Last time: super basic adversary method

- [Ambainis '00] The (Basic) Adversary Method
- The super basic adversary method
  - For φ = (YES, NO). Suppose $Y \subseteq$ YES and $Z \subseteq$ NO s.t.
    - For each $y \in Y$, there exist $\geq m$ strings $z \in Z$ s.t. $\text{dist}(y, z) = 1$
    - For each $z \in Z$, there exist $\geq m'$ strings $y \in Y$ s.t. $\text{dist}(y, z) = 1$
  - Then cost of quantum query algorithm to solve φ is at least $c\sqrt{mm'}$

Recap of the proof so far

- Suppose a quantum algorithm solves φ = (YES, NO)
- Define $R = \{(y, z) \in Y \times Z : \mathrm{dist}(y, z) = 1\}$
- Suppose $|\Psi_w^t\rangle$ is state after t-th query on input w. Define

$$\text{Progress}_t = \sum_{(y,z)\in R} |\langle \Psi_y^t \mid \Psi_z^t \rangle|.$$

- Suffices to show for all t

$$\text{Progress}_t - \text{Progress}_{t+1} \leq \frac{2}{\sqrt{mm'}} |R|$$

Recap of the proof so far

- Fix any t and $t+1$.
- Consider any pair $(y, z) \in R$, differing on j^*-th coordinate.
- Before: $|\Psi_y^t\rangle = \sum_i \alpha_i |i\rangle \otimes |\phi_i\rangle$, $|\Psi_z^t\rangle = \sum_i \beta_i |i\rangle \otimes |\phi_i'\rangle$
- After: $|\Psi_y^{t+1}\rangle = \sum_i (-1)^{y_i} \alpha_i |i\rangle \otimes |\phi_i\rangle$, $|\Psi_z^{t+1}\rangle = \sum_i (-1)^{z_i} \beta_i |i\rangle \otimes |\phi_i'\rangle$
- We have shown $\langle \Psi_y^t | \Psi_z^t \rangle - \langle \Psi_y^{t+1} | \Psi_z^{t+1} \rangle = 2\overline{\alpha_{j*}}\beta_{j*}\langle \phi_{j*} | \phi_{j*}' \rangle$, which implies

$$|\langle \Psi_y^t | \Psi_z^t \rangle - \langle \Psi_y^{t+1} | \Psi_z^{t+1} \rangle| \leq 2|\alpha_{j*}||\beta_{j*}| \leq \sqrt{m/m'}|\alpha_{j*}|^2 + \sqrt{m'/m}|\beta_{j*}|^2$$

- Consider any pair $(y, z) \in R$, differing on j^*-th coordinate.

$$\sum_{(y,z)\in R} \sqrt{m/m'}\,|\alpha_{j*}|^2 + \sqrt{m'/m}\,|\beta_{j*}|^2 \leq \ldots$$

Basic Adversary Method

- For φ = (YES, NO). Suppose $Y \subseteq$ YES and $Z \subseteq$ NO s.t.
  - For each $y \in Y$, there exist $\geq m$ strings $z \in Z$ s.t. $\text{dist}(y, z) = 1$
  - For each $z \in Z$, there exist $\geq m'$ strings $y \in Y$ s.t. $\text{dist}(y, z) = 1$
  - For each $y \in Y$ and j, there exist $\leq \ell$ strings $z \in Z$ s.t. $y_j \neq z_j$
  - For each $z \in Z$ and j, there exist $\leq \ell'$ strings $y \in Y$ s.t. $y_j \neq z_j$
- Then cost of quantum query algorithm to solve φ is at least $c\sqrt{mm'/\ell\ell'}$

Application of Basic Adversary Method

- Grover search problem, but promised there are at least k ones.
- Query complexity is at least …?

History

- [Bennett–Bernstein–Brassard–Vazirani ca. ’96]: Proved a cost lower bound for φ = “OR”: $\gtrsim \sqrt{N}$ queries are necessary. They called their technique the Hybrid Method
- [Ambainis ’00]: The (Basic) Adversary Method
- [Many groups]: Variants on the Adversary Method
- [Høyer–Lee–Špalek ’07]:“Negative-weights”, aka General Adversary Method
- [Reichardt ’09]: The General Adversary Method is optimal — there is always a matching upper bound (query algorithm)!

Mixed states and density matrices

- Mixed state: p_1 probability of $|\Psi_1\rangle$, …, p_m probability of $|\Psi_m\rangle$, where $\sum p_i = 1$ and each $|\Psi_i\rangle$ is unit in $\mathbb{C}^d$
- Definition: density matrix $\rho = \sum_{i=1}^{m} p_i |\Psi_i\rangle\langle\Psi_i|$
- Question: Measure in basis $|u_1\rangle, \ldots, |u_d\rangle$, what is the probability that readout is $|u_i\rangle$?
- Example 1: 50% of $|0\rangle$, 50% of $|1\rangle$
- Example 2: 50% of $|+\rangle$, 50% of $|-\rangle$

- Example 3: 100% of $|0\rangle$
- Example 4: 100% of $-|0\rangle$
- Example 4: 100% of $i|0\rangle$
- Question: Measure in standard basis $|u_1\rangle, \ldots, |u_d\rangle$, what is the probability that the readout is $|u_i\rangle$?
- Properties: ρ is a density matrix
    - ρ is Hermitian
    - ρ is positive-semidefinite (PSD), that is, $\rho \succeq 0$
    - $\mathrm{tr}(\rho) = 1$

- Equivalent definition: A d-dimensional density matrix is a Hermitian d by d matrix ρ with $\rho \geq 0$ and $\mathrm{tr}(\rho) = 1$. Why?

- CF. A probability distribution on {1, 2, …, d} is a vector $p \in \mathbb{R}^d$ such that $p_i \geq 0$ and $\sum_i p_i = 1$

- Question: how does a unitary transformation affect ρ?

- Question: how does a measurement in the standard basis affect ρ?

- Question: adjoining two mixed states?

- Definition: Maximally mixed state has density matrix $\begin{pmatrix} 1/d & & \\ & \ddots & \\ & & 1/d \end{pmatrix}$

- This is the quantum analog of uniform distribution