's chaos expansion** (Weiner 1938).

The term "chaotic system" in mathematical chaos theory (Lorenz 1963) refers to nonlinear classical deterministic systems, whose development very much depends on their initial conditions and since these conditions are not known precisely, the system's development in the long run cannot be predicted.

It is plausible that natural chaotic phenomenon (like the weather) reflects both the Lorenz chaos and the Weiner chaos.

Correlations

(Correlation principle:) "Cat states on two qubits are subject to correlated errors". (proposed 2005/6)

1. The correlation principle for ***gated qubits*** is part of the standard assumptions on noisy quantum circuits

2. The correlation principle holds for NISQ systems.

3. Quantum fault-tolerance would refute the correlation principle.

4. The correlation principle (as an assumption on the noise) causes current fault-tolerance schemes to fail.

Consequences for cats

Following the tradition of using cats for quantum thought experiments, consider an ordinary living cat. In a world devoid of quantum computers:

- It will be impossible to teleport the cat;
- It will be impossible to reverse time in the life of the cat;
- It will be impossible to implement the cat on a very different geometry;
- It will be impossible to superpose the lives of two distinct cats;
- The life of this cat cannot be predicted.

Here, our “cat” may represent realistic (but involved) quantum evolutions described by a quantum computer with 10-20 qubits.

Lewis Wein (look him up)

NISQ devices – recent claims

Goal 1: Demonstrate quantum supremacy on random circuits (namely, circuits that are based on randomly choosing the computation process, in advance), with 50–100 qubits.

Claimed, 2019, Google's *Sycamore (+* USTC's)

The Google researchers claimed to achieve in 300 seconds a sampling task that requires 10,000 years for a supercomputer.

Goal 2: Demonstrate quantum supremacy via systems of non-interacting bosons.

Claimed, 2020, USTC's *Jiuzhang*

The USTC researchers claimed to achieve in 300 seconds a sampling task that requires a billion years for a supercomputer.

Goal 3: Create distance-5 surface codes on NISQ circuits that require a little over 100 qubits.

Some progress reported by several groups.

Classical “spoofing” for recent supremacy claims

The supremacy claims regarding boson sampling are largely refuted by an algorithm from my 2014 work with Guy Kindler. (There are also works by Popova and Rubtsov 2021 and Villalonga, Niu, Li, Neven, Platt, Smelyanskiy and Boixo 2021.)

For the Google experiments, new algorithms improve the classical running time by a factor of a billion thus severely weakening the supremacy claims. Pan, Chen, and Zhang 2021; Kalachev, Panteleev, Yung 2021; Lui, et als 2021; and other groups. (Following various improvements and breakthroughs since 2019)

My statistical work with Rinott and Shoham

Statistical Science
0, Vol. 0, No. 00, 1–26
https://doi.org/10.1214/21-STS836

Statistical Aspects of the Quantum Supremacy Demonstration

Yosef Rinott, Tomer Shoham and Gil Kalai

Abstract. In quantum computing, a demonstration of *quantum supremacy* (or quantum advantage) consists of presenting a task, possibly of no practical value, whose computation is feasible on a quantum device, but cannot be performed by classical computers in any feasible amount of time. The notable claim of quantum supremacy presented by Google's team in 2019 consists of demonstrating the ability of a quantum circuit to generate, albeit with considerable noise, bitstrings from a distribution that is considered hard to simulate on classical computers. Very recently, in 2020, a quantum supremacy claim was presented by a group from the University of Science and Technology of China, using a different technology and generating a different distribution, but sharing some statistical principles with Google's demonstration.

Verifying that the generated data is indeed from the claimed distribution and assessing the circuit's noise level and its fidelity is a statistical undertaking. The objective of this paper is to explain the relations between quantum computing and some of the statistical aspects involved in demonstrating quantum supremacy in terms that are accessible to statisticians, computer scientists, and mathematicians. Starting with the statistical modeling and analysis in Google's demonstration, which we explain, we study various estimators of the fidelity, and different approaches to testing the distributions generated by the quantum computer. We propose different noise models, and discuss their implications. A preliminary study of the Google data, focusing mostly on circuits of 12 and 14 qubits is given in different parts of the paper.

Key words and phrases: Google's quantum computer, random distributions, estimation of sampling weights, size bias.

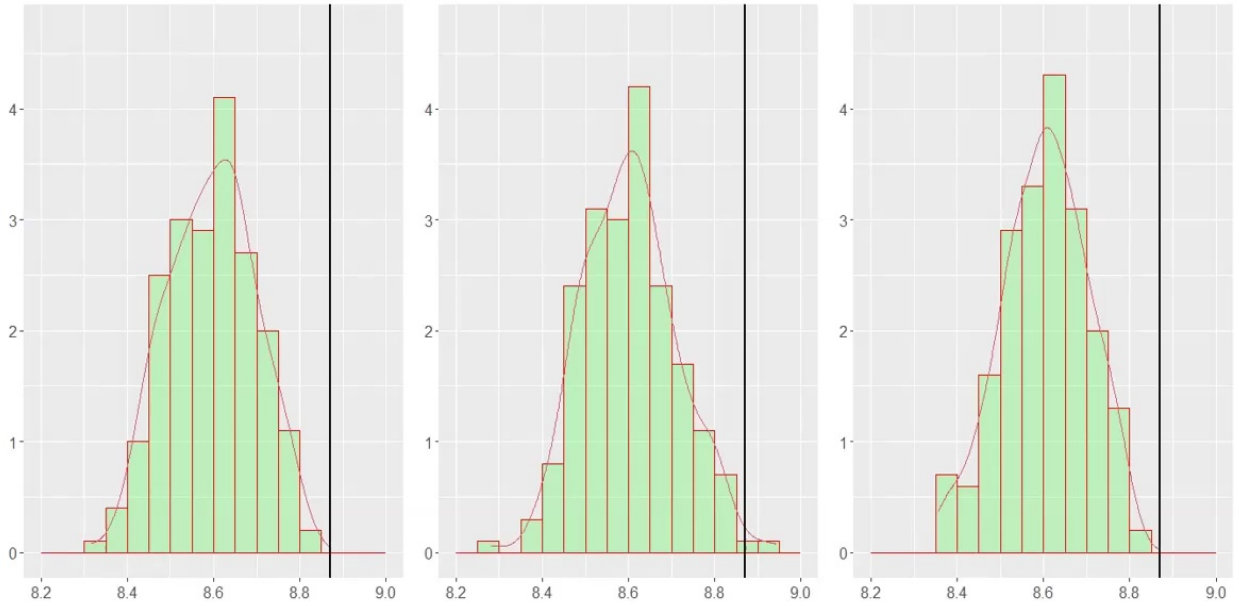
1. INTRODUCTION

Google's announcement of quantum supremacy [3] was compared by various writers to landmark achievements such as the Wright brothers' invention of a motor-operated airplane, Fermi's demonstration of a nuclear chain reaction, and the discovery of the Higgs boson. It computers in general, have not at this point performed any practical task (such as factoring large integers). Instead, Google's quantum computer performs a *sampling task*; that is, it generates random bitstrings, with considerable noise, from a discrete distribution supported on M values, with probabilities whose computations are far be-

One of our findings:
The empirical distribution is **very different** from the Google noise model!

There are also other concerns regarding the Google experiment.

Non-stationarity (perhaps even chaos) for Sycamore samples



Thank you very much!

תודה רבה!

Henry and Manya
Noskwith Professor
(along with Tamar
Ziegler)