How hard is it to approximate the Jones polynomial?

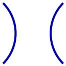
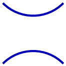
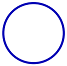
Greg Kuperberg

UC Davis

June 17, 2009

The Jones polynomial and quantum computation

Recall the Jones polynomial ($\cong$ Kauffman bracket):

 $= -q^{1/2}$  $- q^{-1/2}$   $= -q - q^{-1}$

What does it have to do with quantum computation?

Theorem (Freedman, Kitaev, Wang; Aharonov, Jones, Landau)

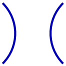
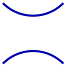
If $t = q^2$ is a root of unity, then a quantum computer can "additively" approximate the Jones polynomial in polynomial time.

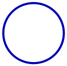
Theorem (Freedman, Larsen, Wang)

If $t = q^2 = \exp(2\pi i/r)$ with $r = 5$ or $r \geq 7$, then approximation of $V(L, t)$ is universal for quantum computation.

The Jones polynomial and quantum computation

Recall the Jones polynomial (≅ Kauffman bracket):

 $= -q^{1/2}$  $- q^{-1/2}$ 

 $= -q - q^{-1}$

What does it have to do with quantum computation?

Theorem (Freedman, Kitaev, Wang; Aharonov, Jones, Landau)

If $t = q^2$ is a root of unity, then a quantum computer can "additively" approximate the Jones polynomial in polynomial time.

Theorem (Freedman, Larsen, Wang)

If $t = q^2 = \exp(2\pi i/r)$ with $r = 5$ or $r \geq 7$, then approximation of $V(L, t)$ is universal for quantum computation.

Good news and bad news

- Additive approximation actually means

$$P[\mathrm{yes}] = \left| \frac{V(L,t)}{[2]^n} \right|^2,$$

where $n = n(D)$ is the bridge number of a diagram D of L.
- Such an approximation is not useful for topology, even if quantum computers existed. But Jones values of special braids are useful for quantum computation.

Theorem (K.)

Let $t = \exp(2\pi i/r)$ with $r = 5$ or $r \geq 7$. Let $a > b > 0$ be constants. Then it is #P-hard to decide whether $|V(L,t)| > a$ or $|V(L,t)| < b$, given the promise that it is one of these.

Good news and bad news

- Additive approximation actually means

$$P[\text{yes}] = \left| \frac{V(L,t)}{[2]^n} \right|^2,$$

  where $n = n(D)$ is the bridge number of a diagram D of L.
- Such an approximation is not useful for topology, even if quantum computers existed. But Jones values of special braids are useful for quantum computation.

Theorem (K.)

Let $t = \exp(2\pi i/r)$ with $r = 5$ or $r \geq 7$. Let $a > b > 0$ be constants. Then it is #P-hard to decide whether $|V(L,t)| > a$ or $|V(L,t)| < b$, given the promise that it is one of these.

Related results

Theorem (Jaeger, Vertigan, Welsh)

Exact computation of $V(L,t)$ *is* $\#\mathrm{P}$*-hard unless* $t^4 = 1$ *or* $t^6 = 1$.

Theorem (Goldberg, Jerrum)

Approximate computation of the Tutte polynomial $T(G,x,y)$ *is* NP*-hard for many values, and* $\#\mathrm{P}$*-hard for some values.*

- Both of these are graph-theoretic reductions. Goldberg and Jerrum use non-planar graphs.
- Our result uses a more direct connection between the Jones polynomial and computational models.

What is quantum probability?

Answer: Non-commutative probability

Probability can be defined by random variable algebras:

- Ω - a σ-algebra of boolean random variables
- $\mathcal{M} = L^\infty(\Omega)$ - the bounded $\mathbb{C}$ random variables

The algebra $\mathcal{M}$ can be described by axioms:

- It is a commutative algebra with $*$ (for $\mathbb{C}$ conjugation).
- It is a Banach space, and $||a^*a|| = ||a||^2$.
- It has a pre-dual ${}^\#\mathcal{M}$. $({}^\#\mathcal{M} \cong L^1(\Omega))$

This makes $\mathcal{M}$ a commutative von Neumann algebra.
Quantum probability is exactly the same, except that $\mathcal{M}$ can be non-commutative.

What is quantum probability?

Answer: Non-commutative probability

Probability can be defined by random variable algebras:

- Ω - a σ-algebra of boolean random variables
- $\mathcal{M} = L^\infty(\Omega)$ - the bounded $\mathbb{C}$ random variables

The algebra $\mathcal{M}$ can be described by axioms:

- It is a commutative algebra with $*$ (for $\mathbb{C}$ conjugation).
- It is a Banach space, and $||a^*a|| = ||a||^2$.
- It has a pre-dual ${}^\#\mathcal{M}$. (${}^\#\mathcal{M} \cong L^1(\Omega)$)

This makes $\mathcal{M}$ a commutative von Neumann algebra.

Quantum probability is exactly the same, except that $\mathcal{M}$ can be non-commutative.

What is quantum probability?

Answer: Non-commutative probability

Probability can be defined by random variable algebras:

- Ω - a σ-algebra of boolean random variables
- $\mathcal{M} = L^\infty(\Omega)$ - the bounded $\mathbb{C}$ random variables

The algebra $\mathcal{M}$ can be described by axioms:

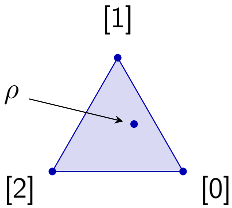
- It is a commutative algebra with $*$ (for $\mathbb{C}$ conjugation).
- It is a Banach space, and $||a^* a|| = ||a||^2$.
- It has a pre-dual $^\#\mathcal{M}$. $(^\#\mathcal{M} \cong L^1(\Omega))$

This makes $\mathcal{M}$ a commutative von Neumann algebra.
Quantum probability is exactly the same, except that $\mathcal{M}$ can be non-commutative.

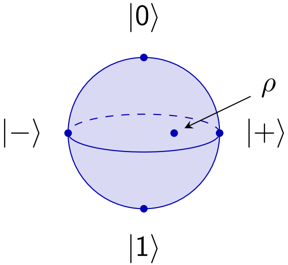
More on quantum probability

- A state is an expectation functional $\rho : \mathcal{M} \to \mathbb{C}$.
- If $\mathcal{A}$ and $\mathcal{B}$ are two systems, then the joint system is $\mathcal{A} \otimes \mathcal{B}$.
- Quantum probability is empirically true.

The state region of a classical trit $3\mathbb{C}$ vs that of a qubit $\mathcal{M}_2$:



classical trit



qubit

What is quantum computation?

A Bourbaki definition

A $\otimes$ category $\mathcal{C}$ can be viewed as a computational model. You can make (uniform) circuits of gates in $\mathcal{C}$, by definition locally bounded diagrams. The circuit size is the computation "time".

model	poly time	objects	morphisms	$\otimes$
deterministic	P	sets	functions	$\times$
probabilistic	BPP	$L^\infty(\Omega)$	stochastic maps	$\otimes$
quantum	BQP	$\mathcal{M}$	stochastic maps	$\otimes$

- Actually, the third column is overly fancy. We are interested in finite or finite-dimensional objects.
- In relevant cases, the input can be a bit string and the output can be converted to a bit or a bit string.

What is quantum computation?

A Bourbaki definition

A $\otimes$ category $\mathcal{C}$ can be viewed as a computational model. You can make (uniform) circuits of gates in $\mathcal{C}$, by definition locally bounded diagrams. The circuit size is the computation "time".

model	poly time	objects	morphisms	$\otimes$
deterministic	P	sets	functions	$\times$
probabilistic	BPP	$L^\infty(\Omega)$	stochastic maps	$\otimes$
quantum	BQP	$\mathcal{M}$	stochastic maps	$\otimes$

- Actually, the third column is overly fancy. We are interested in finite or finite-dimensional objects.
- In relevant cases, the input can be a bit string and the output can be converted to a bit or a bit string.

What is quantum computation?

Reduction to a CS definition

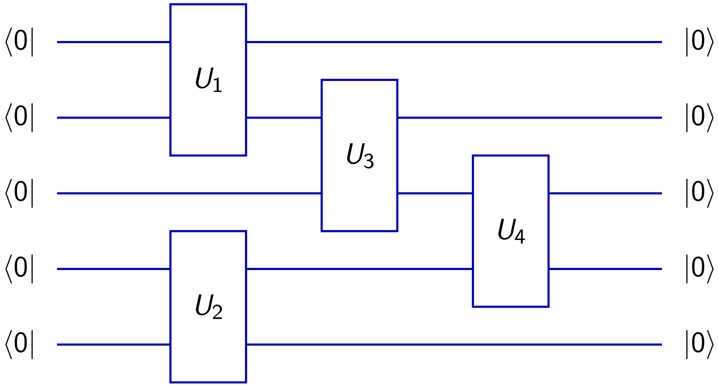
- The initial state can be pure: $\rho(a) = \langle\psi|a|\psi\rangle$.
- Stinespring's theorem: Every quantum map $\mathcal{M}_a^\# \to \mathcal{M}_b^\#$ comes from a unitary operator $U \in U(d)$.
- The "output" can be measured by pairing with a pure state.
- Local boundedness: You can compute with $\mathcal{M}_2^{\otimes n}$ (n qubits).
- Local generation: Two-qubit gates $\in \mathrm{U}(4)$ generate $\mathrm{U}(2^n)$.
- Dense generation: A better-founded model has finitely many gates that densely generate $\mathrm{U}(4)$ or $\mathrm{U}(2^n)$.

What is quantum computation?

Reduction to a CS definition

- The initial state can be pure: $\rho(a) = \langle\psi|a|\psi\rangle$.
- Stinespring's theorem: Every quantum map $\mathcal{M}_a^\# \to \mathcal{M}_b^\#$ comes from a unitary operator $U \in U(d)$.
- The "output" can be measured by pairing with a pure state.
- Local boundedness: You can compute with $\mathcal{M}_2^{\otimes n}$ (n qubits).
- Local generation: Two-qubit gates $\in \mathrm{U}(4)$ generate $\mathrm{U}(2^n)$.
- Dense generation: A better-founded model has finitely many gates that densely generate $\mathrm{U}(4)$ or $\mathrm{U}(2^n)$.

A quantum circuit



- Each $U_k \in \mathrm{U}(4)$ and $C \in \mathrm{U}(32)$ (or $\mathrm{U}(2^n)$).
- You could instead use qudits and make the gates k-local.

Quantum computation with quantum invariants

Theorem (Freedman, Larsen, Wang)

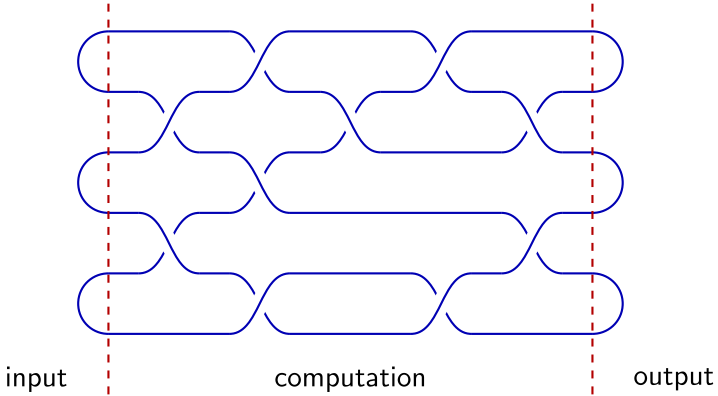
If $t = \exp(2\pi i/r)$ with $r = 5$ or $r \geq 7$, and if $n \geq 3$ ($n \geq 5$ when $r = 10$), then the Jones representation $\rho : B_n \to \mathrm{U}(N)$ is dense in $\mathrm{PSU}(N)$.

Theorem (Freedman, Kitaev, Wang; Aharonov, Jones, Landau)

A truncated Temperley-Lieb category with $r \geq 5$ is computationally equivalent to standard QC with $\mathrm{Vect}_{<\infty}(\mathbb{C})$.

Note: Unlike general quantum algebra, quantum probability and computation require unitary/Hermitian structures over $\mathbb{C}$.

A plat link diagram as a quantum circuit



By FLW, the Jones polynomial of this is a quantum circuit.

Other complexity classes

You can define many complexity classes within one category (by using controlled non-bounded structure).

- NP = A certificate of "yes" can be confirmed in P.
- PP = vote by a majority of fixed-length certificates.
- #P = output is the number of accepted certificates.
- A^B = class A using B as an oracle (or black box).

Example: If V is a variety over $\mathbb{F}_2$, whether it has an $\mathbb{F}_2$-rational point is in NP, whether it has at least N such points is in PP, and counting them is in #P.

In fact, these are all complete problems.

Other complexity classes

You can define many complexity classes within one category (by using controlled non-bounded structure).

- NP = A certificate of "yes" can be confirmed in P.
- PP = vote by a majority of fixed-length certificates.
- $\#$P = output is the number of accepted certificates.
- A^B = class A using B as an oracle (or black box).

Example: If V is a variety over $\mathbb{F}_2$, whether it has an $\mathbb{F}_2$-rational point is in NP, whether it has at least N such points is in PP, and counting them is in $\#$P.

In fact, these are all complete problems.

Complexity class relations

Theorem (Adleman, DeMarrais, Huang; et al)

$$\mathrm{BQP} \subseteq \mathrm{PP}.$$

Theorem (Toda)

$$\mathrm{NP}^{\mathrm{NP}^{\cdot^{\cdot^{\cdot^{\mathrm{NP}}}}}} \subseteq \mathrm{P}^{\#\mathrm{P}} = \mathrm{P}^{\mathrm{PP}}.$$

- No relation between BQP and NP is known.
- By Toda's theorem, PP is thought to be very large.

PostBQP

Theorem (Aaronson)

$$\mathrm{PostBQP} = \mathrm{PP}.$$

- By definition, PostBQP is BQP with free retries. The computer outputs "yes", "no", or "try again"; only the ratio of "yes" to "no" matters.
- Equivalently, Alice and Bob each do a quantum computation. They may both be very unlikely to output "yes". In PostBQP, we say "yes" if Alice is twice as likely to succeed as Bob; and "no" if vice-versa.
- PostBPP can also be defined; it is not much larger than NP.

PostBQP

Theorem (Aaronson)

$$\mathsf{PostBQP} = \mathsf{PP}.$$

- By definition, PostBQP is BQP with free retries. The computer outputs "yes", "no", or "try again"; only the ratio of "yes" to "no" matters.
- Equivalently, Alice and Bob each do a quantum computation. They may both be very unlikely to output "yes". In PostBQP, we say "yes" if Alice is twice as likely to succeed as Bob; and "no" if vice-versa.
- PostBPP can also be defined; it is not much larger than NP.

PostBQP

Theorem (Aaronson)

$$\mathrm{PostBQP} = \mathrm{PP}.$$

- By definition, PostBQP is BQP with free retries. The computer outputs "yes", "no", or "try again"; only the ratio of "yes" to "no" matters.
- Equivalently, Alice and Bob each do a quantum computation. They may both be very unlikely to output "yes". In PostBQP, we say "yes" if Alice is twice as likely to succeed as Bob; and "no" if vice-versa.
- PostBPP can also be defined; it is not much larger than NP.

Putting it all together

Theorem

Let $t = \exp(2\pi i/r)$ with $r = 5$ or $r \geq 7$. Let $a > b > 0$. Then $|V(L,t)| > a$ vs $|V(L,t)| < b$ is $\#\mathrm{P}$-hard.

Proof.

- Estimating $|V(L,t)|$ is universal for quantum computation.
- But without bridge number normalization, we are estimating exponentially small probabilities.
- Thus, a rough estimate of $|V(L,t)|$ is PostBQP-hard.
- How hard is that? By Aaronson's theorem, PP-hard.
- Which is the same as $\#$P-hard, by playing high-low. □

Putting it all together

Theorem

Let $t = \exp(2\pi i/r)$ *with* $r = 5$ *or* $r \geq 7$*. Let* $a > b > 0$*. Then* $|V(L,t)| > a$ *vs* $|V(L,t)| < b$ *is* #P*-hard.*

Proof.

- Estimating $|V(L,t)|$ is universal for quantum computation.
- But without bridge number normalization, we are estimating exponentially small probabilities.
- Thus, a rough estimate of $|V(L,t)|$ is PostBQP-hard.
- How hard is that? By Aaronson's theorem, PP-hard.
- Which is the same as #P-hard, by playing high-low.

□

Putting it all together

Theorem

Let $t = \exp(2\pi i/r)$ *with* $r = 5$ *or* $r \geq 7$*. Let* $a > b > 0$*. Then* $|V(L,t)| > a$ *vs* $|V(L,t)| < b$ *is* $\#\mathrm{P}$*-hard.*

Proof.

- Estimating $|V(L,t)|$ is universal for quantum computation.
- But without bridge number normalization, we are estimating exponentially small probabilities.
- Thus, a rough estimate of $|V(L,t)|$ is PostBQP-hard.
- How hard is that? By Aaronson's theorem, PP-hard.
- Which is the same as $\#$P-hard, by playing high-low. □

Putting it all together

Theorem

Let $t = \exp(2\pi i/r)$ with $r = 5$ or $r \geq 7$. Let $a > b > 0$. Then $|V(L,t)| > a$ vs $|V(L,t)| < b$ is $\#\mathrm{P}$-hard.

Proof.

- Estimating $|V(L,t)|$ is universal for quantum computation.
- But without bridge number normalization, we are estimating exponentially small probabilities.
- Thus, a rough estimate of $|V(L,t)|$ is PostBQP-hard.
- How hard is that? By Aaronson's theorem, PP-hard.
- Which is the same as $\#$P-hard, by playing high-low.

□

Putting it all together

Theorem

Let $t = \exp(2\pi i/r)$ *with* $r = 5$ *or* $r \geq 7$*. Let* $a > b > 0$*. Then* $|V(L,t)| > a$ *vs* $|V(L,t)| < b$ *is* $\#\mathrm{P}$*-hard.*

Proof.

- Estimating $|V(L,t)|$ is universal for quantum computation.
- But without bridge number normalization, we are estimating exponentially small probabilities.
- Thus, a rough estimate of $|V(L,t)|$ is PostBQP-hard.
- How hard is that? By Aaronson's theorem, PP-hard.
- Which is the same as #P-hard, by playing high-low. $\square$

Related results and questions

The reductions suggest that the divide-and-conquer algorithms to compute $V(L, t)$ and similar are nearly optimal.

Theorem (K.)

If $t^r \neq 1$, the Jones representation ρ_n is Zariski dense in $\mathrm{PSL}(N, \mathbb{C})$.

Corollary

If $t^r \neq 1$ and some Jones representation ρ_n is indiscrete, then it is dense, so estimating $|V(L, t)|$ is $\#\mathrm{P}$-hard.

Non-unitary linear computation is okay in context. Indiscreteness may be more than needed for hardness.

Question

How hard is it to compute $\deg |V(L, t)|$?

Related results and questions

The reductions suggest that the divide-and-conquer algorithms to compute $V(L,t)$ and similar are nearly optimal.

Theorem (K.)

If $t^r \neq 1$, the Jones representation ρ_n is Zariski dense in $\mathrm{PSL}(N,\mathbb{C})$.

Corollary

If $t^r \neq 1$ and some Jones representation ρ_n is indiscrete, then it is dense, so estimating $|V(L,t)|$ is $\#\mathrm{P}$-hard.

Non-unitary linear computation is okay in context. Indiscreteness may be more than needed for hardness.

Question

How hard is it to compute $\deg |V(L,t)|$?

Related results and questions

The reductions suggest that the divide-and-conquer algorithms to compute $V(L, t)$ and similar are nearly optimal.

Theorem (K.)

If $t^r \neq 1$, the Jones representation ρ_n is Zariski dense in $\mathrm{PSL}(N, \mathbb{C})$.

Corollary

If $t^r \neq 1$ and some Jones representation ρ_n is indiscrete, then it is dense, so estimating $|V(L, t)|$ is $\#\mathrm{P}$-hard.

Non-unitary linear computation is okay in context. Indiscreteness may be more than needed for hardness.

Question

How hard is it to compute $\deg |V(L, t)|$?