New Hardness Results for the Permanent Using Linear Optics

Daniel Grier   Luke Schaeffer
MIT

Permanent Review

Permanent: Given $n \times n$ matrix $A = \{a_{i,j}\}$

$$\mathrm{per}(A) = \sum_{\sigma \in \mathrm{S}_n} \prod_{i=1}^{n} a_{i,\sigma(i)}$$

Example:

$$A = \begin{pmatrix} 0 & -1 & 2 \\ 3 & 4 & -2 \\ 1 & 2 & 1 \end{pmatrix}$$

$$\mathrm{per}(A) = 0 + 0 - 3 + 2 + 12 + 8 = 19$$

Permanent complexity

Ryser's/Glynn's formula: Permanent can be computed in time $O(n2^n)$.

Question: Can the permanent be efficiently computed?

→ **Probably not:** $\textsc{Per} \in \mathsf{PH} \implies \mathsf{PH}$ collapses

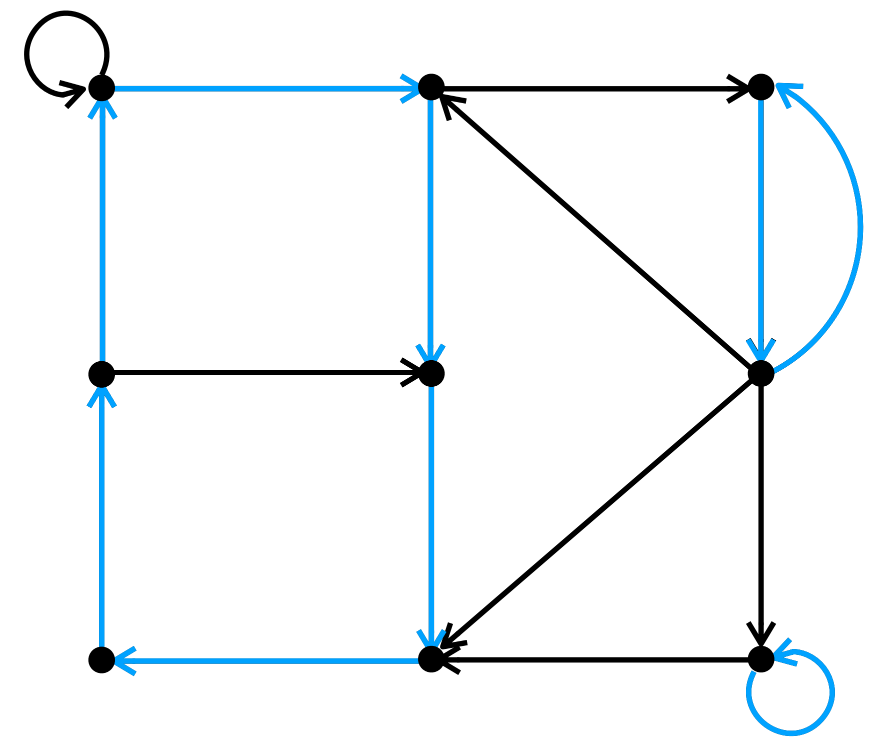
Theorem [Valiant (1979)]: The permanent of a matrix is $\#\mathsf{P}$-hard to compute.

$\#\mathsf{P}$**-hardness:** Let $\textsc{Per}$ be an oracle which computes the permanent of a matrix.

$$\#\mathsf{P} \subseteq \mathsf{FP}^{\textsc{Per}}$$

Permanent counts cycle covers

$$A = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$



Combinatorial interpretation:

- If A is adjacency matrix, then
  $\mathrm{per}(A)$ = the number of cycle covers of graph.

- If A is adjacency matrix with edge weights, then
  $\mathrm{per}(A)$ = the sum of the weighted cycle covers of graph.

Valiant's reduction

Idea behind Valiant's proof: Construct graph such that the weighted cycle covers correspond to the number of solutions to a 3SAT formula.

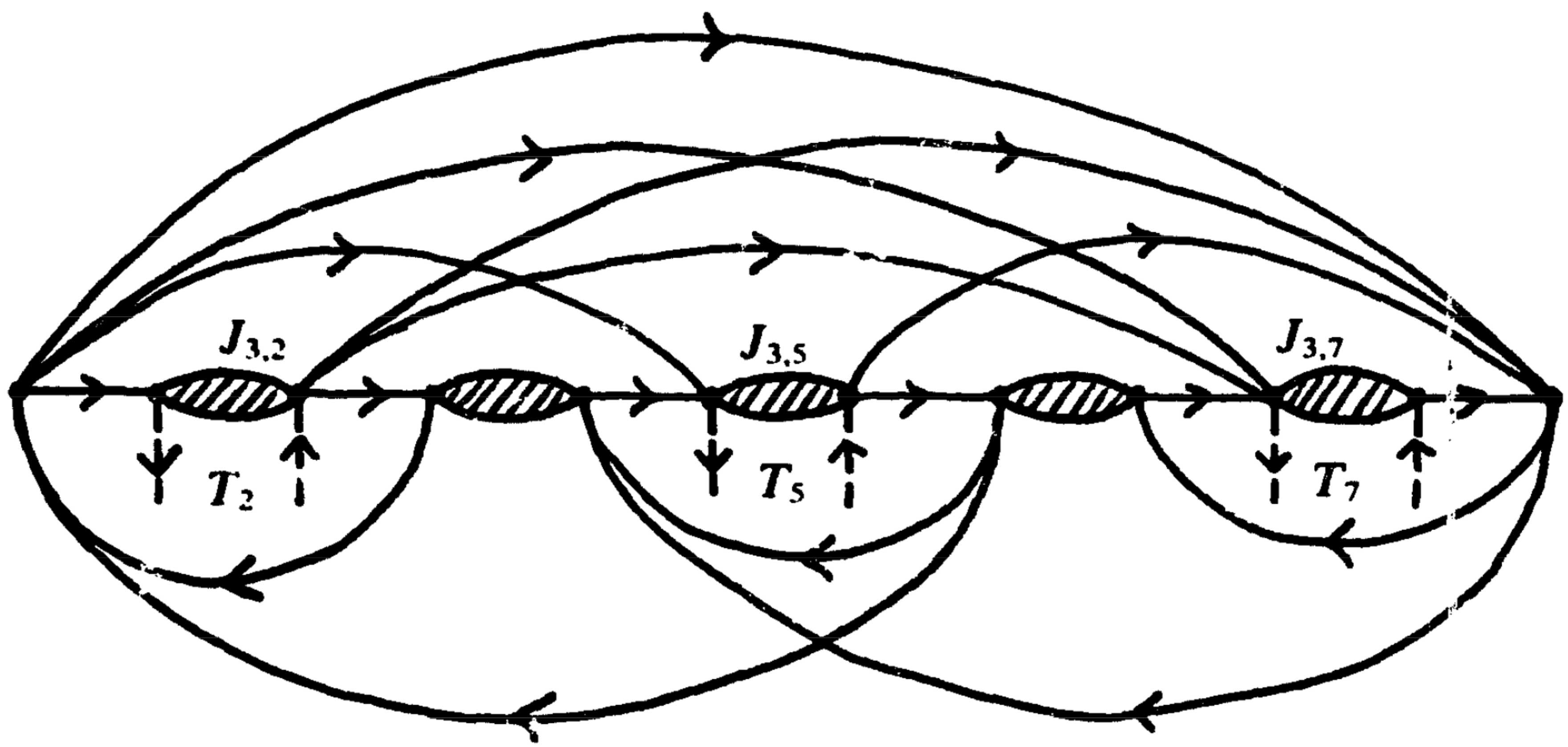


Figure: A single "interchange" in Valiant's original proof

Going beyond Valiant's reduction

Drawbacks to Valiant's reduction:

1) Relies on complicated cycle cover gadgets

- Ben-Dor and Halevi (1993): Simplified cycle cover argument
- Terry Rudolph (2009): Built subclass of quantum circuits with amplitudes proportional to the permanent
- Scott Aaronson (2011): #P-hardness of permanent from linear optics

→ **Why Quantum?** Offload difficulty onto well-known theorems in linear optics

2) Not suited for "structured" matrices

- Invertible: Valiant's matrices are probably invertible, but tedious to prove
- Unitary: Valiant's matrices are not unitary, and no obvious way forward

Plan: Modify Aaronson's proof and use quantum reductions to handle classes of matrices not suited for reductions based on cycle covers.

#P-hardness for new classes of matrices

Theorem: The permanent of an $n \times n$ matrix A in any of the classical Lie groups over the complex numbers is $\#$P-hard:

$$\textbf{General linear: } A \in \mathrm{GL}(n) \text{ iff } \det(A) \neq 0$$

$$\textbf{Orthogonal: } A \in \mathrm{O}(n) \text{ iff } AA^T = I_n$$

$$\textbf{Unitary: } A \in \mathrm{U}(n) \text{ iff } AA^\dagger = I_n$$

$$\textbf{Symplectic: } A \in \mathrm{Sp}(2n) \text{ iff } A^T \Omega A = \Omega \text{ where } \Omega = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$$

Theorem: Let $p \neq 2, 3$ be prime. There exists a finite field of characteristic p, namely $\mathbb{F}_{p^4}$, such that the permanent of an orthogonal matrix in $\mathbb{F}_{p^4}$ is hard for the class $\mathrm{Mod}_p\mathrm{P}$.

Dichotomy

$p = 2$: Permanent = determinant

$p = 3$: Nontrivial algorithm due to Kogan (1996)

Theorem: The permanent of an orthogonal matrix over $\mathbb{F}_p$ is $\mathrm{Mod}_p\mathrm{P}$-hard for 1/16th of all primes.

Outline of Aaronson's proof

Input: Given polynomially sized circuit $C : \{0,1\}^n \to \{0,1\}$
Output: Number of unsatisfying assignments minus satisfying assignments to C

$$\Delta_C := \sum_{x \in \{0,1\}^n} (-1)^{C(x)}$$

our contribution (① to ②)

① Encode Δ_C into the transition amplitude of a quantum circuit Q over qubits

② Convert Q into a linear optical network L

③ Use correspondence between linear optics and permanents

$$\Delta_C \propto \langle 0 \dots 0 | \, Q \, | 0 \dots 0 \rangle \quad \propto \quad \langle 1, 0, \dots | \, \varphi(L) \, | 1, 0, \dots \rangle \quad \propto \quad \mathrm{per}(L_{I,I})$$

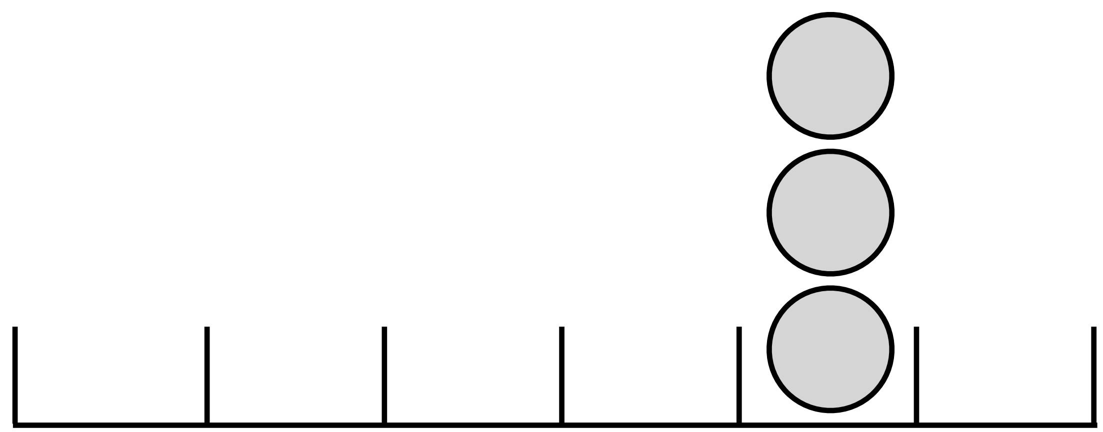
Comparison of linear optics

Quantum computing with qudits	Linear optics with photons
States: $\lvert\psi\rangle \in (\mathbb{C}^m)^{\otimes n}$	**States:** $\lvert\psi\rangle \in (\mathbb{C}^m)^{\odot n}$ ↓ *symmetric* tensor product $v_1 \odot \ldots \odot v_n = \frac{1}{n!} \sum_{\sigma \in \mathrm{S}_n} v_{\sigma(1)} \otimes \ldots \otimes v_{\sigma(n)}$
Operations: $U \in \mathrm{U}(m^n)$	**Operations:** $L^{\otimes n}$ for $L \in \mathrm{U}(m)$

Linear Optics - States

States: n photons and m modes

photons ~ indistinguishable balls
modes ~ distinct bins/locations



Notation: Let $|s_1, s_2, \ldots, s_m\rangle$ be the state with s_1 photons in the first mode, s_2 in the second, and so on.

For example: $\frac{|1,1,1,0,0,0\rangle + |0,2,0,0,1,0\rangle}{\sqrt{2}}$

Linear Optics - Transformations

Idea: Linear optical transformation is specified by its action on a single photon. Apply homomorphism to lift to entire Hilbert space for multiple photons.

φ**-transition formula:** Given $m \times m$ unitary L, the amplitude from state $|S\rangle = |s_1, s_2, \ldots, s_m\rangle$ to state $|T\rangle = |t_1, t_2, \ldots, t_m\rangle$ is

$$\langle T| \varphi(L) |S\rangle = \frac{\mathrm{per}(L_{S,T})}{\sqrt{s_1! s_2! \ldots s_m! t_1! t_2! \ldots t_m!}}$$

where $L_{S,T}$ is the matrix obtained by taking

- s_i copies of row i from L
- t_i copies of column i from L

Example:

$$L = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \begin{array}{l} |S\rangle = |1,1\rangle \\ |T\rangle = |2,0\rangle \end{array} \quad L_{S,T} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \quad \langle 2,0| \varphi(L) |1,1\rangle = \frac{1}{\sqrt{2}}$$

Observation: If $|S\rangle = |T\rangle = |1, \ldots, 1\rangle$, then $\langle T| \varphi(L) |S\rangle = \mathrm{per}(L)$.

Outline of #P-hardness proof

Input: Given polynomially sized circuit $C : \{0,1\}^n \to \{0,1\}$
Output: Number of satisfying assignments minus unsatisfying assignments to C

$$\Delta_C := \sum_{x \in \{0,1\}^n} (-1)^{C(x)}$$

① Encode Δ_C into the transition amplitude of a quantum circuit Q over qubits

② Convert Q into a linear optical network L

③ Use correspondence between linear optics and permanents

Postselected linear optics is quantum universal

Theorem [Knill, Laflamme, Milburn (2001)]:
Postselected linear optical circuits are universal for quantum computation.

Formally, given quantum circuit Q with polynomially many CSIGN and single-qubit gates, there exists linear optical circuit L with polynomially many modes such that

$$\langle I|\,\varphi(L)\,|I\rangle = \frac{1}{4^\Gamma}\,\langle 0\cdots 0|\,Q\,|0\cdots 0\rangle$$

where,

$$|I\rangle = |0,1,0,1,\ldots,0,1\rangle$$

$\Gamma =$ number of CSIGN gates in Q

Note: CSIGN + single-qubits gates are universal for quantum computation

$$\mathrm{CSIGN}\,|x_1x_2\rangle = (-1)^{x_1x_2}\,|x_1x_2\rangle$$

Theorem [Aaronson (2011)]:

not unitary

$$\frac{\Delta_C}{2^n} = \langle 0\ldots 0|\,Q\,|0\ldots 0\rangle = 4^\Gamma\,\langle I|\,\varphi(L)\,|I\rangle = 4^\Gamma \mathrm{per}(L_{I,I})$$

KLM protocol - representing states

Theorem [Knill, Laflamme, Milburn (2001)]:
Given quantum circuit Q with polynomially many CSIGN and single-qubit gates, there exists linear optical circuit L with polynomially many modes such that

$$\langle I| \varphi(L) |I\rangle = \frac{1}{4^\Gamma} \langle 0 \cdots 0| Q |0 \cdots 0\rangle$$

where $|I\rangle = |0, 1, 0, 1, \ldots, 0, 1\rangle$

Representing qubits with linear optical states:

Problem: qubit is either in state $|0\rangle$ or $|1\rangle$, but number of photons is conserved

Solution: use two modes and one photon to encode a single qubit

Dual rail encoding

$|0\rangle \rightarrow |0, 1\rangle$

$|1\rangle \rightarrow |1, 0\rangle$

qubits linear optical state

→ This is the source of non-unitarity in Aaronson's proof

Add new encoding phase to KLM

Goal: Construct linear optical circuit L from Q such that

$$\langle 1,1,\ldots,1|\,\varphi(L)\,|1,1,\ldots,1\rangle \propto \langle 0\cdots 0|\,Q\,|0\cdots 0\rangle$$

Problem: KLM uses dual rail encoding.

Solution: Prepare the dual rail encoding using another gadget.

KLM solution: 1 qubit represented by 1 photon and 2 modes

Our solution: 1 qubit represented by 4 photons and 4 modes

$$|1,1,1,1\rangle$$

Encoding gadget →

$$|0,1,2,1\rangle$$

dual rail encoding

dumpster

postselected photon

Add new encoding phase to KLM

Goal: Construct linear optical circuit L from Q such that

$$\langle 1, 1, \ldots, 1| \, \varphi(L) \, |1, 1, \ldots, 1\rangle \propto \langle 0 \cdots 0| \, Q \, |0 \cdots 0\rangle$$

Problem: KLM uses dual rail encoding.

Solution: Prepare the dual rail encoding using another gadget.

KLM solution: 1 qubit represented by 1 photon and 2 modes

Our solution: 1 qubit represented by 4 photons and 4 modes

$$|1, 1, 1, 1\rangle$$

Encoding gadget ⟶

$$|0, 1, 2, 1\rangle$$

Decoding gadget ⟶

$$|1, 1, 1, 1\rangle$$

Putting it all together

Theorem:

$$\frac{\Delta_C}{2^n} = \langle 0\ldots 0|\, Q\, |0\ldots 0\rangle$$

$$= (-\sqrt{6})^n \left(3\sqrt{\frac{3}{2}}\right)^{\Gamma} \langle 1,\ldots,1|\, \varphi(L)\, |1,\ldots,1\rangle$$

$$= (-\sqrt{6})^n \left(3\sqrt{\frac{3}{2}}\right)^{\Gamma} \mathrm{per}(L)$$

unitary

How do you find gadgets?

1. Guess transformation
2. Use constraint solver

$$E = \frac{1}{\sqrt{6}} \begin{pmatrix} \sqrt{2} & -\sqrt{2} & \sqrt{2} \\ 0 & \sqrt{3} & \sqrt{3} \\ -2 & -1 & 1 \end{pmatrix}$$

Permanent hardness over finite fields

Theorem: Permanent is $\#$P-hard for unitary matrices.

↓

Theorem: Let $p \neq 2, 3$ be prime. There exists a finite field of characteristic p, namely $\mathbb{F}_{p^4}$, such that the permanent of an orthogonal matrix in $\mathbb{F}_{p^4}$ is Mod$_p$P-hard.

Proof: Inspect gadgets carefully

All entries in $\mathbb{Q}(\alpha)$

$$\alpha = \sqrt{2+\sqrt{2}} + \sqrt{3+\sqrt{6}}$$

$$E = \frac{1}{\sqrt{6}} \begin{pmatrix} \sqrt{2} & -\sqrt{2} & \sqrt{2} \\ 0 & \sqrt{3} & \sqrt{3} \\ -2 & -1 & 1 \end{pmatrix}$$

$$V = \frac{1}{3\sqrt{2}} \begin{pmatrix} -\sqrt{2} & -2 & 2 & 2\sqrt{2} \\ 2 & -\sqrt{2} & -2\sqrt{2} & 2 \\ -\sqrt{6+2\sqrt{6}} & \sqrt{6-2\sqrt{6}} & -\sqrt{3+\sqrt{6}} & \sqrt{3-\sqrt{6}} \\ -\sqrt{6-2\sqrt{6}} & -\sqrt{6+2\sqrt{6}} & -\sqrt{3-\sqrt{6}} & -\sqrt{3+\sqrt{6}} \end{pmatrix}$$

Summarizing matrix permanent complexity

	$\mathbb{C}^{n\times n}$	$\mathrm{SO}(n)$	$\{0,1\}^{n\times n}$	$x^T A x \geq 0$
exact	**#P-hard** [Valiant 79]	**#P-hard** [GS 2017]	**#P-hard** [Valiant 79]	**#P-hard** [GS 2017]
approximate	**#P-hard** [Valiant 79]	**#P-hard** [GS 2017]	**FPTAS** [JSV 2004]	**???**

Open Problems:

- Is there a polynomial-time approximation algorithm for permanents of positive-semidefinite matrices?
  - best known: polynomial time 4.84^n-approximation [AGGS 2017]
- Are orthogonal permanents over $\mathbb{F}_p$ hard for $\mathrm{Mod}_p\mathrm{P}$ for all $p \neq 2, 3$?
- Are there more insights about the permanent to be gained through this linear optical lens?
  - [CCG 2016] : under restricted conditions on the eigenvalues, can outperform Gurvits's *additive* approximation algorithm