Quantum binary quadratic form reduction

A $n^2 \log n$ depth circuit and application to lattice reduction

Nicolas David[†] and Thomas Espitau and Akinori Hosoyamada

[†] Inria Paris, NTT Corporation, Tokyō, Japan

Quantum computing appears to be very promising due to its applications to different paradigms among several domains of computer science such as number theory, encryption, search, information theory and more [1] [2] [3], proposing exponential speedup on some specific search tasks. Among these breakthroughs in terms of complexity, the design of efficient quantum circuits for more low level tasks, such as basic integer operations (e.g. addition [4], multiplication [5] and division [6]) is a current active domain of research. Based on these base circuits, more complex designs have been made such as quantum circuit for GCD [7]. Our goal is to design an effective quantum circuit for reducing quadratic forms. If reducing quadratic forms is important in itself, its application to cryptanalysis is also of the utmost important since it gives the first step to the design of a quantum version of the celebrated lattice reduction algorithm LLL. This latter algorithm is crucially used in cryptanalysis and in particular in the security assessment of lattice-based cryptography.

Contributions. In this work, the first description of quantum circuits tackling the following problems are proposed:

Computing logarithm's floor of integer in base 2 We give here an optimized shallow circuit to perform this computation, using labeling of a binary tree. Roughly speaking, the leaves will correspond to the values of the bit representation of the input integer and each level of the tree will transmit the information of the size of its children, using a quantum subcircuit for node computation. All in all this gives a $\log n$-deep, n-wide circuit, where the naive approach (seeking for the left-most 0 in the representation) would give a n-deep circuit.

Computing scalar multiplication by a power 2 We propose an optimized shallow circuit for bit rotation (multiplication by a *variable* power of 2) of depth $\log n$ and width $n \log n$ and size $n \log n$. Our technique relies on the shallow circuit of a rotation by one bit (á la Moore and Nilsson [7]) and combining them with parallel control and fine-grained management of the ancilae.

Reducing definite quadratic forms Our main circuit is built on a novel generalization of Gauss's reduction, loosely using the binary design of Stein's *Binary Algorithm* [8]. In the same way this algorithm is practically faster than the Euclidean algorithm by saving bit operations, our quadratic form reduction will outperform Gauss algorithms. Using this new (classical) design with the subcircuits introduced above, we give a $n \log n$-deep, n^2-wide, $n^2 \log n$-size circuit.

References

1. D Mermin. Breaking rsa encryption with a quantum computer: Shor's factoring algorithm. *Lecture notes on Quantum computation*, pages 481–681, 2006.
2. Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996.
3. Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *arXiv preprint arXiv:2003.06557*, 2020.
4. Yasuhiro Takahashi and Noboru Kunihiro. A fast quantum circuit for addition with few qubits. *Quantum Information & Computation*, 8(6):636–649, 2008.
5. Luis Antonio Brasil Kowada, Renato Portugal, and Celina M. H. de Figueiredo. Reversible karatsuba's algorithm. *J. Univers. Comput. Sci.*, 12(5):499–511, 2006.
6. Himanshu Thapliyal, Edgard Muñoz-Coreas, T. S. S. Varun, and Travis S. Humble. Quantum circuit designs of integer division optimizing t-count and t-depth. *IEEE Trans. Emerg. Top. Comput.*, 9(2):1045–1056, 2021.
7. Mehdi Saeedi and Igor L Markov. Quantum Circuits for GCD Computation with $n/logn$ Depth and n Ancillae. *arXiv preprint arXiv:1304.7516*, 2013.
8. Josef Stein. Computational problems associated with racah algebra. *Journal of Computational Physics*, 1(3):397–405, 1967.