UTS
UNIVERSITY OF TECHNOLOGY SYDNEY

CENTRE FOR
QUANTUM COMPUTATION & COMMUNICATION TECHNOLOGY
AUSTRALIAN RESEARCH COUNCIL CENTRE OF EXCELLENCE

A Combinatorial Approach to Complexity Transitions in Quantum Physics

Ryan Mann

(Joint work with Michael Bremner)

Quantum vs Classical Computation

Open problem: Are quantum computers more powerful than classical computers?

Progress: Using approximate counting methods (which underlies the complexity of quantum computing).

Recent success in rigorously identifying complexity transitions in statistical physics models.

Independence polynomial (Jan and Ivona's talks).

Matching polynomial (Leslie's talk).

Hypergraph colourings (Heng's talk).

Ising model (Piyush and Guus' talks and this talk).

Can we apply these techniques to quantum physics models? typically complex-valued.

Recent techniques of **[Barvinok 15+]** and **[Patel and Regts 17]** allow us to study complex-valued models.

What does a quantum computer do?

1) Prepare some initial state $|0^n\rangle$

   e.g. $|0^4\rangle$.

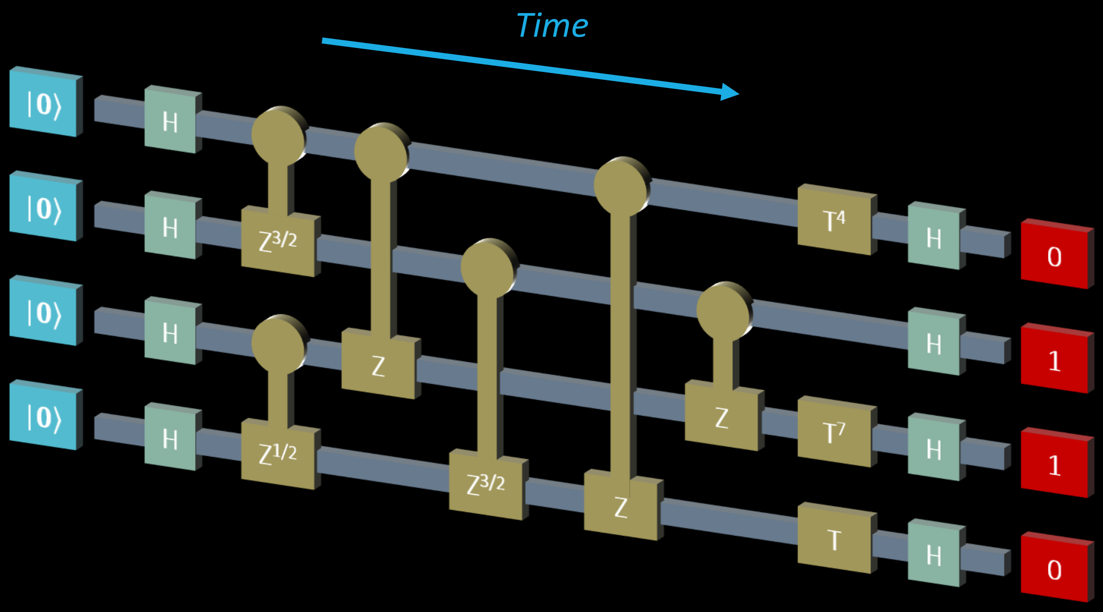
2) Apply quantum gates $U|0^n\rangle$

   e.g. $\mathrm{H}^{\otimes 4}\mathrm{D}\mathrm{H}^{\otimes 4}|0^4\rangle$.

3) Measure $\mathbf{Pr}[x] \coloneqq |\langle x|U|0^n\rangle|^2$.

   e.g. 0110 with probability

   $\left|\langle 0110|\mathrm{H}^{\otimes 4}\mathrm{D}\mathrm{H}^{\otimes 4}|0^4\rangle\right|^2$.



A example quantum computation.

Quantum States

Pure state: $|\psi\rangle \coloneqq \sum_k \alpha_k |\psi_k\rangle$
A unit vector in a complex Hilbert space.
Its adjoint is given by $\langle\psi| \coloneqq \sum_k \alpha_k^* \langle\psi_k|$.

Inner product: $\langle\phi|\psi\rangle$
Probability amplitude for observing $|\phi\rangle$ given $|\psi\rangle$.
The probability is $|\langle\phi|\psi\rangle|^2$.

Composition: $(|\psi\rangle \otimes |\phi\rangle)_{ij} \coloneqq \psi_i \phi_j$
States compose via the tensor product.

Entanglement: A state is entangled if it cannot be written as a composition.

E.g. $|\psi\rangle_{AB} \coloneqq \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)$.

Quantum Bits

The fundamental object in quantum computing is the qubit

$$|\psi\rangle \coloneqq \alpha|0\rangle + \beta|1\rangle,$$

where $\{|0\rangle, |1\rangle\}$ are the computational basis states,

$$|0\rangle \coloneqq \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle \coloneqq \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Typically, we write an n-qubit state as

$$|\psi\rangle \coloneqq \sum_{x \in \{0,1\}^n} \alpha_x \, |x\rangle,$$

where $|x\rangle \coloneqq |\mathrm{x}_1\rangle \otimes \cdots \otimes |x_n\rangle$.

We have $\mathbf{Pr}[x] \coloneqq |\langle x|\psi\rangle|^2 = |\alpha_x|^2$.

Quantum State Evolution

Quantum gate: A unitary operator $G \in \mathrm{SU}(2^c)$.

Quantum circuit: A sequence of gates acting on n qubits $U = \mathrm{G}_1\mathrm{G}_2 \ldots \mathrm{G}_{\mathrm{poly}(n)} \in \mathrm{SU}(2^n)$.

Universality: A set of gates $\{G_i\}$ is universal if it generates a dense subset of $\mathrm{SU}(2^c)$.

Theorem[Solovay Kitaev]: *Density implies efficiency, i.e.*

$$\left\|\mathrm{G}_{\mathrm{i}_1}\mathrm{G}_{\mathrm{i}_2} \ldots \mathrm{G}_{\mathrm{i}_{\mathrm{O}(\log^4(1/\epsilon))}} - \mathrm{U}\right\| \leq \epsilon.$$

The Hamiltonian picture: $U = e^{-iHt}$.

H is a Hermitian operator (self-adjoint).

$|\psi(t)\rangle = \mathrm{e}^{-\mathrm{iHt}}|\psi(0)\rangle$.

The Hadamard Test

The Hadamard test is an efficient quantum algorithm for producing a random variable $\boldsymbol{Z}$ with

$$\mathbf{Pr}[\pm] \coloneqq \frac{1}{2}\left(1 \pm \mathbf{Re}(\langle 0^n | U | 0^n \rangle)\right).$$

Therefore,

$$\mathbb{E}(\boldsymbol{Z}) \coloneqq \mathbf{Re}(\langle 0^n | U | 0^n \rangle).$$

By the Chernoff-Hoeffding bound, we can efficiently approximate $\mathbf{Re}(\langle 0^{\mathrm{n}} | \mathrm{U} | 0^{\mathrm{n}} \rangle)$, such that w.h.p.,

$$|A - \mathbf{Re}(\langle 0^n | U | 0^n \rangle)| \leq \frac{1}{\mathrm{poly}(n)}.$$

We can apply a similar argument for $\mathbf{Im}(\langle 0^n | U | 0^n \rangle)$.

Complexity of Quantum Computing

What is the complexity of $\langle 0^n | U | 0^n \rangle$?

Exact: GapP-hard.

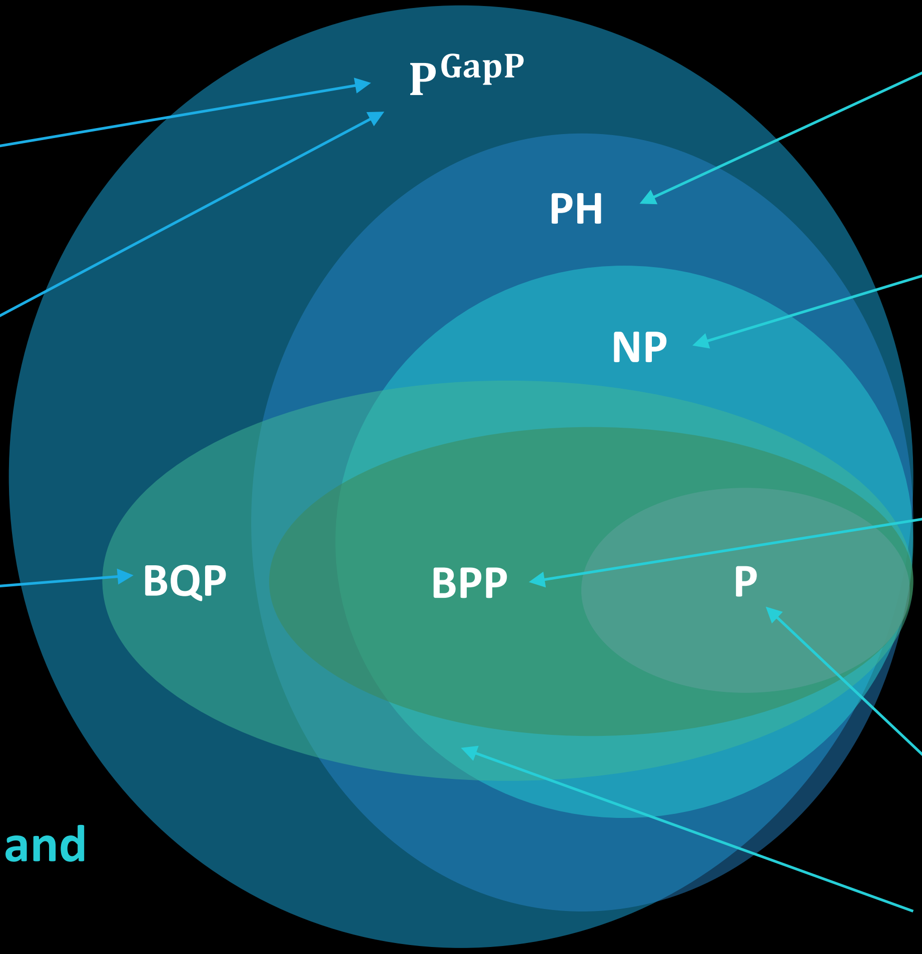
The closure of **#P** under subtraction.

Relative error: GapP-hard.

Additive error: BQP-hard.

The quantum equivalent of **BPP**.

Can we use this to separate quantum and classical computation?



PH: Polynomial Hierarchy.

NP: Non-deterministic Polynomial time.

BPP: Bounded-error Probabilistic Polynomial time.

P: Polynomial time.

Factoring.

Quantum Computation and Approximate Counting

Theorem[Fenner et al. 98]:
For any $g \in \mathbf{GapP}$, there's a polynomial-time quantum circuit C, such that

$$\langle 0^{\mathrm{n}}|C(x)|0^{\mathrm{n}}\rangle = \frac{g(x)}{2^{\mathrm{n}}}.$$

Efficient quantum algorithm for approximating any problem in **GapP** (and **#P**),

$$|A - g(x)| \leq \frac{2^n}{\mathrm{poly}(n)}.$$

Conjecture: No efficient classical algorithm.

Nature can solve really hard problems… but we can't directly access the solution.

Complexity of Random Quantum Sampling

Line of work initiated by **[Aaronson and Arkhipov 11]** and **[Bremner, Montanaro, and Shepherd 15]**.

Task: Approximately sample from $\mathbf{Pr}_{\mathrm{U}}[x] \coloneqq |\langle x|U|0^n\rangle|^2$ for random U. Close in l_1 norm.

Conjecture: $\langle x|U|0^n\rangle$ is **GapP-hard** to approximate (relative error) on average.

Theorem: *Assume conjecture is true. Then there is no efficient classical algorithm unless the Polynomial Hierarchy collapses, i.e.,* $\mathbf{BPP} \neq \mathbf{BQP}$.

Conjecture is still open. See **[Bouland et al. 18]** for some recent progress on this.

The Ising Model

Described by a weighted graph $G = (V, E)$.

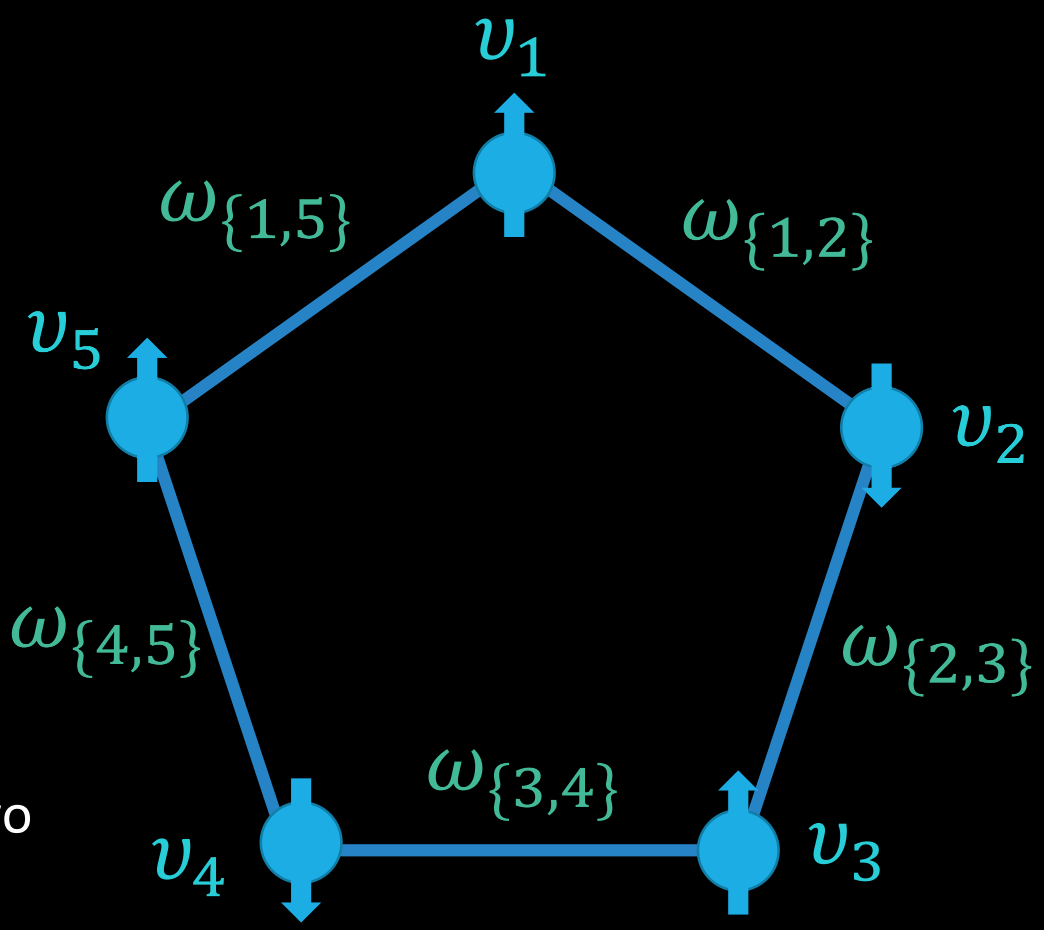
Vertices: Two-state spins $\{-1, +1\}$.

Edges: Interactions between them.

Vertex weights $\Upsilon = \{\upsilon_v\}_{v \in V}$: Characterise external fields.

Edge weights $\Omega = \{\omega_e\}_{e \in E}$: Characterise interaction strengths.

Configuration: Assignment of each spin to one of two possible states $\{-1, +1\}$.



The Ising Model Partition Function

The Ising model partition function is a weighted sum over all possible configurations

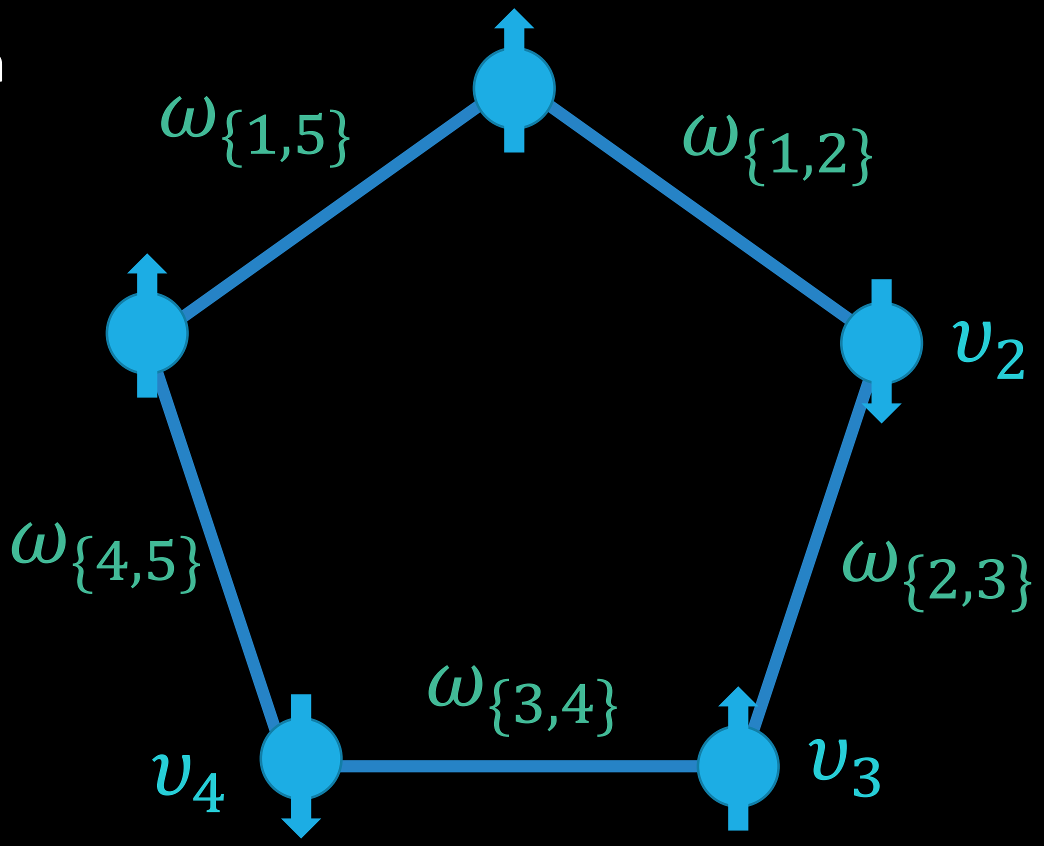
$$Z_{\text{Ising}}(G; \Omega, \Upsilon) := \sum_{\sigma \in \{-1,+1\}^V} w(\sigma)\,,$$

where

$$w(\sigma) := \exp\left(\sum_{\{u,v\} \in \mathrm{E}} \omega_{\{u,v\}} \sigma_u \sigma_v + \sum_{v \in \mathrm{V}} \upsilon_v\, \sigma_v \right).$$

Ferromagnetic: $\omega_e > 0$.

Anti-ferromagnetic: $\omega_e < 0$.



The IQP Model

IQP – *Instantaneous Quantum Polynomial time*.

Can be defined by an Ising Hamiltonian over a graph $G = (V, E)$,

$$H_G = \sum_{\{i,j\}\in E} \omega_{\{i,j\}} X_i X_j + \sum_{k\in V} v_k X_k\,,$$

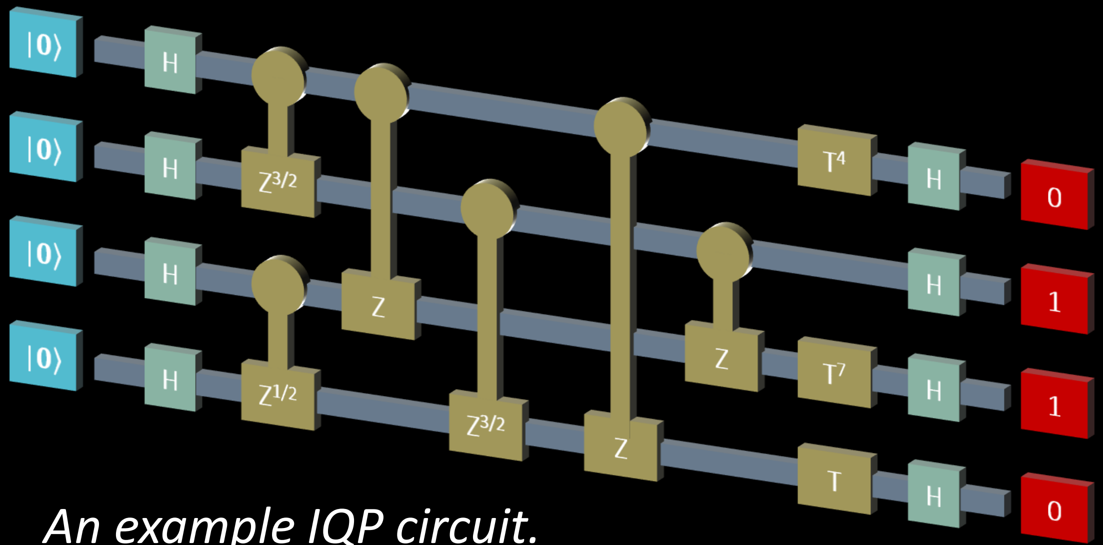
where

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Vertices: Qubits.

Vertex weights: One-qubit gates $e^{-iv_k X_k}$

Edge weights: Two-qubit gates $e^{-iw_{\{i,j\}} X_i X_j}$.



An example IQP circuit.

Circuits are of the form $C = H^{\otimes n} \mathrm{D} H^{\otimes n}$ for some diagonal matrix D.

Properties of IQP Circuits

Probability amplitudes are equivalent to Ising model partition functions with imaginary weights,

$$\langle 0^{|V|} | e^{-iH_G} | 0^{|V|} \rangle = \frac{Z_{\text{Ising}}(G; i\Omega, i\Upsilon)}{2^n}.$$

IQP circuits are universal under post selection

[Bremner, Jozsa, and Shepherd 10].

Implies approximating $Z_{\text{Ising}}(G; i\Omega, i\Upsilon)$ up to additive error is **BQP-hard** (even for bounded-degree graphs).

When can we classically approximate Z_{Ising}?

Motivating Complex-Valued Ising Model Partition Functions

Computer Science

- **GapP-hard** to compute exactly and approximate (relative error) **[Goldberg and Guo 14]**.
- Natural extension to the real case.

Statistical Physics

- Physical phase transitions are the real limit points of the complex zeros.

Quantum Physics

- Probability amplitudes are proportional to partition functions with imaginary temperature.
- Nature is described by complex-valued Ising models.
- **BQP-hard** to approximate (additive error).

Random IQP Sampling

Task: Approximately sample from a random IQP circuit.

Complete graph or sparse graph $p = O\left(\frac{\log(|V|)}{|V|}\right)$ with weights chosen from $\frac{i\pi}{8}\{0, \ldots, 7\}$.

Conjecture: Z_{Ising} is **GapP-hard** to approximate up to relative error on a constant fraction of instances.

Theorem [Bremner, Montanaro, and Shepherd]:

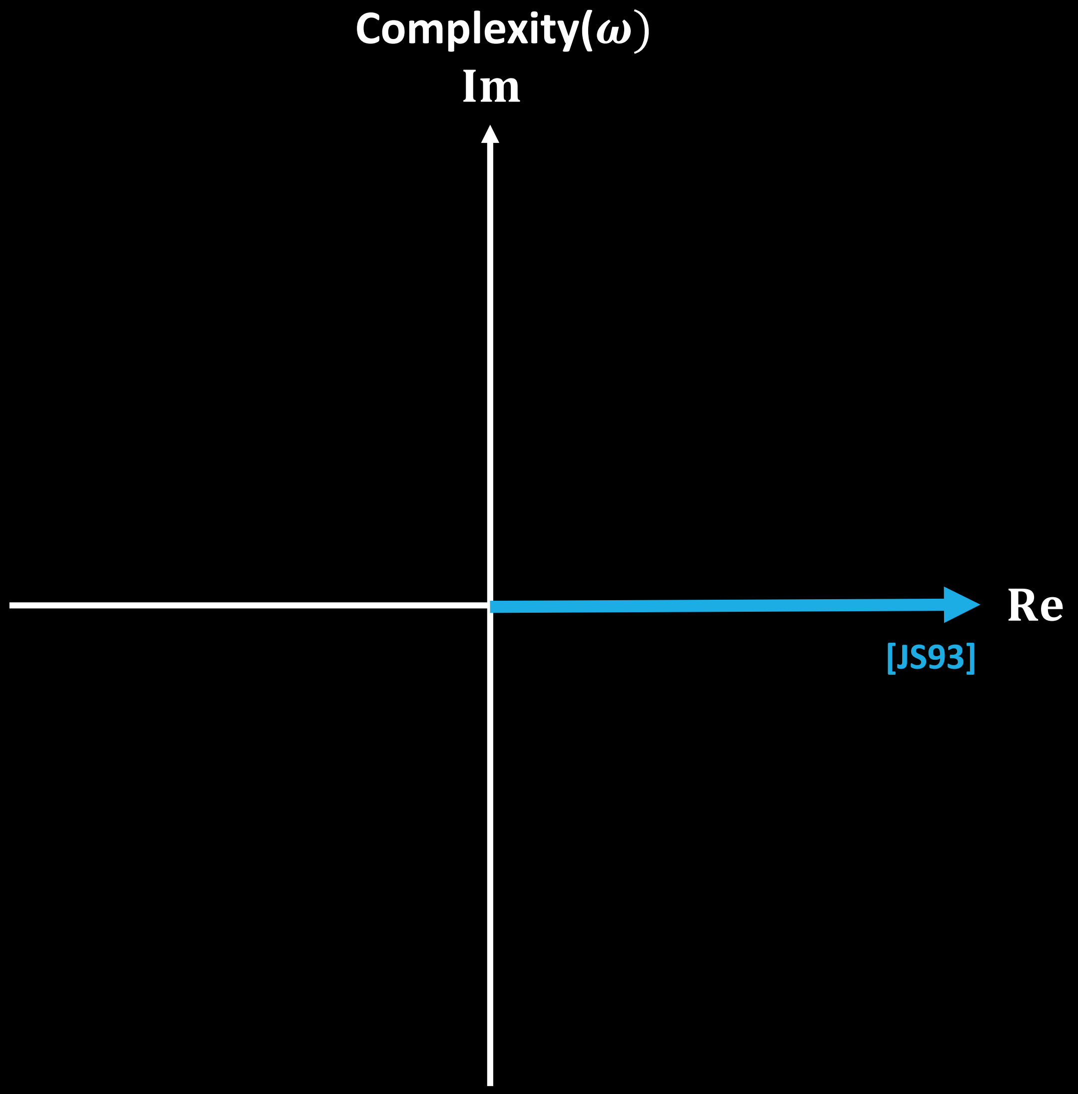
Assume conjecture is true. Then there is no efficient classical algorithm unless the Polynomial Hierarchy collapses.

Complexity of random complex-valued Z_{Ising} is important for separating quantum and classical computation.

Approximating the Partition Function

Approximations:

[JS93] Jerrum and Sinclair (FPRAS).

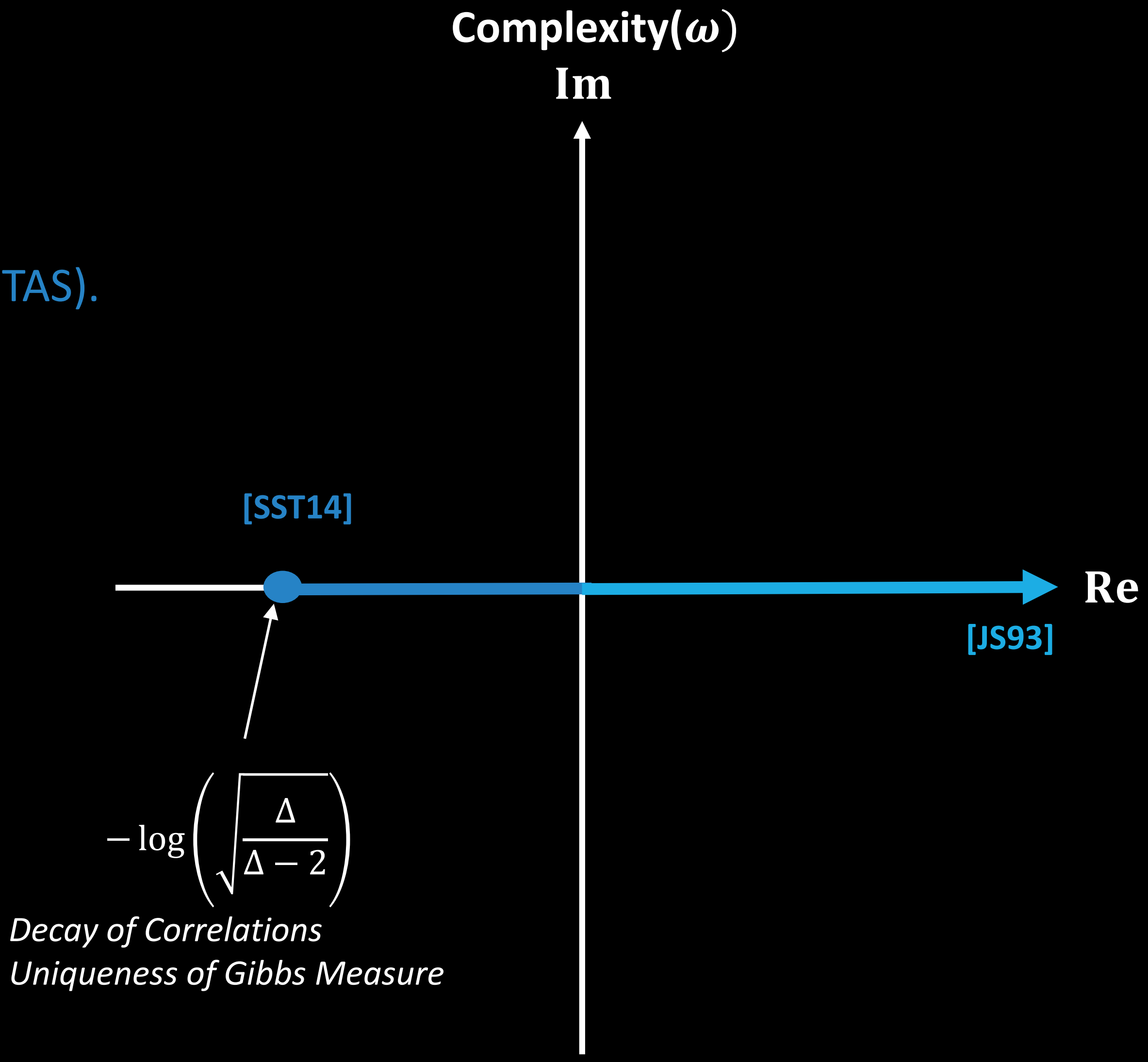


Approximating the Partition Function

Approximations:

[JS93] Jerrum and Sinclair (FPRAS).

[SST14] Sinclair, Srivastava, and Thurley (FPTAS).



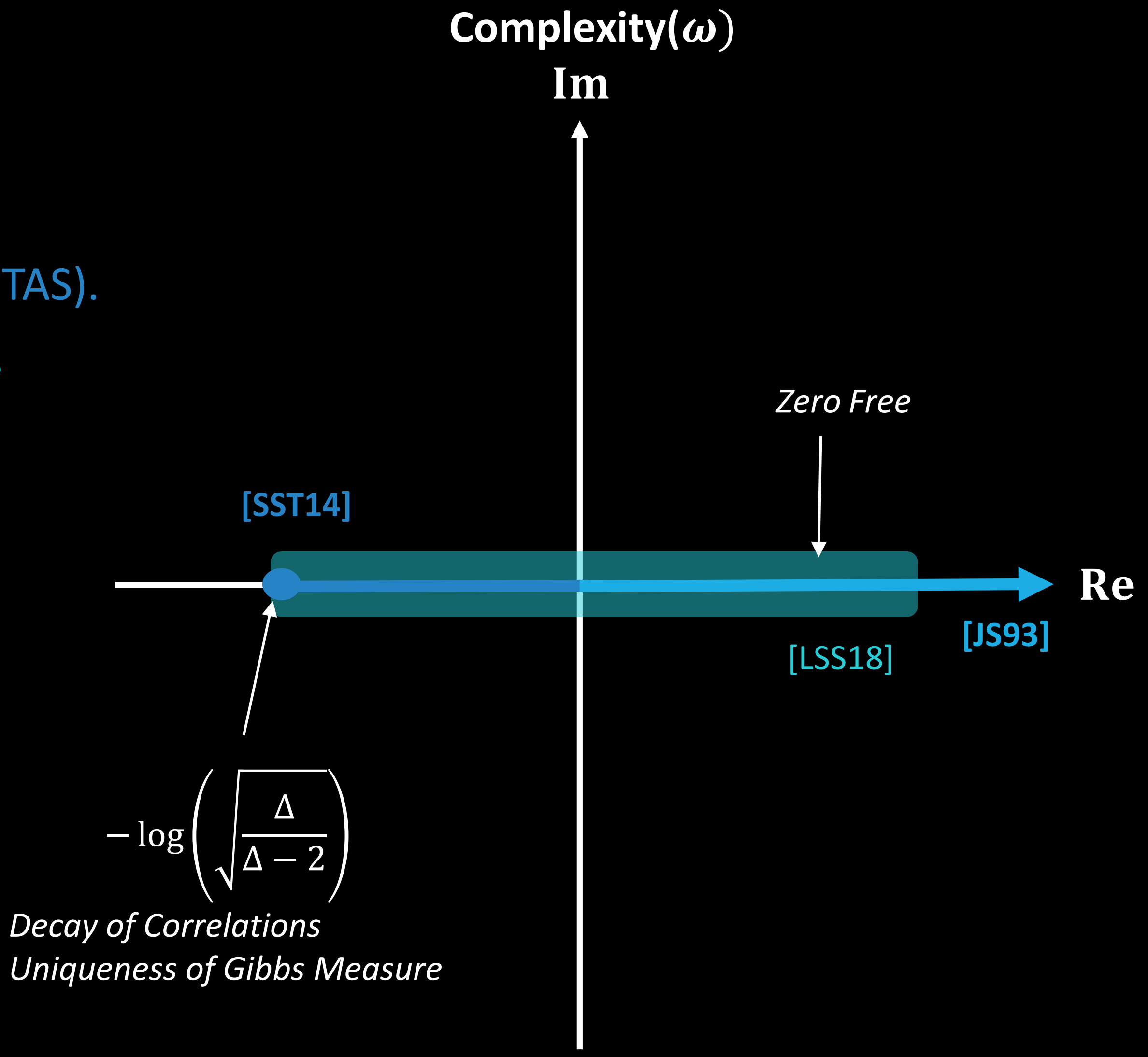
Approximating the Partition Function

Approximations:

[JS93] Jerrum and Sinclair (FPRAS).

[SST14] Sinclair, Srivastava, and Thurley (FPTAS).

[LSS18] Liu, Sinclair, and Srivastava (FPTAS).



Approximating the Partition Function

Approximations:

[JS93] Jerrum and Sinclair (FPRAS).

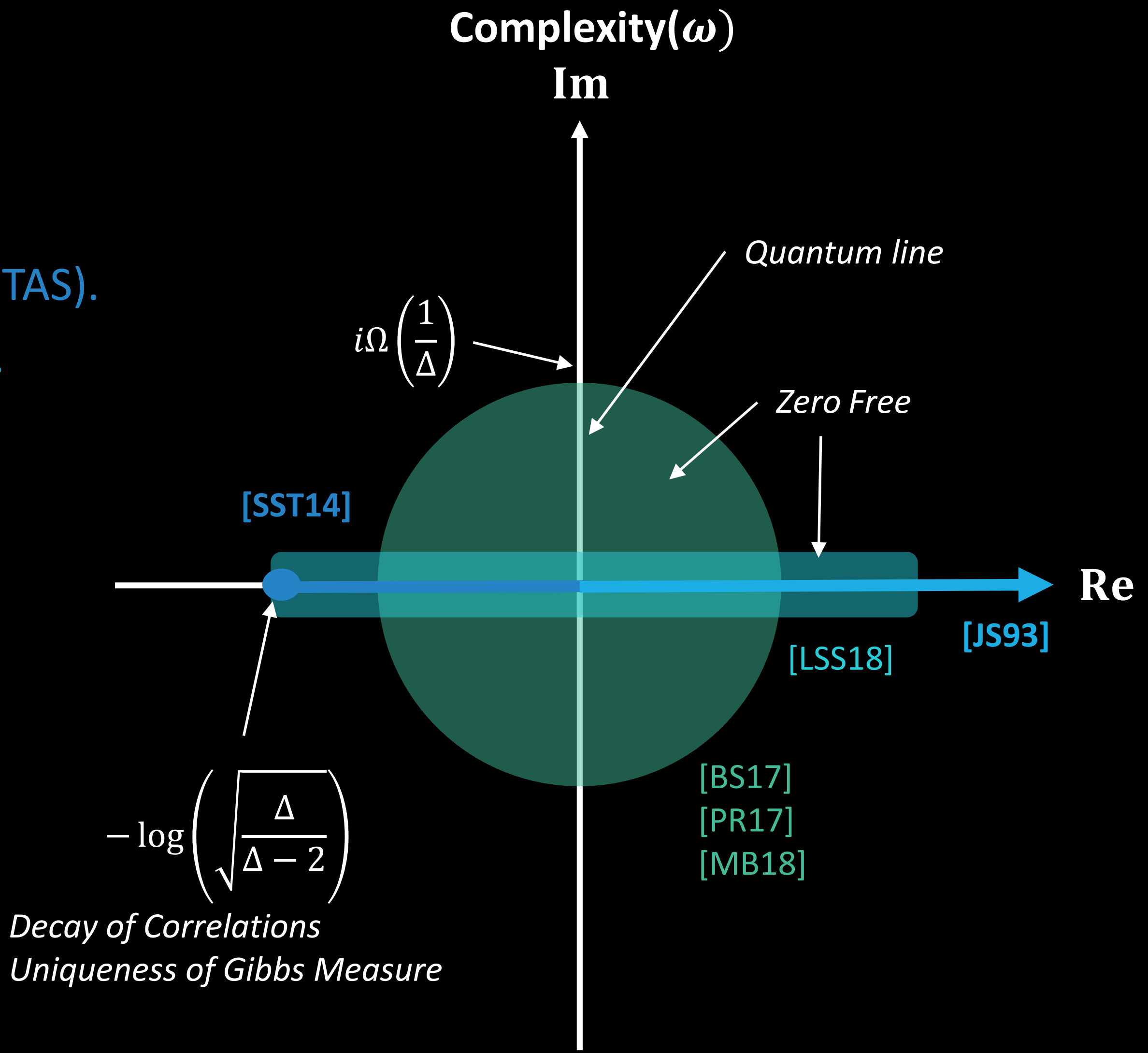
[SST14] Sinclair, Srivastava, and Thurley (FPTAS).

[LSS18] Liu, Sinclair, and Srivastava (FPTAS).

[BS17] Barvinok and Soberón (FQPTAS).

[PR17] Patel and Regts (FPTAS).

[MB18] This talk (FPTAS) (with field).



Approximating the Partition Function

Approximations:

[JS93] Jerrum and Sinclair (FPRAS).

[SST14] Sinclair, Srivastava, and Thurley (FPTAS).

[LSS18] Liu, Sinclair, and Srivastava (FPTAS).

[BS17] Barvinok and Soberón (FQPTAS).

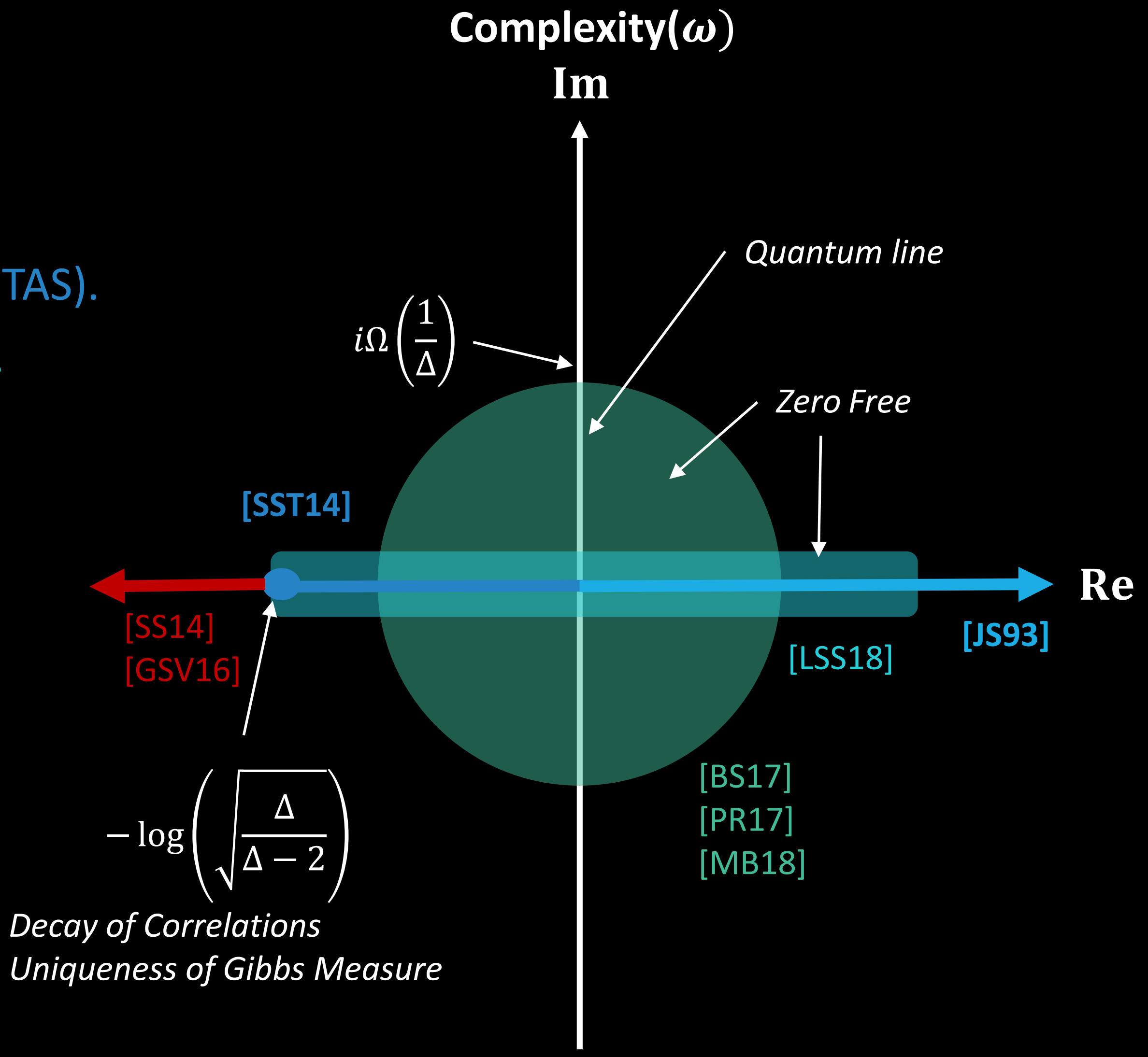
[PR17] Patel and Regts (FPTAS).

[MB18] This talk (FPTAS) (with field).

Hardness:

[SS14] Sly and Sun.

[GSV16] Galanis, Štefankovič, and Vigoda.



Approximating the Partition Function

Approximations:

[JS93] Jerrum and Sinclair (FPRAS).

[SST14] Sinclair, Srivastava, and Thurley (FPTAS).

[LSS18] Liu, Sinclair, and Srivastava (FPTAS).

[BS17] Barvinok and Soberón (FQPTAS).

[PR17] Patel and Regts (FPTAS).

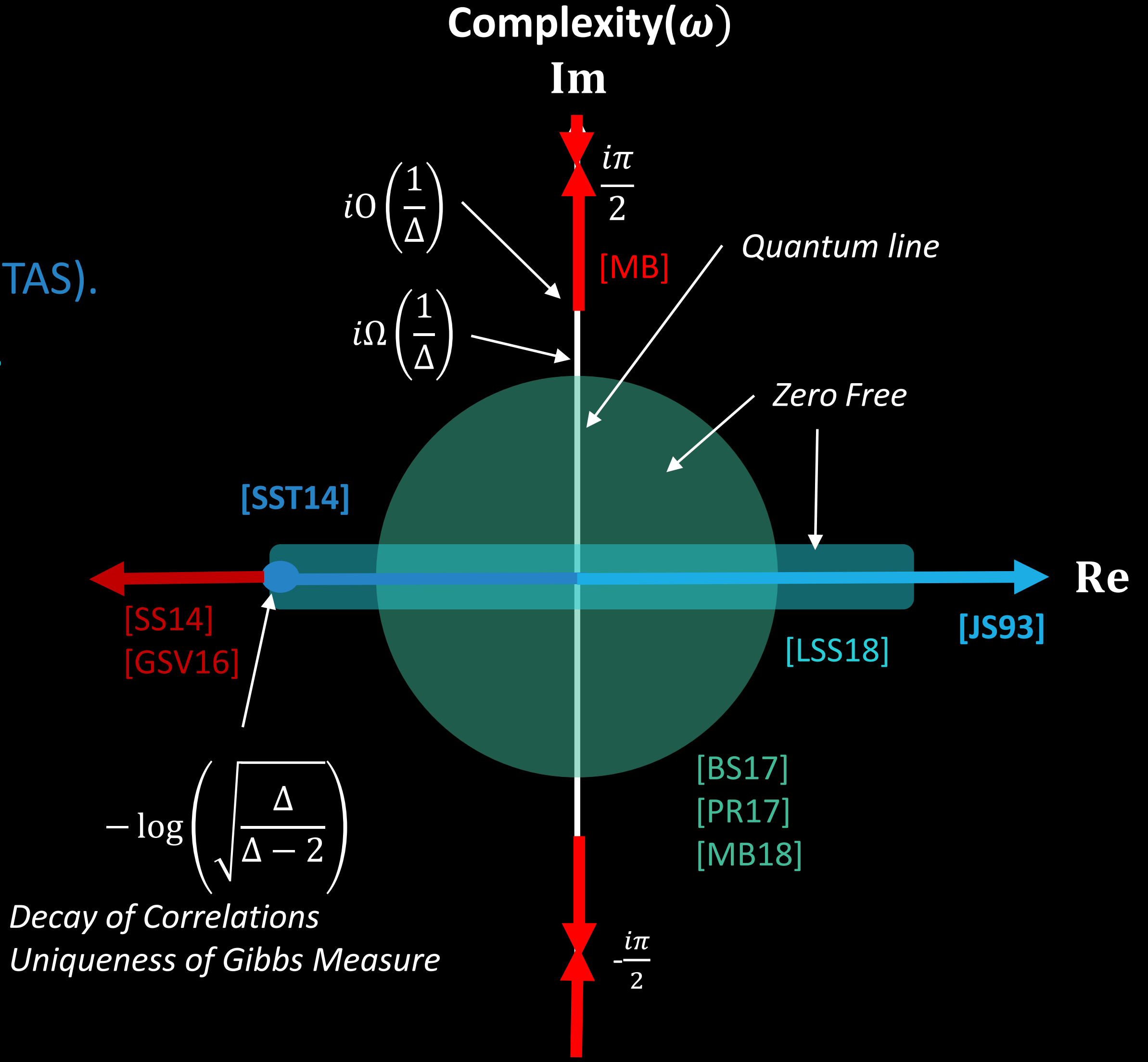
[MB18] This talk (FPTAS) (with field).

Hardness:

[SS14] Sly and Sun.

[GSV16] Galanis, Štefankovič, and Vigoda.

[MB] This talk.



Statement of Results: Approximation Algorithm

Deterministic polynomial-time algorithm for approximating complex-valued Z_{ising} on graphs of maximum degree Δ when $\left|1 - e^{\pm\omega_e}\right| < \delta_{\Delta+1}$ and $\left|1 - e^{\pm v_v}\right| < \delta_{\Delta+1}$.

$$\delta_\Delta \coloneqq \max_{0<\alpha<\frac{2\pi}{3\Delta}} \left[\sin\left(\frac{\alpha}{2}\right)\cos\left(\frac{\alpha\Delta}{2}\right)\right].$$

Radius of zero-free disc δ_Δ comes from **[Barvinok's monograph]**.

This gives $\delta_3 = 0.18$, $\delta_4 = 0.13$, $\delta_5 = 0.11$, and in general, $\delta_\Delta = \Omega(1/\Delta)$.

Statement of Results: Quantum Simulation and Hardness

Efficient classical simulation of probability amplitudes of the form $\langle 0^{|V|} | e^{-iH_G} | 0^{|V|} \rangle$, for graphs of maximum degree Δ when $|\omega_e|, |\upsilon_v| < 2\arcsin\left(\frac{\delta_{\Delta+1}}{2}\right)$.

Hexagonal lattice: Up to $\pi/23$ rotations.

Square lattice: Up to $\pi/29$ rotations

General: Up to $\Omega(1/\Delta)$ rotations.

Algorithm is almost optimal!

Hardness Results: For $|\omega_e| \leq O(1/\Delta)$,

GapP-hard: relative-error.
BQP-hard: for additive-error.

Approximation Algorithm I

Reduction to the pinned graph homomorphism partition function (allows external fields).

Graph Homomorphism Partition Function:

Let $G = (V, E)$ be a graph with the $m \times m$ symmetric matrices $\mathcal{A} = \{(a_{ij}^e)\}_{e \in E}$ assigned to its edges, then

$$\mathrm{Hom}(G; \mathcal{A}) \coloneqq \sum_{\phi : V \to [m]} \prod_{\{u,v\} \in E} a_{\phi(u)\phi(v)}^{\{u,v\}}.$$

Barvinok and Soberón 17: quasi-polynomial time approximation algorithm for $\mathrm{Hom}(G; \mathcal{A})$, when $|1 - a_{ij}^e| \le \Omega(1/\Delta)$ *(using ~~Barvinok interpolation~~).*

Barvinok's philosophy

Patel and Regts 17: Improvement to polynomial time (expressing coefficients as connected induced subgraph counts).

Approximation Algorithm II

Sketch of proof:

Apply slight extension of the Patel and Regts approach to the pinned $\mathrm{Hom}(G;\mathcal{A})$.

Zero-free region:

Lemma[Barvinok's Monograph]:

When $\left|1 - a_{ij}^{e}\right| \leq \delta_\Delta$ then pinned $\mathrm{Hom}(G;\mathcal{A}) \neq 0$.

Result: Polynomial time approximation scheme for Z_{ising} when $\left|1 - e^{\pm\omega_e}\right| < \delta_{\Delta+1}$ and $\left|1 - e^{\pm v_v}\right| < \delta_{\Delta+1}$.

Reduction increases maximum degree by one.

Hardness

Sketch of proof:

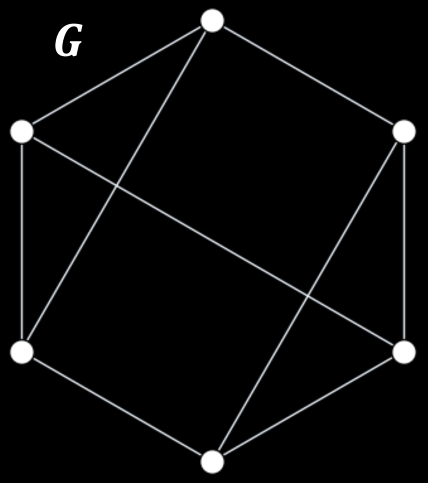
GapP-hard/BQP-hard on graphs of maximum degree 3 with imaginary weights $|\omega| \leq \pi/2$.

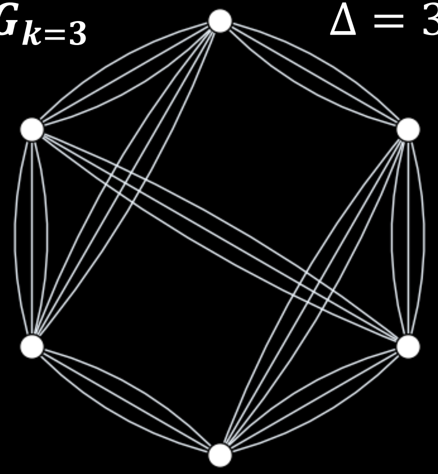
Let $\boldsymbol{G}$ be a *worst-case graph* and $\boldsymbol{G}_{\mathbf{k}}$ the ***k**-thickening* of $\boldsymbol{G}$.

Allowing $|\omega| \leq \pi/(2k) = 3\pi/(2\Delta)$ on $\boldsymbol{G}_{\mathbf{k}}$.

Then we can choose weightings so that
$Z_{\text{Ising}}(\mathbf{G}_{\mathbf{k}}) = Z_{\text{Ising}}(\boldsymbol{G})$.

Implies **GapP/BQP-hardness** of $Z_{\text{Ising}}(\mathbf{G}_{\mathbf{k}})$ with $|\omega| \leq 3\pi/(2\Delta)$.





Implication of Results

Quantum complexity transition at $|\omega_e| \leq \Theta\left(\frac{1}{\Delta}\right)$

Additive: **P** to **BQP-hard**.

Relative: **P** to **GapP-hard.**

Classical FPTAS for short time evolved Hamiltonians, i.e., e^{-iHt} for $t \leq \Omega\left(\frac{1}{\Delta}\right)$.

Quantum circuits with bounded interference, i.e., $\langle 0^n|U|0^n\rangle \neq 0$.

Quantum circuits with limited teleportation (no X gates).

Formal relationship between the geometry of zeros and complexity of quantum computing.

Other Probabilities?

Does this apply to other probability amplitudes, i.e., $\langle x|U|0^n\rangle$?

Not obvious, we require X gates,

$$\langle x|U|0^n\rangle = \left\langle 0^n \middle| X_i^{x_i} U \middle| 0^n \right\rangle,$$

But for $U = I$,

$$\langle 0|X|0\rangle = i \left\langle 0 \middle| \exp\left(-\frac{i\pi}{2} X\right) \middle| 0 \right\rangle = \langle 1|0\rangle = 0.$$

Implies $Z_{\text{Ising}} = 0$ (we get a zero).

(Can we use decay of correlations?)

Open Problems

Identify exact quantum complexity transition point.

Probe transition point.
(*entanglement dynamics?*)

Extend arguments to other probabilities/sampling problems.
(*Decay of correlation methods?*)

Apply these techniques to many-body physics.

Relationship to other methods: *Markov-chain Monte Carlo, decay of correlations, tensor network methods, stabiliser rank, etc.*

Lovász Local Lemma

Trivial Local Lemma:

Let $\{A_k\}$ *be a sequence of independent events with* $\mathbf{Pr}[A_k] < 1$, then $\mathbf{Pr}[\wedge_k \bar{A}_k] > 0$.

Lovász extended this to the dependent case.

Lovász Local Lemma:

Let $\{A_k\}$ *be a sequence of events with* $\mathbf{Pr}[A_k] \leq p$ *and each event depends on at most* Δ *other events.*

Provided $p \leq \frac{1}{e(\Delta+1)} = \Theta\left(\frac{1}{\Delta}\right)$, *then* $\mathbf{Pr}[\wedge_k \bar{A}_k] > 0$.

Useful in existence proofs.

Quantum Lovász Local Lemma

Our Scheme:

Event A_k: Measuring outcome 1 on qubit k.

Dependence: Maximum degree Δ.

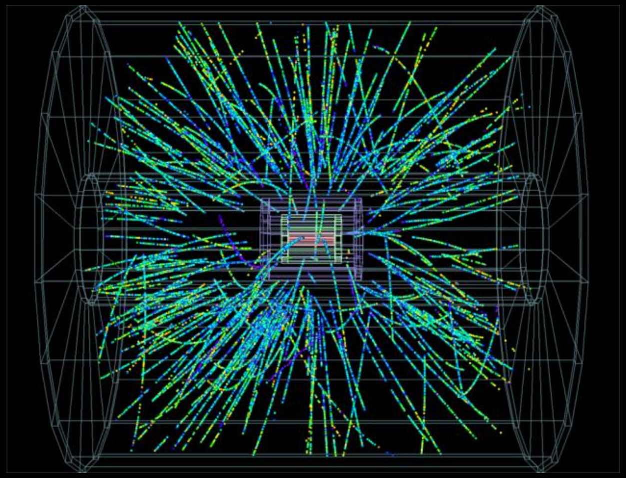
Provided $|\omega_e|, |v_v| \leq O\left(\frac{1}{\Delta}\right)$, then $\Pr[0^n] > 0$. ($\mathbf{Pr}[\wedge_k \bar{A}_k] > 0$).

When can you decide if interference cancels out an event? (**NP-hard** in general).

Applications: Existence in quantum physics?

Note: There are other versions of a quantum Lovász Local Lemma with a different flavour.

Quantum Field Theory



(Image: CERN).

Is there a non-zero probability of detecting a certain particle?

End.