Boson Sampling

Zichen He

In this note, we mainly discussed Boson sampling which is a restricted model of non-universal quantum computation introduced by Scott Aaronson and Alex Arkhipov. We introduced setup of the model including identical photons and a linear-optical network. We indicated how permanent is related to the output of the model. We did not show why there is no efficient classical algorithm that samples from the same probability distribution as a linear-optical network.

BACKGROUND

One motivation to invest time and money on quantum computation is that there might be proved quantum advantage, which means quantum computer can solve problems that classical computer cannot solve efficiently. There is one famous quantum algorithm called Shor's algorithm. Shor proved that people can factor an integer in polynomial time on a quantum computer. It might be a quantum advantage if people can prove integer factorization is not a P problem and people did not find such an algorithm yet. Unfortunately, Shor's algorithm needs to be run on a universal quantum computer, which is well beyond current technology. What experiment can we do currently to show some quantum advantage? Scott Aaronson presented a model that may work at era of noisy intermediate-scale quantum (NISQ).

BOSON SAMPLING

The model involves a quantum system of n identical photons and m modes, where $m \geq n$. We can place photons in any mode. Let s_i represent the number of photons in the ith mode and $\sum_i^m s_i = n$. During the computation, photons are never created or annihilated, so the system has the basis $\{|s_i, \ldots, s_m\rangle | s_i \geq 0, \sum_{i=1}^m = n\}$. One can easily check the system has dimension $M = \binom{m+n-1}{n}$. Then the general state of the system has the form

$$|\psi\rangle = \sum_{S \in \Psi_{m,n}} \alpha_S |S\rangle$$

where $\Psi_{m,n}$ is the set of labels on the basis states. Assume our computer or system starts in the standard initial state $|1_n\rangle := |1, \ldots, 1, 0, \ldots, 0\rangle$ where the first n nodes contain one photon each.

This system is different from a standard quantum computer, so which unitary transformations can we perform on the states? In the linear optics model, any unitary transformation on m modes can be decomposed into a product of optical elements, each of which acts nontrivially on at most two modes. The two best-known optical elements are called phaseshifters and beamsplitters. It is easy to understand their behavious on single photon: phaseshifter multiplies a single amplitude by $e^{i\theta}$, and beamsplitter modifies two amplitudes for some specified angle. By Reck's theorem, any unitary transformation could be decomposed into a product of such two optical elements. Furthermore, the decomposition has size $O(m^2)$. Note that even if we can make universal quantum gates, Boson sampling is not believed to be universal. It is because that in boson sampling only a single measurement is allowed, a measurement of all the modes at the end of the computation. The model doesn't allow adaptive measurements for example projective measurements, so it cannot efficiently involve ancilla resources, implement quantum teleportations or error corrections.

How do we describe the action of the optical element on multiple photons? Phaseshifting is easily generalized to be like:

$$|s_1, \ldots, s_m\rangle \to e^{i\theta s_i} |s_1, \ldots, s_m\rangle$$

For beamsplitter, it is not very obvious. There is a natural homomorphism φ, which maps an $m \times m$ unitary transformation U to the corresponding $M \times M$ unitary matrix, where $\varphi(U)$ acts on n photons. Then we can write

$$\varphi(U) = \varphi(U_T \ldots U_1) = \varphi(U_T) \ldots \varphi(U_1)$$

where U_t is an optical element. Physically, the linear interferometer described by U performs a linear transformation of the creation operators $a_i^\dagger$ of the circuit's input modes:

$$b_j^\dagger = \sum_{i=1}^N U_{ji} a_i^\dagger$$

When U is a 2×2 matrix with matrix elements a, b, c, d, by definition and a lot of calculation

$$\langle s, t | \varphi(U) | u, v \rangle = \begin{cases} 0 & s + t \neq u + v \\ \sqrt{\frac{u!v!}{s!t!}} \sum \binom{s}{k} \binom{t}{l} a^k b^{s-k} c^l d^{t-l} & \text{else} \end{cases}$$

where u, v and s, t represent the number of photons at two modes. Even if we can write down $\varphi(U)$ explicitly, it is not obvious that $\varphi(U)$ is unitary. There is a beautiful alternative interpretation by multivariant polynomials.

Substitute creation operators by formal variables ($b_j^\dagger = x'_j$, $a_i^\dagger = x_i$):

$$\begin{bmatrix} x'_1 \\ \vdots \\ x'_m \end{bmatrix} = \begin{bmatrix} u_{11} & \dots & u_{1m} \\ \vdots & & \vdots \\ u_{m1} & \dots & u_{mm} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix}$$

For any initial state with n photons, we represent it by the sum of n-monomials. For example, the standard initial state $|1_n\rangle$ corresponds to the degree n-monomial $J_{m,n}(x_1, \dots, x_m) = x_1 \dots x_n$. To transform the standard initial state, we apply the unitary matrix U to the vector x_i's. The new state represented by a polynomial (actually is also monomial) looks like

$$p(x_1, \dots, x_m) = J_{m,n}(x'_1, \dots, x'_m) = \prod_{i=1}^{n} (u_{i1}x_1 + \dots + u_{im}x_m)$$

Rewrite $p(x_1, \dots, x_m)$ as a linear combination of monomials with degree n

$$p(x_1, \dots, x_m) = \sum a_S x_1^{s_1} \dots x_m^{s_m}$$

where $\sum s_i = n$. Define Fock-space inner product

$$\langle p, q \rangle = \sum_S \bar{a_S} b_S s_1! \dots s_m!$$

This inner product can be also interpretated as the expectation of a Gaussian distribution. By the rotation invariance of the Gaussian distribution, the transformation U is unitary under such inner product. Next, we define an isomorhpism from any general state $|\psi\rangle = \sum \alpha_S |S\rangle$ to a polynomial $P_{|\psi\rangle} = \sum \frac{\alpha_S x^S}{\sqrt{s_1! \dots s_m!}}$. The isomorphism preserves the inner product and commutes with any unitary transformation:

$$\begin{array}{ccc} |\psi\rangle & \xrightarrow{\varphi(U)} & \varphi(U)|\psi\rangle \\ \downarrow & & \downarrow \\ P_{|\psi\rangle} & \xrightarrow{U} & UP_{|\psi\rangle} \end{array}$$

What we can conclude from this commutative diagram is

- $\varphi(U)$ is unitary
- $a_S \sqrt{s_1! \dots s_m!} = \alpha_S$ where a_S is the coefficient in the polynomial and α_S is the amplitude of a quantum state.

It seems that we have linked the coefficients of some polynomials with probability of some output states under the model.

HARDNESS OF COMPUTING PERMANENT

Given an $m \times m$ matrix V, the permanent is

$$\mathrm{Per}(V) = \sum_{\sigma \in S_m} \prod_{i=1}^{m} v_{i,\sigma(i)}$$

let $V_{n,n}$ be the top-left $n \times n$ submatrix of V. By definition,

$$V[J_{m,n}] = \prod_{i=1}^{n} (v_{i1}x_1 + \dots + v_{im}x_m)$$

Then $\langle J_{m,n}, V[J_{m,n}] \rangle$ is just the coefficient of $J_{m,n} = x_1 \dots x_n$ in the above polynomial. This coefficient can be calculated as

$$\sum_{\sigma \in S_n} \prod_{i=1}^{n} v_{i,\sigma(i)} = \mathrm{Per}(V_{n,n})$$

Hence for any V,

$$\mathrm{Per}(V_{n,n}) = \langle J_{m,n}, V[J_{m,n}] \rangle = \langle 1_n | \varphi(V) | 1_n \rangle$$

More generally, for any basis states $S, T \in \Psi_{m,n}$,

$$\mathrm{Per}(U_{S,T}) = \langle S | \varphi(U) | T \rangle \sqrt{s_1! \dots s_m! t_1! \dots t_m!}$$

Note if s_i and t_j are all zeros or ones, $U_{S,T}$ is just a $n \times n$ submatrix of U; otherwise, $U_{S,T}$ is like a submatrix of U but with repeated rows or columns. Therefore, to find the permanent of a $n \times n$ submatrix of V, we could repeat running the model and the model has depth $O(m^2)$ by previous argument. If we fix the error bound to be ϵ, Gurvits showed that the probability of measuring a particular basis state can be estimated to within ϵ error in $\mathrm{poly}(n, 1/\epsilon)$ time.

In contrast with computing determinant which is tractable because of Gauss elimination, exactly computing permanent or just approximating permanent of a $n \times n$ matrix is #P-hard. The main result of this paper [1] is that

- The exact BosonSampling problem is not efficiently solvable by a classical computer, otherwise it will cause some problems in complexity theory.
- Approximating BosonSampling is not efficiently solvable by a classical computer, otherwise it will cause some problems in complexity theory.

Therefore, Boson sampling might be a quantum advantage theoretically.

EXPERIMENTS

People never gave up showing quantum advantage by noisy intermediate-scale quantum machine. At 2019, Google claimed quantum supremacy using a programmable superconducting processor [2]. At 2020, USTC claimed quantum computational advantage using photons [3] (Gaussian boson sampling). Both are time dependent, because the competition between classical computers and quantum computers is not over yet.

[1] S. Aaronson and A. Arkhipov, "The Computational Complexity of Linear Optics," 2010. 2

[2] "Quantum Supremacy using a Programmable Superconducting Processor," *Nature* **574** (2019) 505–510. 3

[3] "Quantum computational advantage using photons," *Science* **370** (2020), no. 6523 1460–1463. 3