

Origin of Quantum Supremacy, the Hafnian Master Theorem and Atomic Boson Sampling

V V KOCHAROVSKY¹

¹*Department of Physics and Astronomy, Texas A&M University, College Station TX, USA*
Contact Email: vitya.kocharovsky@gmail.com

We present the recently found Hafnian Master Theorem (1), Fig. 1 [1]. The theorem discloses an easy-to-compute generating function for hafnians (which are $\#P$ -hard for computing) and, for any symmetric $2m \times 2m$ matrix S , states the following formula:

$$\frac{1}{\sqrt{\det(I - ZPS)}} = \sum_{\{n_k\}} \text{haf} \tilde{S}(\{n_k\}) \prod_{k=1}^m \frac{z_k^{n_k}}{n_k!}, \quad (1)$$

where $Z = \text{diag}\{z_k, z_k | k = 1, \dots, m\}$, P is a direct sum of σ_x Pauli matrices. The famous Permanent Master Theorem, found by MacMahon in 1916, is its particular case and applies only to permanents.

The Hafnian Master Theorem proves quantum supremacy of atomic boson sampling in a BEC trap that we recently suggested [2] as an alternative to the well-known Gaussian boson sampling in an optical interferometer. Both boson samplings are interesting for demonstrating quantum supremacy of quantum simulators over classical computers. Just one extra step has to be done for pioneering such an atomic boson sampling experiment as compared to the recent successful experiment [3] on measuring statistics of the total noncondensate occupation calculated in [4]. It is to split the noncondensed atoms into a few separate groups, each combining a subset of excited states, and perform simultaneous measurement of their occupations. The characteristic function and joint excited-state occupation probabilities are given, basically, by the left and right hand sides of Eq. (1).

The Hafnian Master Theorem explains the origin of quantum supremacy in many-body quantum systems. Despite a paradigm stating that a function and its Fourier transform contain the same information, it is clear that the $\#P$ -hardness appears due to a multiple Fourier integration. The point is that the information encrypted in the probability of occurrence of just one set of the occupation numbers $\{n_k\}$ corresponds to the information encrypted in the values of the characteristic function at an exponentially large (with respect to $n = \sum_k n_k$) number of points, that is, an exponentially large subset of points in the space of Fourier variables $\{z_k\}$.

The Hafnian Master Theorem provides a pathway to a unified analysis of the nature's $\#P$ -hard problems, including problems in quantum computing, computer science, theory of computational complexity, combinatorics, statistics, cryptography, theory of graphs, number theory, physics of many-body systems, critical phenomena, quantum field theory, *etc.* [2,5]

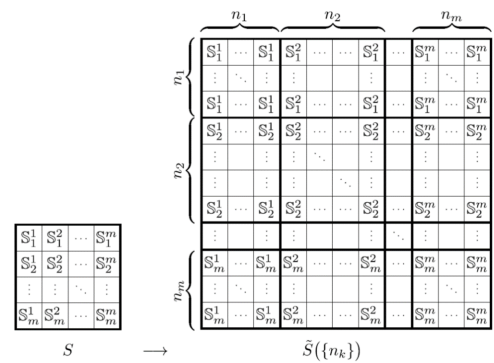


Figure 1: A block structure of the $(2 \sum_k n_k) \times (2 \sum_{k'} n_{k'})$ matrix $\tilde{S}(\{n_k\})$ built from the matrix S for a given m -tuple $\{n_k | k = 1, \dots, m\}$. The integer n_k is the number of degenerate (2×2) -block rows and the equal number of degenerate (2×2) -block columns placed into the matrix $\tilde{S}(\{n_k\})$ instead of the S -matrix's k -th (2×2) -block row and k -th (2×2) -block column, respectively. A block $S_k^{k'} = (s_{r,k}^{r',k'})$, sitting at the intersection of the k -th (2×2) -block row and k' -th (2×2) -block column, is the 2×2 matrix with the entries $s_{r,k}^{r',k'}$ enumerated by the intra-block indexes $r = 1, 2$ (for rows) and $r' = 1, 2$ (for columns)

References

- [1] V V Kocharovsky, V I V Kocharovsky and S V Tarasov, *Linear Algebra Appl.* **651**, 144 (2022)

- [2] V V Kocharovsky, VI V Kocharovsky and S V Tarasov, arXiv:2201.00427v2 (2022)
- [3] M A Kristensen, M B Christensen, M Gajdacz, M Iglicki, K Pawłowski, C Klempt, J F Sherson, K Rzażewski, A J Hilliard and J J Arlt, Phys. Rev. Lett. **122**, 163601 (2019)
- [4] S V Tarasov, VI V Kocharovsky and V V Kocharovsky, Phys. Rev. A **102**, 043315 (2020)
- [5] V V Kocharovsky, VI V Kocharovsky and S V Tarasov, Entropy **22**, 322 (2020)