CS269Q Project Progress Report

Yousef Hindy and Pieter-Jan Stas

May 2019

1 What we have achieved so far

We have managed to implement a (3,5) quantum secret sharing scheme in pyQuil. We have done this following directions from R. Laflamme et al's [1] paper and H. Lu et al's paper [2]. H. Lu's paper references R. Laflamme's paper for the qubit encoding scheme, but unfortunately, we encountered quite some errors in the paper and had to rederive the correcting code for it to work properly. The basic idea is that we entangled the five qubits so that when you discard any two, you are left with a superposition over bell states that contains the information of the original state. By applying the transformations (Hadamards and then a Bell-state measurement), you can figure out what transformation you need to make on the state to get back to the original qubit state. So now we have a code that can perfectly transmit a quantum secret if the receiver has at least 3 out of the 5 encoded qubits. We have our code and example notebook in a github repository.

2 What we plan on doing next

In the next steps we plan on taking, we want to implement other quantum secret sharing schemes with different values of k and n via the polynomial-based algorithm described in Cleve et. al [3]. Ideally, we would be able to implement a scheme that can take any arbitrary values for k and n (subject to the constraints described in the paper), although this goal might be a little ambitious. Once we implement other quantum secret sharing schemes we can also explore how realistically reliable they are in noisy quantum systems.

References

[1] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error correction code," 1996.

[2] H. Lu, Z. Zhang, L.-K. Chen, Z.-D. Li, C. Liu, L. Li, N.-L. Liu, X. Ma, Y.-A. Chen, and J.-W. Pan, "Secret sharing of a quantum state," 2016.

[3] R. Cleve, D. Gottesman, and H.-K. Lo, “How to share a quantum secret,” *Physical Review Letters*, vol. 83, no. 3, p. 648, 1999.