Contribution ID: **54** Type: **Oral Presentation**

Simulation of Shor's algorithm on a tensor network-based quantum emulator

Shor's algorithm is a major milestone in the race to quantum supremacy which proposes to factorize semiprimes in time polynomial to the length of the binary string representation of the number. However, its practical implementation is limited due to several constraints in modern-day quantum hardware. Moreover, studies benchmarking the Shor's algorithm on quantum simulators are relatively few, focusing mostly on the success probability of factorization as the sole metric and statevector simulations as the primary technique. Our work presents a comprehensive study of the algorithm on a tensor network powered quantum simulator. In addition to the success probability, we also analyze the probability distribution of the sampled bitstring using different sampling strategies, quantify and evaluate the entanglement generated in the modular exponentiation circuit and examine the significance of so called 'lucky runs', cases where the number is factorized correctly even though the theoretical conditions are not completely met.

Several advancements have been made to allow for better scaling of Shor's algorithm. Some algorithms focus on reducing the number of qubits required to implement the quantum circuit [1, 2], others use specific optimization techniques to reduce the circuit depth and complexity [3, 4] while some others use methods like GPU accelerators and parallelization techniques [5, 6]. Building on the existing literature, we leverage the power of tensor networks to simulate larger instances as well as benchmark various aspects of its performance on our emulator.

We perform matrix product state (MPS) simulations of the Shor's algorithm based on the modular exponentiation quantum circuit proposed by Vedral, Barenco and Ekert [7]. This choice is driven by the fact that the scalability of the simulation is now dependent on the maximum bond dimension of the MPS and not on the number of qubits as for statevector simulations. Crucially, the bond dimension also allows systematic control over simulation fidelity and accumulated errors which is usually very difficult to do in noisy quantum hardware. The simulations are averaged over multiple semiprimes with the same bit length to minimize statistical errors. We compute the success probability across varying bond dimensions and numbers with increasing bit length, while also profiling simulation time, circuit preprocessing/optimization time, and time for post-processing steps such as bitstring sampling and extraction of prime factors. To demonstrate that our results are trustworthy and credible, we implement a fidelity estimate for all simulations and also compare with exact (statevector) simulations for the smallest semi-prime.

Further, two different sampling methods are used to obtain the bitstring representing the final state and an evaluation is made on their probability distribution and how it varies with the bond dimension. We also give attention to distinguishing between "true"runs, where the correct order and factors are obtained and "lucky" runs where incorrect orders still lead to valid factorizations.

We benchmark our simulations on Quantum Matcha Tea, a logical quantum computer emulator fueled by MPS and Tree Tensor Networks (TTNs). We benchmark how the success probability scales with increasing bond dimension and how the underlying probability distribution obtained through sampling influences this quantity. Further, we use the Kullback–Leibler (KL) divergence to measure how accurate our obtained distribution is to the ideal output distribution as discussed in [8] and analyze the distribution of the bitstrings that are able to correctly determine the order of the modular exponentiation function. We further attempt to examine if a lower bound for the success probability depending on the bond dimension of the MPS can be determined. Finally, we also discuss potential improvements and future directions.

References:

1. S. Beauregard, arXiv preprint quant-ph/0205095 (2003).
2. A.G. Fowler et al, Quantum Info. Comput. 4, 237 (2004).
3. X. Liu et al, Security and Communication Networks, 2023, 2963110 (2023).
4. H.T. Larasati et al, IEEE Access, vol. 11, pp. 54910-54927 (2023).
5. X.J. Tan and P. Gao, AIP Advances, 14(2) (2024).
6. C. Zalka, arXiv preprint quant- ph/9806084 (1998).
7. V. Vedral et al, Physical Review A, 54(1):147–153 (1996).
8. A. Dang et al, Quantum 3, 116 (2019).

Author: Ms DATTA, Asmita (University of Padova)

Co-authors: Dr BACCARI, Flavio (University of Padova); Dr SILOI, Ilaria (University of Padova); Prof. MONTANGERO, Simone (University of Padova)

Presenter: Ms DATTA, Asmita (University of Padova)

Session Classification: B - Contributed Talk