Limitations on Transversal Computation through Quantum Homomorphic Encryption*

Michael Newman[1] and Yaoyun Shi[2]

[1]Department of Mathematics
[2]Department of Electrical Engineering and Computer Science
University of Michigan, Ann Arbor, MI 48109, USA
mgnewman@umich.edu, shiyy@umich.edu

Abstract

Transversality is a simple and effective method for implementing quantum computation fault-tolerantly. However, no quantum error-correcting code (QECC) can transversally implement a quantum universal gate set (Eastin and Knill, *Phys. Rev. Lett.*, 102, 110502). Since reversible classical computation is often a dominating part of useful quantum computation, whether or not it can be implemented transversally is an important open problem. We show that, other than a small set of non-additive codes that we cannot rule out, no binary QECC can transversally implement a classical reversible universal gate set. In particular, no such QECC can implement the Toffoli gate transversally.

We prove our result by constructing an information theoretically secure (but inefficient) quantum homomorphic encryption (ITS-QHE) scheme inspired by Ouyang *et al.* (arXiv:1508.00938). Homomorphic encryption allows the implementation of certain functions directly on encrypted data, i.e. homomorphically. Our scheme builds on almost any QECC, and implements that code's transversal gate set homomorphically. We observe a restriction imposed by Nayak's bound (*FOCS* 1999) on ITS-QHE, implying that any ITS quantum *fully* homomorphic scheme (ITS-QFHE) implementing the full set of classical reversible functions must be highly inefficient. While our scheme incurs exponential overhead, any such QECC implementing Toffoli transversally would still violate this lower bound through our scheme.

*Full paper available at https://arxiv.org/abs/1704.07798.