Quantum Secret Sharing

Abrahim Ladha

November 15, 2019

things quantum computers can do

- Factor integers in $O(n^3)$ compared to $O(\sqrt{p})$ for p the smallest factor
- Database search in $O(\sqrt{N})$ (compared to $O(N)$)
- Solve a linear system in $O(\log(N)\kappa^2)$ (compared to $O(N\kappa)$)

Applications

- Secure Quantum Multiparty Computation
- Quantum Interactive Proofs
- Quantum Oblivious Transfer
- Quantum Bit commitment (is impossible)
- Quantum Key Distribution

review

- $i = \sqrt{-1}$
- $\mathbb{C} = \{a + bi | a, b \in \mathbb{R}\}$
- $\alpha = (a + bi)$, define the complex conjugate as $\alpha^* = a - bi$
- $\alpha = (a + bi), |\alpha| = \sqrt{a^2 + b^2} = \sqrt{(a + bi)(a - bi)} = \sqrt{\alpha^* \alpha}$
- A Unitary matrix U has inverse $U^\dagger$

Brakets

- There exists a vector space V such that $\forall \left|\psi_1\right\rangle, ..., \left|\psi_n\right\rangle \in V$
- For $\alpha_1, ...\alpha_n \in \mathbb{C}$ such that $\sum |\alpha_i|^2 = 1$ then
- $\sum \alpha_i \left|\psi_i\right\rangle \in V$

Brakets

- There exists a vector space V such that $\forall \left|\psi_1\right\rangle, ..., \left|\psi_n\right\rangle \in V$
- For $\alpha_1, ...\alpha_n \in \mathbb{C}$ such that $\sum |\alpha_i|^2 = 1$ then
- $\sum \alpha_i \left|\psi_i\right\rangle \in V$
- $\forall \left|\psi\right\rangle \in V$, there exists $\left\langle\psi\right| \in V_*$ such that $\left\langle\psi\right| := \left|\psi\right\rangle^\dagger = \left|\psi\right\rangle^{*T}$
- Its natural to define the inner product for $\left|\psi\right\rangle, \left|\phi\right\rangle \in V$ as $\langle\phi|\psi\rangle = \left|\phi\right\rangle^\dagger \left|\psi\right\rangle$

Examples

- We define the outer product as $|\phi\rangle \langle\psi| = (M)_{ij} = [\phi_i \psi_j^*]$
- What is $\langle\psi|\psi\rangle$?

Examples

- We define the outer product as $|\phi\rangle \langle\psi| = (M)_{ij} = [\phi_i \psi_j^*]$
- What is $\langle\psi|\psi\rangle$?
- Let $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
- What is $|0\rangle \langle 0| + |1\rangle \langle 1|$?

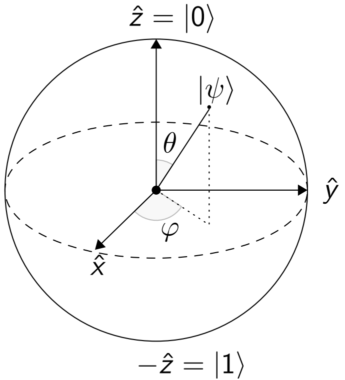
Qubits

- A qubit is a ket in the basis $|0\rangle, |1\rangle$
- $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ such that $|\alpha|^2 + |\beta|^2 = 1$

Qubits

- A qubit is a ket in the basis $|0\rangle, |1\rangle$
- $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ such that $|\alpha|^2 + |\beta|^2 = 1$
- We can tensor product states to form strings
- $|0\rangle \otimes |0\rangle \otimes ... |0\rangle = |00...0\rangle$

Bloch Sphere



$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$$

Operators

- QM tells us the evolution of any *closed* system is linear and unitary.
- If $|\psi\rangle \to |\phi\rangle$, then there exists some U such that $|\phi\rangle = U|\psi\rangle$
- Unitary matrices all have eigenvalues ± 1
- $U^\dagger U = I$

Measurement

- Define a set of measurement operators $\{M_i = |i\rangle \langle i|\}$
- Probabilty of measurement of state $|i\rangle$ is $\langle \psi| M_i |\psi\rangle$

Measurement

- Define a set of measurement operators $\{M_i = |i\rangle \langle i|\}$
- Probabilty of measurement of state $|i\rangle$ is $\langle\psi| M_i |\psi\rangle$
- Let $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$
- $\langle\psi| M_0 |\psi\rangle = \langle\psi|0\rangle \langle 0\psi\rangle$
- $(\alpha^* \langle 0|0\rangle + \beta^* \langle 1|0\rangle)(\alpha \langle 0|0\rangle + \beta \langle 1|0\rangle)$
- $\alpha^*\alpha = |\alpha|^2$

Entanglement

- Sometimes we cannot always write a two qubit state in a nice separable form like $|\psi\rangle \otimes |\phi\rangle$
- Consider $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- This is a maximally entangled Bell state.
- Measurement of one qubit will alter the other.

Density Operators

- Sometimes we don't completely know the state, so we introduce a new notation
- If our state is $|\psi_i\rangle$ with probability p_i, then we say our state is
- $\rho := \sum p_i |\psi_i\rangle \langle\psi_i|$
- Evolution: $\rho = \sum p_i |\psi_i\rangle \langle\psi_i| \rightarrow \sum p_i U |\psi_i\rangle \langle\psi_i| U\dagger = U\rho U^\dagger$
- Measurement: $tr(M_i M_i^\dagger \rho)$

No-Cloning Theorem

- You cannot clone arbitrary quantum data

No-Cloning Theorem

- You cannot clone arbitrary quantum data
- Proof: assume you can. Then $\exists U$ such that $U |\psi\rangle |0\rangle = |\psi\rangle |\psi\rangle$

No-Cloning Theorem

- You cannot clone arbitrary quantum data
- Proof: assume you can. Then $\exists U$ such that $U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$,$U|\phi\rangle|0\rangle = |\phi\rangle|\phi\rangle$
- $\langle 0|\langle\phi| U^\dagger U|\psi\rangle|0\rangle = \langle\phi|\langle\phi|\psi\rangle|\psi\rangle$
- $\langle 0|\langle\phi|\psi\rangle|0\rangle = \langle\phi|\psi\rangle^2$
- $\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2$

No-Cloning Theorem

- You cannot clone arbitrary quantum data
- Proof: assume you can. Then $\exists U$ such that $U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$,$U|\phi\rangle|0\rangle = |\phi\rangle|\phi\rangle$
- $\langle 0|\langle\phi| U^\dagger U|\psi\rangle|0\rangle = \langle\phi|\langle\phi|\psi\rangle|\psi\rangle$
- $\langle 0|\langle\phi|\psi\rangle|0\rangle = \langle\phi|\psi\rangle^2$
- $\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2$
- Then $\langle\phi|\psi\rangle = 0, 1$ only, which is not general. A contradiciton □

Threshold Schemes

- A (k, n) threshold scheme on a piece of data is an algorithm to break it up into n pieces such that any subset of size k can be used to reconstruct the data, but any subset of size $< k$ contains no information about the data.
- (n, n) scheme for data d: For $1, ..., n-1$ do $x_i \overset{\$}{\leftarrow} \{0,1\}^{|d|}$,
- $x_n = x_1 \oplus ... \oplus x_{n-1} \oplus d$
- To reconstruct, $d = x_1 \oplus ... \oplus x_n$
- Shamir Secret Sharing allows for any possible (k, n) scheme with $k \leq n$

A bound on threshold schemes

- If $n \geq 2k$, then no possible (k, n) threshold scheme exists.

A bound on threshold schemes

- If $n \geq 2k$, then no possible (k, n) threshold scheme exists.
- Proof: Assume to the contrary it is possible. Apply the (k,n) scheme to the state to produce n shares
- Take two disjoint sets of k shares each. We can do this since $n \geq 2k$.
- Reconstruct the state twice with these two disjoint subsets.
- This contradicts the no-cloning theorem. □

Two more quick results

- If a set of players I is authorized, then $\bar{I}$ is not authorized
- More than a single player will not be able to reconstruct the secret

(2,3) example

- A qutrit is $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle$ Consider the map:
- $|0\rangle \mapsto |000\rangle + |111\rangle + |222\rangle$
- $|1\rangle \mapsto |012\rangle + |120\rangle + |201\rangle$
- $|2\rangle \mapsto |021\rangle + |102\rangle + |012\rangle$

(2,3) example

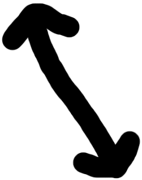
- $|S\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle$
- $|S\rangle \mapsto V|S\rangle$

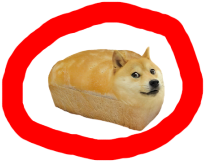
$$\begin{aligned} V|S\rangle = \frac{1}{\sqrt{3}}\alpha(&|000\rangle + |111\rangle + |222\rangle) + \\ &\beta(|012\rangle + |120\rangle + |201\rangle) + \\ &\gamma(|021\rangle + |102\rangle + |012\rangle) \end{aligned}$$

(2,3) example

- We need to prove that V exists, that its unitary
- For two arbitary qutrits $|\phi\rangle, |\psi\rangle$ we inner product $V|\phi\rangle, V|\psi\rangle$
- $\langle\phi| V^\dagger V |\psi\rangle = \alpha^\dagger\alpha' + \beta^\dagger\beta' + \gamma^\dagger\gamma' = \langle\phi|\psi\rangle$
- $\langle\phi| V^\dagger V |\psi\rangle = \langle\phi|\psi\rangle \iff V^\dagger V = I \iff V$ is unitary.

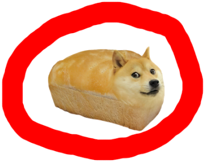
$$|S\rangle \mapsto V\,|S\rangle$$





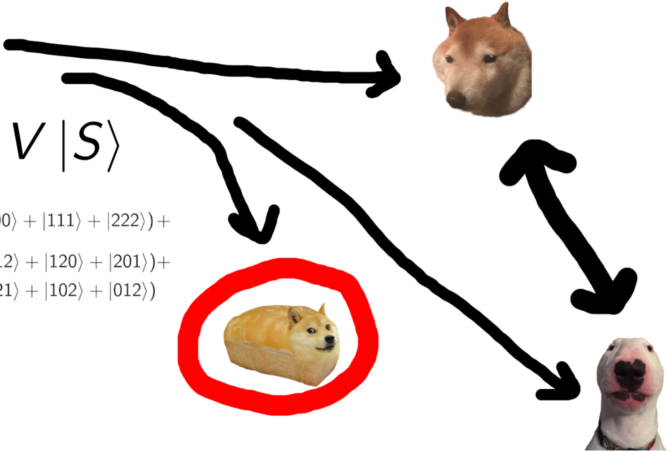
$$|S\rangle \mapsto V|S\rangle$$

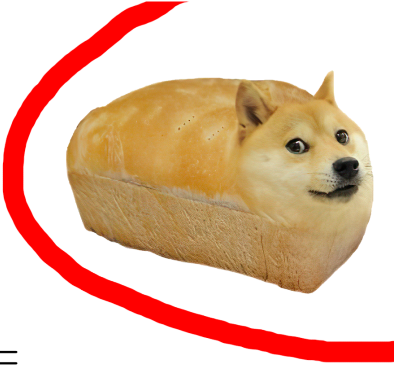
$$V|S\rangle = \frac{1}{\sqrt{3}}(\alpha(|000\rangle + |111\rangle + |222\rangle) + \beta(|012\rangle + |120\rangle + |201\rangle) + \gamma(|021\rangle + |102\rangle + |012\rangle))$$



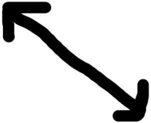
$$|S\rangle \mapsto V|S\rangle$$

$$V|S\rangle = \frac{1}{\sqrt{3}}(\alpha(|000\rangle + |111\rangle + |222\rangle) + \beta(|012\rangle + |120\rangle + |201\rangle) + \gamma(|021\rangle + |102\rangle + |012\rangle))$$





$$\rho_1 = tr_{23}(|\psi\rangle\langle\psi|) =$$
$$\frac{1}{3}\left(|0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2|\right)$$

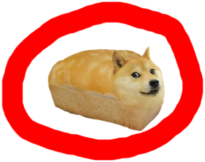


$\rho_A \otimes \rho_B \otimes \rho_C$

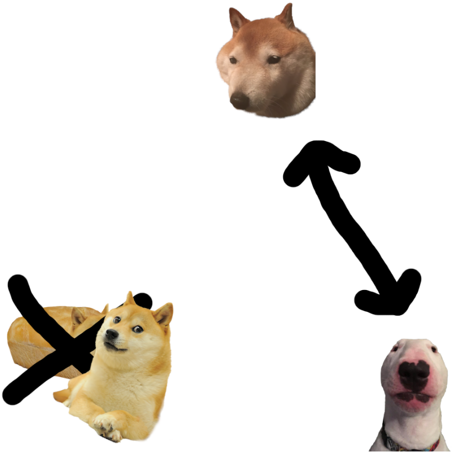
Add ρ_A to ρ_B, then new ρ_B to ρ_A (all mod 3)

$(\alpha |0\rangle + \beta |1\rangle + \gamma |2\rangle) \otimes (|00\rangle + |12\rangle + |21\rangle) \otimes \rho_C$

$$|S\rangle \mapsto V\,|S\rangle$$



$$|S\rangle \mapsto V\,|S\rangle$$



References

- Cleve, Richard, Daniel Gottesman, and Hoi-Kwong Lo. "How to share a quantum secret." Physical Review Letters 83.3 (1999): 648.
- Hillery, Mark, Vladimír Bužek, and André Berthiaume. "Quantum secret sharing." Physical Review A 59.3 (1999): 1829.
- Crépeau, Claude, Daniel Gottesman, and Adam Smith. "Secure multi-party quantum computation." Proceedings of the thiry-fourth annual ACM symposium on Theory of computing. ACM, 2002.
- Aharonov, Dorit, et al. "Interactive proofs for quantum computations." arXiv preprint arXiv:1704.04487 (2017).