Permanents and boson sampling

Stefan Scheel, Universität Rostock

Summer School on Modern Quantum Technologies

Menu

Outline:

- permanents in linear optics
- computational complexity
- boson sampling as intermediate model for quantum computation

Quantum optics of macroscopic systems

Permanents in linear optics

lossless beam splitter transformation for photonic amplitude operators:

$$\hat{\mathbf{b}} = \mathbf{T}\hat{\mathbf{a}} = \hat{U}^{\dagger}\hat{\mathbf{a}}\hat{U}\,, \quad \hat{U} = \exp\left[-i\hat{\mathbf{a}}^{\dagger}\boldsymbol{\Phi}\hat{\mathbf{a}}\right]\,, \quad \mathbf{T} = \exp\left[-i\boldsymbol{\Phi}\right]$$

- equivalent to discrete-time Heisenberg equation of motion
- transform quantum states by discrete-time Schrödinger equation using inverse transformation $\hat{\varrho}' = \hat{U}\hat{\varrho}\hat{U}^{\dagger}$

$$\langle\dot{\hat{O}}\rangle = \mathrm{Tr}[\hat{\varrho}\dot{\hat{O}}] = \mathrm{Tr}[\hat{\varrho}\underbrace{\hat{U}^{\dagger}\hat{O}\hat{U}}_{\text{Heisenberg}}] = \mathrm{Tr}[\underbrace{\hat{U}\hat{\varrho}\hat{U}^{\dagger}}_{\text{Schrödinger}}\hat{O}] = \mathrm{Tr}[\dot{\hat{\varrho}}\hat{O}]$$

Permanents in linear optics

transformation matrix **T** $\in$SU(2), but $\hat{U}$ in general is not:

- *n*-photon Fock space is *symmetric* tensor product of single-photon spaces
- quantum-state transformation $\hat{\varrho}' = \hat{U}\hat{\varrho}\hat{U}^\dagger$ according to a subgroup of SU($2n$)

example: matrix representation of $\hat{U}$ in basis $\{|0,0\rangle, |1,0\rangle, |0,1\rangle, |2,0\rangle, |1,1\rangle, |0,2\rangle\}$

$$\mathbf{U} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & T & -R^* & 0 & 0 & 0 \\ 0 & R & T^* & 0 & 0 & 0 \\ 0 & 0 & 0 & T^2 & \sqrt{2}T^*R^* & R^{*2} \\ 0 & 0 & 0 & \sqrt{2}TR & (|T|^2 - |R|^2) & -\sqrt{2}T^*R^* \\ 0 & 0 & 0 & R^2 & -\sqrt{2}TR & T^{*2} \end{pmatrix} = \bigoplus_{n=0}^{\infty} \mathbf{U}_n$$

- **U** is block-diagonal with respect to Fock layers of total photon numbers $(0, 1, 2)$
- **U** has direct product structure

Permanents in linear optics

matrix transforming quantum states acts on symmetric subspace $\Rightarrow$ can be constructed from permanents of transmission matrix $\mathbf{T}$

define set of all non-decreasing integer sequences $\boldsymbol{\omega}$ as
$G_{n,N} = \{\boldsymbol{\omega} : 1 \leq \omega_1 \leq \ldots \leq \omega_n \leq N\}$

matrix elements of $\hat{U}$ in the Fock basis are matrix permanents

$$\langle m_1, \ldots, m_N | \hat{U} | n_1, \ldots, n_N \rangle = \left(\prod_i n_i! \right)^{-1/2} \left(\prod_j m_j! \right)^{-1/2} \text{per}\, \mathbf{T}[\boldsymbol{\Omega}'|\boldsymbol{\Omega}]$$

$\boldsymbol{\Omega} = (1^{n_1}, 2^{n_2}, \ldots, N^{n_N}), \boldsymbol{\Omega}' = (1^{m_1}, 2^{m_2}, \ldots, N^{m_N})$

$\mathbf{T}[\boldsymbol{\Omega}'|\boldsymbol{\Omega}]$: $N \times N$-matrix with elements from $\mathbf{T}$ with row and column indices $\boldsymbol{\Omega}'$, $\boldsymbol{\Omega}$

S. Scheel, *quant-ph/0406127*; S. Scheel and S.Y. Buhmann, Acta Phys. Slovaca **58**, 675–810 (2008).

Quantum optics of macroscopic systems

Permanents in linear optics

unitary transformation of N-mode Fock state with total n photons

$$\hat{U}|n_1,\ldots,n_N\rangle = \left(\prod_i n_i!\right)^{-1/2} \sum_{\omega\in G_{n,N}} \frac{1}{\mu(\omega)} \operatorname{per}\mathbf{T}[\omega|\boldsymbol{\Omega}]|m_1(\omega),\ldots,m_N(\omega)\rangle$$

$m_i(\boldsymbol{\omega})$: multiplicities of occurence of index i in non-increasing integer sequence $\boldsymbol{\omega}$

$$\mu(\boldsymbol{\omega}) = \prod_i m_i(\boldsymbol{\omega})!$$

$\operatorname{per}\mathbf{T} = \sum_{\sigma\in S_n}\prod_i^n T_{i\sigma_i}$ matrix permanent of $\mathbf{T}$, S_n: (symmetric) group of permutations

immediate consequence: $\operatorname{per}\mathbf{T} = \langle 1,1,\ldots,1|\hat{U}|1,1,\ldots,1\rangle$

e.g. $\langle 1,1|\hat{U}|1,1\rangle = \operatorname{per}\mathbf{T} = T_{11}T_{22}+T_{12}T_{21} = |T|^2-|R|^2$

S. Scheel, *quant-ph/0406127*; S. Scheel and S.Y. Buhmann, Acta Phys. Slovaca **58**, 675–810 (2008).

Permanents in linear optics

unitary transformation of N-mode Fock state with total n photons

$$\hat{U}|n_1,\ldots,n_N\rangle = \left(\prod_i n_i!\right)^{-1/2} \sum_{\omega\in G_{n,N}} \frac{1}{\mu(\omega)} \operatorname{per}\mathbf{T}[\omega|\Omega]|m_1(\omega),\ldots,m_N(\omega)\rangle$$

$m_i(\omega)$: multiplicities of occurence of index i in non-increasing integer sequence ω

$\mu(\omega) = \prod_i m_i(\omega)!$

$\operatorname{per}\mathbf{T} = \sum_{\sigma\in S_n} \prod_i^n T_{i\sigma_i}$ matrix permanent of $\mathbf{T}$, S_n: (symmetric) group of permutations

immediate consequence: $\operatorname{per}\mathbf{T} = \langle 1,1,\ldots,1|\hat{U}|1,1,\ldots,1\rangle$

e.g. $\langle 1,1|\hat{U}|1,1\rangle = \operatorname{per}\mathbf{T} = T_{11}T_{22} + T_{12}T_{21} = |T|^2 - |R|^2$

S. Scheel, *quant-ph/0406127*; S. Scheel and S.Y. Buhmann, Acta Phys. Slovaca **58**, 675–810 (2008).

Complexity of computing matrix permanents

What is a permanent anyway, and why is it so special?

matrix determinant: $\det \mathbf{M} = \sum_{\sigma \in S_n} (-1)^{\chi(\sigma)} \prod_i^n M_{i\sigma_i}$

- has its roots in linear algebra
- volume of parallelepiped spanned by the column vectors of $\mathbf{M}$
- only defined for square matrices
- similarity (principal axes) transformation $\mapsto$ diagonal form
- computational demand: $\mathcal{O}(n^3)$ for LU/QR/Cholesky decomposition

Complexity of computing matrix permanents

What is a permanent anyway, and why is it so special?

matrix permanent: $\det \mathbf{M} = \sum_{\sigma \in S_n} \prod_{i}^{n} M_{i\sigma_i}$

- has its roots in combinatorics and graph theory
- # permutations with restricted positions, weights of perfect matchings of a graph
- also defined for rectangular matrices
- only invariant under permutations
- computational demand: $\mathcal{O}(n2^n)$ for exact computation

Complexity of computing matrix permanents

Theorem (Valiant)

The complexity of computing the permanent of $n \times n(0, 1)$-matrices is NP-hard and, in fact, of at least as great difficulty (to within a polynomial factor) as that of counting the number of accepting computations of any nondeterministic polynomial time Turing machine.

consequences:

- computing permanents is really hard (#P-complete, i.e. not possible in polynomial time)
- designing linear-optical networks for a specific task requires computing the permanent of the network $\Rightarrow$ designing LOQC is itself hard

L.G. Valiant, Theor. Comp. Science **8**, 189 (1979).

Complexity of computing matrix permanents

approximations to permanents:

- Jerrum, Sinclair, and Vigoda: matrix elements nonnegative: approximations to $\mathrm{per}\,\mathbf{M}$ can be made in probabilistic polynomial time
- matrix elements complex: even approximating $\mathrm{per}\,\mathbf{M}$ to within a constant factor is #P-complete!

M. Jerrum, A. Sinclair, and E. Vigoda, J. ACM **51**, 671 (2010).

Boson sampling model

Extended Church–Turing Thesis: all computational problems that are efficiently solvable by realistic physical device, are solvable by a probabilistic Turing machine.

Shor: Predicting the (probabilistic) results of a given quantum-mechanical experiment, to finite accuracy, cannot be done by a classical computer in probabilistic polynomial time, unless factoring integers can as well.

Shor's argument is only valid if factoring is classically hard (not known)!

Does one need a fully fledged universal quantum computer to disprove Extended Church–Turing Thesis? Aaronson and Arkhipov: no, linear optics is enough!

$\Rightarrow$ quantum computation with noninteracting bosons (boson sampling)

S. Aaronson and A. Arkhipov, *The computational complexity of linear optics*, Theory of Computing **9**, 143–252 (2013).

Boson sampling model

Extended Church–Turing Thesis: all computational problems that are efficiently solvable by realistic physical device, are solvable by a probabilistic Turing machine.

Shor: Predicting the (probabilistic) results of a given quantum-mechanical experiment, to finite accuracy, cannot be done by a classical computer in probabilistic polynomial time, unless factoring integers can as well.

Shor's argument is only valid if factoring is classically hard (not known)!

Does one need a fully fledged universal quantum computer to disprove Extended Church–Turing Thesis? Aaronson and Arkhipov: no, linear optics is enough!

$\Rightarrow$ quantum computation with noninteracting bosons (boson sampling)

S. Aaronson and A. Arkhipov, *The computational complexity of linear optics*, Theory of Computing **9**, 143–252 (2013).

Boson sampling model

Extended Church–Turing Thesis: all computational problems that are efficiently solvable by realistic physical device, are solvable by a probabilistic Turing machine.

Shor: Predicting the (probabilistic) results of a given quantum-mechanical experiment, to finite accuracy, cannot be done by a classical computer in probabilistic polynomial time, unless factoring integers can as well.

Shor's argument is only valid if factoring is classically hard (not known)!

Does one need a fully fledged universal quantum computer to disprove Extended Church–Turing Thesis? Aaronson and Arkhipov: no, linear optics is enough!

$\Rightarrow$ quantum computation with noninteracting bosons (boson sampling)

S. Aaronson and A. Arkhipov, *The computational complexity of linear optics*, Theory of Computing **9**, 143–252 (2013).

Boson sampling model

Extended Church–Turing Thesis: all computational problems that are efficiently solvable by realistic physical device, are solvable by a probabilistic Turing machine.

Shor: Predicting the (probabilistic) results of a given quantum-mechanical experiment, to finite accuracy, cannot be done by a classical computer in probabilistic polynomial time, unless factoring integers can as well.

Shor's argument is only valid if factoring is classically hard (not known)!

Does one need a fully fledged universal quantum computer to disprove Extended Church–Turing Thesis? Aaronson and Arkhipov: no, linear optics is enough!

$\Rightarrow$ quantum computation with noninteracting bosons (boson sampling)

S. Aaronson and A. Arkhipov, *The computational complexity of linear optics*, Theory of Computing **9**, 143–252 (2013).

Boson sampling model

Extended Church–Turing Thesis: all computational problems that are efficiently solvable by realistic physical device, are solvable by a probabilistic Turing machine.

Shor: Predicting the (probabilistic) results of a given quantum-mechanical experiment, to finite accuracy, cannot be done by a classical computer in probabilistic polynomial time, unless factoring integers can as well.

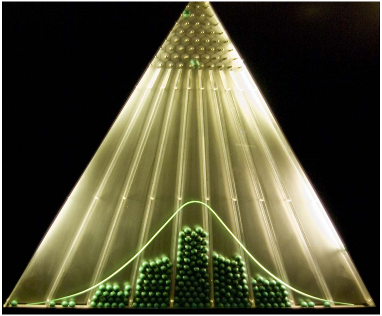
Shor's argument is only valid if factoring is classically hard (not known)!

Does one need a fully fledged universal quantum computer to disprove Extended Church–Turing Thesis? Aaronson and Arkhipov: no, linear optics is enough!

$\Rightarrow$ quantum computation with noninteracting bosons (boson sampling)

S. Aaronson and A. Arkhipov, *The computational complexity of linear optics*, Theory of Computing **9**, 143–252 (2013).

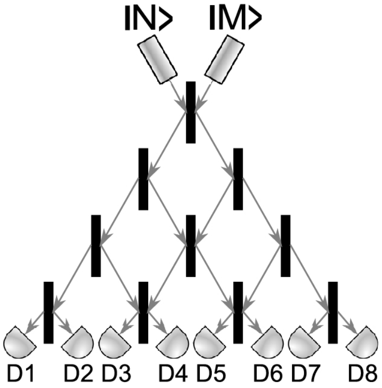
Boson sampling model



- Galton board: 'computer' to generate samples from a binomial distribution
- uses classical particles
- 'input': exact arrangement A of pegs
- 'output': number of balls that have landed in each bin (sample from the joint distribution $\mathcal{D}_A$ over these numbers)

S. Aaronson and A. Arkhipov, *The computational complexity of linear optics*, Theory of Computing **9**, 143–252 (2013).

Boson sampling model



- 'quantum quincunx' (boson sampler): 'computer' to generate samples from a distribution involving permanents
- uses photons
- 'input': beam splitter array **T**
- 'output': distribution of photon numbers across the bins

S. Aaronson and A. Arkhipov, *The computational complexity of linear optics*, Theory of Computing **9**, 143–252 (2013).

Boson sampling model

Theorem (Aaronson and Arkhipov)

The exact boson sampling problem is not efficiently solvable by a classical computer, unless $P^{\#P} = BPP^{NP}$ and the polynomial hierarchy collapses to the third level.

further: even approximating the probability of some particular basis state when a boson computer is measured to within a multiplicative constant is a $\#P$-hard problem.

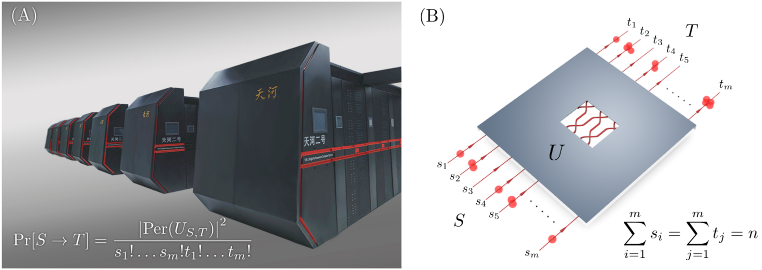
$\Rightarrow$ sampling from a permanent distribution is hard

$\Rightarrow$ although boson sampling does not constitute universal quantum computing, it represents an intermediate computational model that shows quantum supremacy

experimental realization $\Rightarrow$ see next lecture!

S. Aaronson and A. Arkhipov, *The computational complexity of linear optics*, Theory of Computing **9**, 143–252 (2013).

Boson sampling model



world record (as of 2016): computation of permanent of a (48×48)-matrix on then world's fastest supercomputer Tianhe-2 in $\approx$4500s

J. Wu *et al.*, arXiv:1606.05836.

Quantum optics of macroscopic systems

Take-home messages

- probability distribution of obtaining certain combination of photon number patterns at the output of a linear optical network is given by matrix permanents
- permanents are matrix invariants associated with symmetric tensor products of Hilbert spaces
- permanents naturally occur in combinatorics and graph theory in counting problems, not in linear algebra
- computing permanents is computationally hard
- linear-optical networks (boson sampling) provide intermediate computational model for quantum computing without being universal
- experimentally realizable (in contrast to a universal quantum computer)