Contribution ID: **18** Type: **not specified**

Design of a Quantum Walk Circuit to Solve the Subset-sum Problem

Thursday, 12 September 2024 15:50 (15 minutes)

Search algorithms based on quantum walks have emerged as a promising method for addressing computational problems across various domains, including combinatorial optimization and cryptography. Indeed, quantum walks have been proven to provide a theoretical quadratic speedup in search algorithms compared to the classical paradigm of computation. Additionally, recent literature shows reduced computational complexity relative to the widely-used and generic Grover-based quantum search algorithm when it is used to solve specific problems such as element distinctness, information set decoding, and claw finding.

In this work, we present a complete implementation of a quantum walk search to solve the subset-sum problem. By modeling the domain space as nodes of a Johnson graph, we enhanced the efficiency of the solver with respect to existing theoretical quantum proposals. Our analysis assumes a fault-tolerant quantum computation regime, setting aside discussions of noise correction and hardware architectures for future research. We derive closed-form complexity metrics in terms of the number of quantum gates, number of qubits, and the depth of the quantum circuit. Unlike state-of-the-art theoretical approaches, our proposal does not rely on an exponentially-sized QRAM, but only requires a polynomial amount of qubits. We also express the complexity metrics of our circuits using the Clifford+T gate set, widely regarded as the most promising for fault-tolerant quantum computation. Our implementation is compared with a Grover-based search approach, demonstrating improvements in both depth and depth-times-number of qubits metrics across a range of problem sizes, from practically solvable subset-sum instances to those large enough for constructing post-quantum cryptosystems.

The proposed design serves as a building block for efficient quantum search algorithms modeled on Johnson graphs, bridging the gap between existing theoretical complexity analyses and providing finite-regime complexity measures.

Title

Author

Primary author: PERRIELLO, Simone (Politecnico di Milano)

Presenter: PERRIELLO, Simone (Politecnico di Milano)