Inapproximability of Positive Semidefinite Permanents and Quantum State Tomography

arXiv:2111.03142

Alexander Meiburg

University of California, Santa Barbara

Oct 2022

Some facts about permanents

- Defn:

$$\mathrm{Perm}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} A_{i,\sigma(i)} \tag{1}$$

Some facts about permanents

- Defn:

$$\text{Perm}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} A_{i,\sigma(i)} \tag{1}$$

- Naive $O(n!)$ time, can do $O(2^n)$ [Ryser, 63]

Some facts about permanents

- Defn:

$$\text{Perm}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} A_{i,\sigma(i)} \tag{1}$$

- Naive $O(n!)$ time, can do $O(2^n)$ [Ryser, 63]
- #P-hard to compute exactly [Valiant, 79]

Some facts about permanents

- Defn:

$$\mathrm{Perm}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} A_{i,\sigma(i)} \tag{1}$$

- Naive $O(n!)$ time, can do $O(2^n)$ [Ryser, 63]
- #P-hard to compute exactly [Valiant, 79]
- FPRAS if all entries are nonnegative [JSV, 01]

Some facts about permanents

- Defn:

$$\text{Perm}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} A_{i,\sigma(i)} \tag{1}$$

- Naive $O(n!)$ time, can do $O(2^n)$ [Ryser, 63]
- #P-hard to compute exactly [Valiant, 79]
- FPRAS if all entries are nonnegative [JSV, 01]

If A is positive-semidefinite (PSD):

- Can be written as nonnegative integral, so $\text{Perm}(A) \geq 0$

Some facts about permanents

- Defn:

$$\text{Perm}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} A_{i,\sigma(i)} \tag{1}$$

- Naive $O(n!)$ time, can do $O(2^n)$ [Ryser, 63]
- #P-hard to compute exactly [Valiant, 79]
- FPRAS if all entries are nonnegative [JSV, 01]

If A is positive-semidefinite (PSD):

- Can be written as nonnegative integral, so $\text{Perm}(A) \geq 0$
- Is in the class FBPP^{NP} (Stockmeyer counting)

Some facts about permanents

- Defn:

$$\mathrm{Perm}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} A_{i,\sigma(i)} \tag{1}$$

- Naive $O(n!)$ time, can do $O(2^n)$ [Ryser, 63]
- #P-hard to compute exactly [Valiant, 79]
- FPRAS if all entries are nonnegative [JSV, 01]

If A is positive-semidefinite (PSD):

- Can be written as nonnegative integral, so $\mathrm{Perm}(A) \geq 0$
- Is in the class $\mathsf{FBPP}^{\mathsf{NP}}$ (Stockmeyer counting)
- Still hard to compute exactly

Consider $\mathrm{Perm}((1-\epsilon)I + \epsilon A)$ for any A. Polynomial in ϵ, can extrapolate to $\epsilon = 1$.

Some facts about permanents

If A is positive-semidefinite (PSD):

- Can be written as nonnegative integral, so $\text{Perm}(A) \geq 0$
- Is in the class FBPP^{NP} (Stockmeyer counting)
- Still hard to compute exactly
- Can efficiently compute a 4.85^n approximation [Anari+, 17]

Some facts about permanents

If A is positive-semidefinite (PSD):

- Can be written as nonnegative integral, so $\mathrm{Perm}(A) \geq 0$
- Is in the class $\mathsf{FBPP}^{\mathsf{NP}}$ (Stockmeyer counting)
- Still hard to compute exactly
- Can efficiently compute a 4.85^n approximation [Anari+, 17]
- FPRAS if $\lambda_{\mathrm{max}}/\lambda_{\mathrm{min}} \leq 2$ [Barvinok, 20]

Some facts about permanents

If A is positive-semidefinite (PSD):

- Can be written as nonnegative integral, so $\mathrm{Perm}(A) \geq 0$
- Is in the class $\mathsf{FBPP}^{\mathsf{NP}}$ (Stockmeyer counting)
- Still hard to compute exactly
- Can efficiently compute a 4.85^n approximation [Anari+, 17]
- FPRAS if $\lambda_{\max}/\lambda_{\min} \leq 2$ [Barvinok, 20]
- Represent output probabilities of "BosonSampling" quantum computers when inputs are thermal (as opposed to coherent beams)

Some facts about permanents

If A is positive-semidefinite (PSD):

- Can be written as nonnegative integral, so $\mathrm{Perm}(A) \geq 0$
- Is in the class $\mathsf{FBPP}^{\mathsf{NP}}$ (Stockmeyer counting)
- Still hard to compute exactly
- Can efficiently compute a 4.85^n approximation [Anari+, 17]
- FPRAS if $\lambda_{\max}/\lambda_{\min} \leq 2$ [Barvinok, 20]
- Represent output probabilities of "BosonSampling" quantum computers when inputs are thermal (as opposed to coherent beams)
- Quantum connection inspired other algorithms, that also work better when spectral radius is small [CCG, 17]

Some facts about permanents

If A is positive-semidefinite (PSD):

- Can be written as nonnegative integral, so $\mathrm{Perm}(A) \geq 0$
- Is in the class $\mathsf{FBPP}^{\mathsf{NP}}$ (Stockmeyer counting)
- Still hard to compute exactly
- Can efficiently compute a 4.85^n approximation [Anari+, 17]
- FPRAS if $\lambda_{\max}/\lambda_{\min} \leq 2$ [Barvinok, 20]
- Represent output probabilities of "BosonSampling" quantum computers when inputs are thermal (as opposed to coherent beams)
- Quantum connection inspired other algorithms, that also work better when spectral radius is small [CCG, 17]

Question remains: are these hard to approximate?

A question about quantum state estimation

I had many copies of an unknown quantum state $|\psi\rangle$, a unit vector in $\mathbb{C}^d$. I have taken some number n of measurements, and now I would like to estimate ψ as accurately as possible.

A question about quantum state estimation

I had many copies of an unknown quantum state $|\psi\rangle$, a unit vector in $\mathbb{C}^d$. I have taken some number n of measurements, and now I would like to estimate ψ as accurately as possible. Note:

- Measurements γ_i are (wlog) unit vectors in $\mathbb{C}^d$, each ψ has a likelihood $|\psi^\dagger \gamma_i|^2$

A question about quantum state estimation

I had many copies of an unknown quantum state $|\psi\rangle$, a unit vector in $\mathbb{C}^d$. I have taken some number n of measurements, and now I would like to estimate ψ as accurately as possible. Note:

- Measurements γ_i are (wlog) unit vectors in $\mathbb{C}^d$, each ψ has a likelihood $|\psi^\dagger \gamma_i|^2$
- Measurements are already performed. Not a question of picking what to measure

A question about quantum state estimation

I had many copies of an unknown quantum state $|\psi\rangle$, a unit vector in $\mathbb{C}^d$. I have taken some number n of measurements, and now I would like to estimate ψ as accurately as possible. Note:

- Measurements γ_i are (wlog) unit vectors in $\mathbb{C}^d$, each ψ has a likelihood $|\psi^\dagger \gamma_i|^2$
- Measurements are already performed. Not a question of picking what to measure
- State space d is *not* big. Physically, only $\log(d)$ many qubits

A question about quantum state estimation

I had many copies of an unknown quantum state $|\psi\rangle$, a unit vector in $\mathbb{C}^d$. I have taken some number n of measurements, and now I would like to estimate ψ as accurately as possible. Note:

- Measurements γ_i are (wlog) unit vectors in $\mathbb{C}^d$, each ψ has a likelihood $|\psi^\dagger \gamma_i|^2$
- Measurements are already performed. Not a question of picking what to measure
- State space d is *not* big. Physically, only $\log(d)$ many qubits
- Estimating ψ equivalent to estimating a complete basis of its observables

A question about quantum state estimation

I had many copies of an unknown quantum state $|\psi\rangle$, a unit vector in $\mathbb{C}^d$. I have taken some number n of measurements, and now I would like to estimate ψ as accurately as possible. Note:

- Measurements γ_i are (wlog) unit vectors in $\mathbb{C}^d$, each ψ has a likelihood $|\psi^\dagger \gamma_i|^2$
- Measurements are already performed. Not a question of picking what to measure
- State space d is *not* big. Physically, only $\log(d)$ many qubits
- Estimating ψ equivalent to estimating a complete basis of its observables
- Also equivalent to estimating overall probability of these measurement (partition function)

A question about quantum state estimation

I had many copies of an unknown quantum state $|\psi\rangle$, a unit vector in $\mathbb{C}^d$. I have taken some number n of measurements, and now I would like to estimate ψ as accurately as possible. Note:

- Measurements γ_i are (wlog) unit vectors in $\mathbb{C}^d$, each ψ has a likelihood $|\psi^\dagger \gamma_i|^2$
- Measurements are already performed. Not a question of picking what to measure
- State space d is *not* big. Physically, only $\log(d)$ many qubits
- Estimating ψ equivalent to estimating a complete basis of its observables
- Also equivalent to estimating overall probability of these measurement (partition function)

Main result: this is NP-hard to approximate within an exponential factor!

Connection to permanents

Measurements γ_i form an $n \times d$ matrix Γ. Partition function Z is a function only of Γ.

$$Z = \int_{\mathbb{C}_1^d} \prod_i P(\gamma_i | \psi) \, d\psi = \int_{\mathbb{C}_1^d} \prod_i (\psi^\dagger \gamma_i)(\gamma_i^\dagger \psi) \, d\psi$$

Connection to permanents

Measurements γ_i form an $n \times d$ matrix Γ. Partition function Z is a function only of Γ.

$$Z = \int_{\mathbb{C}_1^d} \prod_i P(\gamma_i | \psi)\, d\psi = \int_{\mathbb{C}_1^d} \prod_i (\psi^\dagger \gamma_i)(\gamma_i^\dagger \psi)\, d\psi$$

Invariant under permutations of n rows. Order of observations doesn't matter, each was from a fresh $|\psi\rangle$.

Invariant under a unitary transformation acting on the d-dimensional space. Just a change of basis.

Linear in each γ_i and its adjoint $\gamma_i^\dagger$. Enough to establish:

$$Z = C\, \mathrm{Perm}(\Gamma^\dagger \Gamma)$$

Connection to permanents

$$Z = C\,\mathrm{Perm}(\Gamma^\dagger\Gamma)$$

This matrix $\Gamma^\dagger\Gamma$ is $n \times n$ PSD. Constant C is easily computed as

$$C = \frac{2\pi^n}{(d+n-1)!}$$

Hardness of quantum state estimation $\rightarrow$ hardness of PSD permanents.

Z as an integral over unit sphere is very similar to other formulations (Barvinok) of PSD permanents as a spherical integral

Hardness of state estimation

Integrand

$$\prod_i (\psi^\dagger \gamma_i)(\gamma_i^\dagger \psi)$$

is a polynomial in the coordinates of ψ. Each observation γ_i adds a zero to this polynomial: zero chance that ψ is perpendicular to γ_i.

Hardness of state estimation

Integrand

$$\prod_i (\psi^\dagger \gamma_i)(\gamma_i^\dagger \psi)$$

is a polynomial in the coordinates of ψ. Each observation γ_i adds a zero to this polynomial: zero chance that ψ is perpendicular to γ_i.

Lots of zeros $\rightarrow$ highly oscillatory function $\rightarrow$ hard to maximize.

Hardness of state estimation

Suppose we have measurements in the standard basis. γ_1 is $(1, 0, 0, \dots)$, γ_2 is $(0, 1, 0, \dots)$, and so on.

Hardness of state estimation

Suppose we have measurements in the standard basis. γ_1 is $(1, 0, 0, \ldots)$, γ_2 is $(0, 1, 0, \ldots)$, and so on.

ψ can't have any zero (or small) entries. If kth entry is zero, then $\psi^\dagger \gamma_k$ is zero.

Hardness of state estimation

Suppose we have measurements in the standard basis. γ_1 is $(1, 0, 0, \ldots)$, γ_2 is $(0, 1, 0, \ldots)$, and so on.

ψ can't have any zero (or small) entries. If kth entry is zero, then $\psi^\dagger \gamma_k$ is zero.

By taking many copies of each basis vector (say, $O(d^2)$ many), we ensure that each entry of ψ is roughly equal in magnitude.

Hardness of state estimation

Only significant terms in the integral are:

$$\psi \approx \frac{1}{\sqrt{d}}(e^{i\theta_1}, e^{i\theta_2}, \ldots e^{i\theta_d})$$

By symmetry, we can fix $\theta_1 = 0$. Just a factor of 2π in the integral.

Hardness of state estimation

Only significant terms in the integral are:

$$\psi \approx \frac{1}{\sqrt{d}}(e^{i\theta_1}, e^{i\theta_2}, \dots e^{i\theta_d})$$

By symmetry, we can fix $\theta_1 = 0$. Just a factor of 2π in the integral. Assume we have measurements

$$\gamma_{+,2} = \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0, 0, 0, \dots\right)$$

$$\gamma_{-,2} = \left(\frac{1}{\sqrt{2}}, \frac{-1}{\sqrt{2}}, 0, 0, 0, \dots\right)$$

Then $e^{i\theta_2}$ cannot be close to -1 or $+1$. Probability is maximized with $+i$ and $-i$.

Hardness of state estimation

Only significant terms in the integral are:

$$\psi \approx \frac{1}{\sqrt{d}}(e^{i\theta_1}, e^{i\theta_2}, \dots e^{i\theta_d})$$

By symmetry, we can fix $\theta_1 = 0$. Just a factor of 2π in the integral. Assume we have measurements

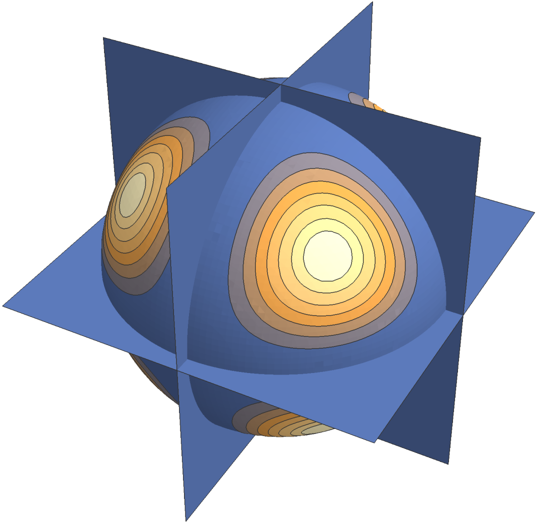
$$\gamma_{+,2} = \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0, 0, 0, \dots \right)$$

$$\gamma_{-,2} = \left(\frac{1}{\sqrt{2}}, \frac{-1}{\sqrt{2}}, 0, 0, 0, \dots \right)$$

Then $e^{i\theta_2}$ cannot be close to -1 or $+1$. Probability is maximized with $+i$ and $-i$.

By taking many copies of $\gamma_{+,k}$ and $\gamma_{-,k}$, ensure that all $e^{i\theta_k}$ are close to $+i$ or $-i$.

$$\psi \approx \frac{1}{\sqrt{d}}(1, \pm i, \cdots \pm i)$$



Hardness of state estimation

At this point, we get a concentration result on these 2^{d-1} points: total integral is proportional to sum of likelihood of these points, plus an exponentially smaller additive error.

Hardness of state estimation

At this point, we get a concentration result on these 2^{d-1} points: total integral is proportional to sum of likelihood of these points, plus an exponentially smaller additive error.

Cut out some of the points (any way you like; there are many). The vector

$$\gamma_{(234)} = \left(0, \frac{-2}{\sqrt{6}}, \frac{1}{\sqrt{6}}, \frac{1}{\sqrt{6}}, 0, 0, 0 \ldots \right)$$

is perpendicular to $(0, 1, 1, 1, 0, 0, 0 \ldots)$, and eliminates the possibility that all three signs are equal.

Hardness of state estimation

At this point, we get a concentration result on these 2^{d-1} points: total integral is proportional to sum of likelihood of these points, plus an exponentially smaller additive error.

Cut out some of the points (any way you like; there are many). The vector

$$\gamma_{(234)} = \left(0, \frac{-2}{\sqrt{6}}, \frac{1}{\sqrt{6}}, \frac{1}{\sqrt{6}}, 0, 0, 0 \dots\right)$$

is perpendicular to $(0, 1, 1, 1, 0, 0, 0 \dots)$, and eliminates the possibility that all three signs are equal.

$$\gamma_{(234),B} = \left(0, \frac{1}{\sqrt{6}}, \frac{-2}{\sqrt{6}}, \frac{1}{\sqrt{6}}, 0, 0, 0 \dots\right)$$

$$\gamma_{(234),C} = \left(0, \frac{1}{\sqrt{6}}, \frac{1}{\sqrt{6}}, \frac{-2}{\sqrt{6}}, 0, 0, 0 \dots\right)$$

to keep the probability symmetric across which of the three signs should differ.

Hardness of state estimation

Reduce from NOT-ALL-EQUAL-3SAT: given some triples of variables, finding an assignment of Boolean variables such that no specified triple has all equal values. NP-complete.

Hardness of state estimation

Reduce from NOT-ALL-EQUAL-3SAT: given some triples of variables, finding an assignment of Boolean variables such that no specified triple has all equal values. NP-complete.

Given a NAE-3SAT problem on v variables, can write down a set of $n = \text{poly}(v)$ measurements Γ on $d = v + 1$ variables, such that:

- If there is a solution to original problem, at least one ψ with high likelihood, Z is at least some $f(n)$.
- If no solution, all ψ exponentially unlikely, Z at most $f(n)2^{-\text{poly}(d)}$.

For any $C < 1$, NP-hard to estimate Z within a factor 2^{n^C}.

Consequences, Future Work

- No APX for PSD permanents (unless $\mathrm{P} = \mathrm{NP}$)
- Haven't ruled out $(1+\epsilon)^n$ approximation algorithms
- These PSD matrices are always rank $d \ll n$. Likely to be more improvements in terms of spectral radius, $\lambda_{\mathrm{min}} > 0$
- Only showed NP-hardness (0 solutions or ≥ 1?). Can likely improve to approximately counting solutions
- Doesn't mean quantum state tomography is *typically* hard: these types of measurements are unlikely
- Would be nice to show that some efficient algorithms for state reconstructions converge with high probability as more measurements are taken (from any basis)

Thank you!