CS 269Q WRITTEN REPORT: QUANTUM SECRET SHARING

KATHARINE WOO (KHWOO98) AND HARRY SHA (HARRY2)

1. Introduction

Sharing secrets is tricky business. For example, Alice solves the P vs. NP problem, but needs time to prepare her solution for the public. However, she also wants a contingency plan if she dies during this time. She wants to share her work with her closest colleagues, Bob and Charlie, but doesn't trust them to not steal and publish her work as their own. Luckily, Alice knows that Bob and Charlie are mortal enemies and would only unite if she dies. Alice desires a secret sharing scheme, an idea developed in classical cryptography to handle these situations.

For our final project, we looked at quantum secret sharing schemes in [1] and [2]. We implemented three schemes, which can be found on our github:
`https://github.com/harrysha1029/cs269-final-project`

In the repository, we have both our implementations and a wiki describing the mathematical background of the three schemes. In the README, there are installation instructions. In addition, there is Jupyter notebook with examples of how to use the functions.

We divide this report into the three schemes. In §2, we discuss the secret sharing scheme from [1] for classical information. In §3, we move on to a secret sharing scheme for quantum information from [1]. Finally in §4, we discuss the multiparty scheme from [2].

2. Sharing classical information

First we establish some notation. We will consider three basis for this protocol: the standard basis, the x basis and the y basis. The x basis has the following basis vectors:

$$|+x\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), |-x\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

These vectors are the eigenvectors of P_X with labeled with their corresponding eigenvalues.

Similarly, the y basis is defined to have basis vectors:

$$|+y\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + i\,|1\rangle\right), |-y\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - i\,|1\rangle\right)$$

These vectors are eigenvectors for P_Y.

Date: May 2019.

2.1. **The protocol.** Alice, Bob and Charlie each have access to one qubit of the following entangled GHZ state

$$|\Psi_0\rangle = \frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle. \tag{1}$$

Alice chooses randomly either the x or y basis to measure in, thus collapsing her state into one of the following: $|+x\rangle, |-x\rangle, |+y\rangle, |-y\rangle$. Her secret is the eigenvalue she measured.

Bob then chooses either the x or y basis and measures and records his state. Charlie does the same. Now, Alice, Bob and Charlie all announce what measurement basis they used and decide to keep or throw away the triplet. This is an important step because Charlie is only guaranteed to measure useful data in 1/2 of the combinations of randomly chosen measurements.

Then using a predetermined table, Bob and Charlie together can determine what Alice's secret is. However, without knowledge of each other's measurements, each outcome is equally likely from Bob and Charlie's perspectives. This prevents Bob or Charlie from determining Alice's secret without each other. For more explanation of this protocol, we refer to `https://github.com/harrysha1029/cs269-final-project/wiki/Hillery_Classical`

2.2. **Future extensions.** We note that since Alice doesn't get to choose her secret, this scheme is more similar to a key exchange, since Alice, Bob and Charlie end up with a shared secret key at the end of the protocol. In addition, security of secret sharing protects this key exchange against passive eavesdroppers.

Future extensions of this protocol would be to extend it to a more general (k, n) secret sharing scheme as defined in §4. We will see a quantum secret sharing scheme for more parties in §4 and [2]. However, since this is sharing classical bits, it perhaps can be generalized cleanly to an arbitrary number of parties. In [1], Hillery et al. generalize this protocol to secret sharing amongst three parties instead of two.

3. Sharing quantum information

3.1. **The protocol.** Let Alice start off with a secret qubit $|\Psi_a\rangle = \alpha|0\rangle + \beta|1\rangle$ that she wants to share with Bob and Charlie. Then using the GHZ triplet from §2 in (1), Alice can create a starting state

$$\begin{aligned}|\Psi_a\rangle \otimes |\Psi_0\rangle = \frac{1}{2\sqrt{2}}\Big(&|\Psi_+\rangle\left(|+x\rangle(\alpha|0\rangle + \beta|1\rangle) + |-x\rangle(\alpha|0\rangle - \beta|1\rangle)\right)\\ &+ |\Psi_-\rangle\left(|+x\rangle(\alpha|0\rangle - \beta|1\rangle) + |-x\rangle(\alpha|0\rangle + \beta|1\rangle)\right)\\ &+ |\Phi_+\rangle\left(|+x\rangle(\beta|0\rangle + \alpha|1\rangle) + |-x\rangle(\beta|0\rangle - \alpha|1\rangle)\right)\\ &+ |\Phi_-\rangle\left(|+x\rangle(-\beta|0\rangle + \alpha|1\rangle) + |-x\rangle(-\beta|0\rangle - \alpha|1\rangle)\right)\Big)\end{aligned}$$

Then, Alice measures her secret qubit, and her GHZ qubit in the Bell basis. Alice does not disclose the result of her measurement to Bob or Charlie. Now, Alice selects one party to measure their qubit in the x direction, in our description, let's assume that Bob measures his bit in the x direction. Alice then sends Charlie the result of her measurement. Then, to recover Alice's secret, Charlie performs a correction to his bit depending on the result of

Alice and Bob's measurement. The correction we need to apply can be easily deduced based on the above representation of the starting state. For example, if Alice measures $|\Phi_+\rangle$, and Bob measures $|+x\rangle$, then Charlie should apply the X gate to recover the secret.

For more explanation of this protocol, we refer to `https://github.com/harrysha1029/cs269-final-project/wiki/Hillery_Quantum`

4. Multiparty secret sharing

First we define a (k, n) secret sharing scheme to be protocol that splits the secret amongst n parties, where any k or more parties together can reconstruct the secret. A famous classical secret sharing scheme is Shamir's secret sharing scheme which uses polynomials over finite fields. In [2], Cleve et al. introduce a similar quantum secret sharing scheme based of off quantum polynomial codes. We first introduce Shamir's secret sharing scheme for comparison.

Let $\mathbb{F}_q$ be a finite field where q is prime. Then it is well known that any k points $(x, y) \in \mathbb{F}_q^2$ that don't contradict each other (ie there is no two points (x, y) and (x, y') where $y \neq y'$) define a polynomial over $\mathbb{F}_q$ of degree $k-1$ up to scalars. Our secret will be some $s \in \mathbb{F}_q$. Then in Shamir's secret sharing scheme, we construct a polynomial $f(t) = a_{k-1}t^{k-1} + a_{k-2}t^{k-2} + ... + a_1 t + s$. Then let the ith share be $(x_i, f(x_i))$ where $x_1, ..., x_n$ are distinct points in $\mathbb{F}_q$.

Now if k parties $\{i_1, ..., i_k\}$ wanted to reconstruct the secret, they need to solve the system of equations:

$$\begin{aligned} a_{k-1}x_{i_1}^{k-1} + a_{k-2}x_{i_1}^{k-2} + ... + a_1 x_{i_1} + s &= y_{i_1} \\ a_{k-1}x_{i_2}^{k-1} + a_{k-2}x_{i_2}^{k-2} + ... + a_1 x_{i_2} + s &= y_{i_2} \\ \vdots \qquad\qquad & \qquad\qquad \vdots \\ a_{k-1}x_{i_k}^{k-1} + a_{k-2}x_{i_k}^{k-2} + ... + a_1 x_{i_k} + s &= y_{i_k} \end{aligned}$$

This is equivalent to solving the following matrix equation

$$\begin{pmatrix} 1 & x_{i_1} & ... & x_{i_1}^{k-1} \\ 1 & x_{i_2} & ... & x_{i_2}^{k-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & x_{i_k} & ... & x_{i_k}^{k-1} \end{pmatrix} \begin{pmatrix} s \\ a_1 \\ \vdots \\ a_{k-1} \end{pmatrix} = \begin{pmatrix} y_{i_1} \\ y_{i_2} \\ \vdots \\ y_{i_k} \end{pmatrix}.$$

The matrix above is called the Vandermonde matrix $V(x_{i_1}, ..., x_{i_k})$ and is invertible as long as $x_{i_1}, ..., x_{i_k}$ are distinct. Thus, $V^{-1}[y_{i_1}, ..., y_{i_k}]^T$ gives a solution to the polynomial coefficients. Hence, the parties can then determine the constant coefficient s.

4.1. The protocol.

In [2], they construct a quantum (k, n) secret sharing scheme. We will use $n = 2k - 1$ because for any smaller n, we can just distribute fewer shares. Now, Alice has some secret

$$|\sigma\rangle = \sum_{i=0}^{\infty} \alpha_i |i\rangle$$

where $\alpha_i = 0$ for all but finitely many i. Let $s = \max\{i : \alpha_i \neq 0\}$. Alice chooses a prime q such that $\max(2k - 1, s) \leq q \leq 2\max(2k - 1, s)$ and publishes it. From now on, we will work in $\mathbb{F}_q$.

Now given some coefficients $\mathbf{c} = (c_0, ..., c_{k-1}) \in \mathbb{F}_q^k$, we define the polynomial $f_{\mathbf{c}}(t) = c_{k-1}t^{k-1} + ... + c_1 t + c_0$. Then we consider the following transformation U:

$$U|i\rangle = \frac{1}{N} \sum_{\substack{\mathbf{c}\in\mathbb{F}_q^k \\ c_{k-1}=i}} |f_{\mathbf{c}}(1), ..., f_{\mathbf{c}}(n)\rangle ,$$

where N is the norm of this sum, q^{k-1}. From now on, we will omit the normalization constant for simplicity of the equation. This resembles the polynomial created in Shamir's scheme except we flip which coefficient is the secret, which makes no difference, and create a superposition of all possible evaluations.

Alice will perform $U|s\rangle$ to create a superposition. She then distributes the n qubits to each party as a share. If k or more parties come together, they can compute the secret. Let these be the first k parties for simplicity. First, they will apply $V(1, ..., k)^{-1}$ to their qubits. This gives them the shared state

$$\sum_{i=0}^{\infty} \alpha_i \sum_{\substack{\mathbf{c}\in\mathbb{F}_q^k \\ c_{k-1}=i}} |c_0, c_1, ..., i\rangle |f_{\mathbf{c}}(k+1), ..., f_{\mathbf{c}}(n)\rangle$$

Applying a cyclical permutation brings the ith state out front to achieve,

$$\sum_{i=0}^{\infty} \alpha_i |i\rangle \sum_{\substack{\mathbf{c}\in\mathbb{F}_q^k \\ c_{k-1}=i}} |c_0, ..., c_{k-2}\rangle |f_{\mathbf{c}}(k+1), ..., f_{\mathbf{c}}(n)\rangle$$

Applying $V(k+1, ..., 2k-1)$ and adding $i \cdot (k+i)^{k-1}$ to register i gives us

$$\left(\sum_{i=0}^{\infty} \alpha_i |i\rangle\right) \otimes \left(\sum_{\mathbf{y}\in\mathbb{F}_q^{k-1}} |y_1, ..., y_{k-1}\rangle |y_1, ..., y_{k-1}\rangle\right)$$

So, the k parties achieve the secret as desired.

This protocol is interesting because it is implementing Shamir's secret sharing scheme in superposition. Instead of choosing a particular random polynomial to evaluate at, it evaluates at all satisfying polynomials.

For more explanation of this protocol, we refer to `https://github.com/harrysha1029/cs269-final-project/wiki/Cleve`

4.2. **Complications.** While implementing this protocol, we ran into difficulties working in $\mathbb{F}_q$. We found that we had to convert each element of $\mathbb{F}_q$ into binary using $\lfloor \log_2(q) \rfloor + 1$ bits. Then for field calculations, we had to convert back and forth.

This process that we ended up implementing to deal with the $\mathbb{F}_q$ and binary conversion was not efficient. In addition, in order to do field calculations such as applying the Vandermonde matrix, we had to apply a conversion between binary and $\mathbb{F}_q$. A future exploration of this project could be to lower the runtime of this process by utilizing superposition of states.

5. Data and Examples

We refer to the Jupyter notebook in `https://github.com/harrysha1029/cs269-final-project/blob/master/Examples.ipynb` for a demonstration of our protocols implemented.

6. Conclusion

We implemented three quantum sharing schemes from [1], [2]. First, Hillery et al.'s scheme for sharing classical bits, which uses properties of quantum computing to be secure against eavesdroppers. Second, Hillery et al.'s secret sharing scheme for quantum bits. Finally, we looked at Cleve et al.'s algorithm for sharing quantum information to any number of parties. We ran into complication while implementing Cleve's algorithm, which works over finite fields rather than standard binary. Hence, an important future direction is to improve the efficiency of these algorithms, especially Cleve's algorithm. Another interesting future direction is to see how classical algorithms, like Shamir's, can inspire quantum algorithms.

Both our project and report can be shared on the course website.

References

[1] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Physical Review A*, vol. 59, no. 3, p. 1829–1834, 1999.

[2] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Physical Review Letters*, vol. 83, no. 3, p. 648–651, 1999.