Adversary-Based Parity Lower Bounds with Small Probability Bias

Badih Ghazi

Setup

- Computing the parity function in the query model with error probability $1/2 - q(n)$ where $q(n) = o(1)$.

Setup

- Computing the parity function in the query model with error probability $1/2 - q(n)$ where $q(n) = o(1)$.
- Using the polynomial method: $\Omega(n)$ for any $q(n) \geq 0$.

Setup

- Computing the parity function in the query model with error probability $1/2 - q(n)$ where $q(n) = o(1)$.
- Using the polynomial method: $\Omega(n)$ for any $q(n) \geq 0$.
- Additive adversary arguments:

Setup

- Computing the parity function in the query model with error probability $1/2 - q(n)$ where $q(n) = o(1)$.
- Using the polynomial method: $\Omega(n)$ for any $q(n) \geq 0$.
- Additive adversary arguments:
  - Reichardt's characterization of $Q(f)$ in terms of $Adv^{\pm}(f)$ holds only in the bounded error case.

$$Q_{1/2-q(n)}(Parity_n) \geq Adv^{\pm}_{1/2-q(n)}(Parity_n) = \Omega((q(n))^2 n)$$

Setup

- Computing the parity function in the query model with error probability $1/2 - q(n)$ where $q(n) = o(1)$.
- Using the polynomial method: $\Omega(n)$ for any $q(n) \geq 0$.
- Additive adversary arguments:
  - Reichardt's characterization of $Q(f)$ in terms of $Adv^{\pm}(f)$ holds only in the bounded error case.

$$Q_{1/2-q(n)}(Parity_n) \geq Adv^{\pm}_{1/2-q(n)}(Parity_n) = \Omega((q(n))^2 n)$$

  - Decays rapidly with $q(n)$.

Setup

- Computing the parity function in the query model with error probability $1/2 - q(n)$ where $q(n) = o(1)$.
- Using the polynomial method: $\Omega(n)$ for any $q(n) \geq 0$.
- Additive adversary arguments:
  - Reichardt's characterization of $Q(f)$ in terms of $Adv^{\pm}(f)$ holds only in the bounded error case.

$$Q_{1/2-q(n)}(Parity_n) \geq Adv^{\pm}_{1/2-q(n)}(Parity_n) = \Omega((q(n))^2 n)$$

  - Decays rapidly with $q(n)$.
  - Gives a trivial constant bound even for $q(n) = 1/\sqrt{n}$.

Setup

- Computing the parity function in the query model with error probability $1/2 - q(n)$ where $q(n) = o(1)$.
- Using the polynomial method: $\Omega(n)$ for any $q(n) \geq 0$.
- Additive adversary arguments:
  - Reichardt's characterization of $Q(f)$ in terms of $Adv^{\pm}(f)$ holds only in the bounded error case.

$$Q_{1/2-q(n)}(Parity_n) \geq Adv^{\pm}_{1/2-q(n)}(Parity_n) = \Omega((q(n))^2 n)$$

  - Decays rapidly with $q(n)$.
  - Gives a trivial constant bound even for $q(n) = 1/\sqrt{n}$.
- Question: Can we get a better lower bound using adversary-based arguments ?

Outline

Outline

- Show a lower bound of $\Omega(n)$ even for exponentially small $q(n)$.

Outline

- Show a lower bound of $\Omega(n)$ even for exponentially small $q(n)$.
  - Proof is based on a "quantum reduction" to the t-fold search problem, with $t = \theta(n)$.

Outline

- Show a lower bound of $\Omega(n)$ even for exponentially small $q(n)$.
  - Proof is based on a "quantum reduction" to the t-fold search problem, with $t = \theta(n)$.
  - Adaptation of the proof of Cleve et. al to our setup.

Outline

- Show a lower bound of $\Omega(n)$ even for exponentially small $q(n)$.
  - Proof is based on a "quantum reduction" to the t-fold search problem, with $t = \theta(n)$.
  - Adaptation of the proof of Cleve et. al to our setup.
  - Holds even for "weak" algorithms for parity.

The quantum reduction

- Notation
  - For any $S \subset [n]$, χ_S: Characteristic vector of S
  - $x|_S$: Restriction of x to the subset S.

The quantum reduction

- Notation
  - For any $S \subset [n]$, χ_S: Characteristic vector of S
  - $x|_S$: Restriction of x to the subset S.
- Observation [Scott Aaronson]: for all $x \in \{0,1\}^n$, we have

$$\frac{1}{\sqrt{2^n}} \sum_{S \subset [n]} (-1)^{Par_n(x|_S)} H_n |\chi_S\rangle = |x\rangle$$

The quantum reduction

- Notation
  - For any $S \subset [n]$, χ_S: Characteristic vector of S
  - $x|_S$: Restriction of x to the subset S.
- Observation [Scott Aaronson]: for all $x \in \{0, 1\}^n$, we have

$$\frac{1}{\sqrt{2^n}} \sum_{S \subset [n]} (-1)^{Par_n(x|_S)} H_n |\chi_S\rangle = |x\rangle$$

- Given an algorithm that produces such a superposition with $r(n)$ queries, get an algorithm that recovers $|x\rangle$ with $r(n)$ queries.

The quantum reduction

- Notation
  - For any $S \subset [n]$, χ_S: Characteristic vector of S
  - $x|_S$: Restriction of x to the subset S.
- Observation [Scott Aaronson]: for all $x \in \{0,1\}^n$, we have

$$\frac{1}{\sqrt{2^n}} \sum_{S \subset [n]} (-1)^{Par_n(x|_S)} H_n |\chi_S\rangle = |x\rangle$$

- Given an algorithm that produces such a superposition with $r(n)$ queries, get an algorithm that recovers $|x\rangle$ with $r(n)$ queries.
- Need to deal with garbage.

The quantum reduction for coherent algorithms

- A parity algorithm is coherent if on inputs x and S, it takes the state $|x\rangle|\chi_S\rangle|z\rangle$ to $|x\rangle|\chi_S\rangle|z + Par_n(x|_S)\rangle$.

The quantum reduction for coherent algorithms

- A parity algorithm is coherent if on inputs x and S, it takes the state $|x\rangle|\chi_S\rangle|z\rangle$ to $|x\rangle|\chi_S\rangle|z + Par_n(x|_S)\rangle$.
- The reduction
  - Start with the state $|x\rangle|0\rangle^{\otimes n}|1\rangle$.

The quantum reduction for coherent algorithms

- A parity algorithm is coherent if on inputs x and S, it takes the state $|x\rangle|\chi_S\rangle|z\rangle$ to $|x\rangle|\chi_S\rangle|z + Par_n(x|_S)\rangle$.
- The reduction
  - Start with the state $|x\rangle|0\rangle^{\otimes n}|1\rangle$.
  - Hadamard the last $n+1$ qubits:

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{(z,\chi_S)\in\{0,1\}^{n+1}} (-1)^z |x\rangle|\chi_S\rangle|z\rangle$$

The quantum reduction for coherent algorithms

- A parity algorithm is coherent if on inputs x and S, it takes the state $|x\rangle|\chi_S\rangle|z\rangle$ to $|x\rangle|\chi_S\rangle|z + Par_n(x|_S)\rangle$.
- The reduction
  - Start with the state $|x\rangle|0\rangle^{\otimes n}|1\rangle$.
  - Hadamard the last $n+1$ qubits:

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{(z,\chi_S)\in\{0,1\}^{n+1}} (-1)^z |x\rangle|\chi_S\rangle|z\rangle$$

  - Apply the coherent parity algorithm and Hadamard the last $(n+1)$ qubits:

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{(z,\chi_S)\in\{0,1\}^{n+1}} (-1)^{z+Par_n(x|_S)} |x\rangle H_n|\chi_S\rangle H_1|z\rangle = |x\rangle|x\rangle|1\rangle$$

The quantum reduction for coherent algorithms

- A parity algorithm is coherent if on inputs x and S, it takes the state $|x\rangle|\chi_S\rangle|z\rangle$ to $|x\rangle|\chi_S\rangle|z + Par_n(x|_S)\rangle$.
- The reduction
  - Start with the state $|x\rangle|0\rangle^{\otimes n}|1\rangle$.
  - Hadamard the last $n+1$ qubits:

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{(z,\chi_S)\in\{0,1\}^{n+1}} (-1)^z |x\rangle|\chi_S\rangle|z\rangle$$

  - Apply the coherent parity algorithm and Hadamard the last $(n+1)$ qubits:

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{(z,\chi_S)\in\{0,1\}^{n+1}} (-1)^{z+Par_n(x|_S)} |x\rangle H_n|\chi_S\rangle H_1|z\rangle = |x\rangle|x\rangle|1\rangle$$

  - Measure the middle n qubits in the standard basis: get x with probability 1!

The quantum reduction for coherent algorithms

- Claim
  - Let Σ_O be any finite set.
  - If there exists a coherent algorithm $\mathcal{A}$ that computes $Parity_n$ using $r(n)$ queries, then for any function $f : \{0,1\}^n \rightarrow \Sigma_O$, there is an algorithm $\mathcal{B}_f$ that computes f exactly using $r(n)$ queries.

The quantum reduction for general algorithms

- Claim
  - Let $t \leq \frac{n}{4e}$, $t = \theta(n)$.
  - Let $q(n) = \Omega(e^{-t/16})$
  - If $\mathcal{A}$ computes $Parity_n$ with error probability $p_x(n)$ for every $x \in \{0,1\}^n$ and for all x with $|x| = t$,

$$\frac{1}{2^n} \sum_{S \subset \{0,1\}^n} p_{x|_S}(n) \leq 1/2 - q(n)$$

  - Then, $\mathcal{A}$ makes $\Omega(n)$ queries.

The quantum reduction for general algorithms

- Claim
  - Let $t \leq \frac{n}{4e}$, $t = \theta(n)$.
  - Let $q(n) = \Omega(e^{-t/16})$
  - If $\mathcal{A}$ computes $Parity_n$ with error probability $p_x(n)$ for every $x \in \{0,1\}^n$ and for all x with $|x| = t$,

$$\frac{1}{2^n} \sum_{S \subset \{0,1\}^n} p_{x|_S}(n) \leq 1/2 - q(n)$$

  - Then, $\mathcal{A}$ makes $\Omega(n)$ queries.
- Corollary
  - $Q_{\frac{1}{2}-e^{-c \cdot n}}(Parity_n) = \Omega(n)$ for any constant $c \leq \frac{1}{87}$.

General parity algorithms

- $\mathcal{A}$ takes the state $|x\rangle|\chi_S\rangle|z\rangle|0\rangle|0\rangle^{\otimes w}$ to

  $$a_{x,S}|x\rangle|\chi_S\rangle|z\rangle|Par_n(x|_S)\rangle|J_{x,S}\rangle + b_{x,S}|x\rangle|\chi_S\rangle|z\rangle|Par'_n(x|_S)\rangle|K_{x,S}\rangle$$

  where $|b_{x,S}|^2 = p_{x|_S}(n)$, $|a_{x,S}|^2 + |b_{x,S}|^2 = 1$ and $|J_{x,S}\rangle$ and $|K_{x,S}\rangle$ are unit vectors.

General parity algorithms

- $\mathcal{A}$ takes the state $|x\rangle|\chi_S\rangle|z\rangle|0\rangle|0\rangle^{\otimes w}$ to

$$a_{x,S}|x\rangle|\chi_S\rangle|z\rangle|Par_n(x|_S)\rangle|J_{x,S}\rangle + b_{x,S}|x\rangle|\chi_S\rangle|z\rangle|Par'_n(x|_S)\rangle|K_{x,S}\rangle$$

  where $|b_{x,S}|^2 = p_{x|_S}(n)$, $|a_{x,S}|^2 + |b_{x,S}|^2 = 1$ and $|J_{x,S}\rangle$ and $|K_{x,S}\rangle$ are unit vectors.

- Apply a CNOT gate and uncompute $\mathcal{A}$:

$$|x\rangle|\chi_S\rangle|z + Par_n(x|_S)\rangle|0\rangle^{\otimes(w+1)} + \sqrt{2}b_{x,S}|M_{x,S,z}\rangle$$

  where $|M_{x,S,z}\rangle$ satisfies the properties $|M_{x,S,0}\rangle = -|M_{x,S,1}\rangle$ and $\{|M_{x,S,0}\rangle\}_{x,S}$ is orthonormal.

General parity algorithms

- $\mathcal{A}$ takes the state $|x\rangle|\chi_S\rangle|z\rangle|0\rangle|0\rangle^{\otimes w}$ to

  $$a_{x,S}|x\rangle|\chi_S\rangle|z\rangle|Par_n(x|_S)\rangle|J_{x,S}\rangle + b_{x,S}|x\rangle|\chi_S\rangle|z\rangle|Par'_n(x|_S)\rangle|K_{x,S}\rangle$$

  where $|b_{x,S}|^2 = p_{x|_S}(n)$, $|a_{x,S}|^2 + |b_{x,S}|^2 = 1$ and $|J_{x,S}\rangle$ and $|K_{x,S}\rangle$ are unit vectors.
- Apply a CNOT gate and uncompute $\mathcal{A}$:

  $$|x\rangle|\chi_S\rangle|z + Par_n(x|_S)\rangle|0\rangle^{\otimes(w+1)} + \sqrt{2}b_{x,S}|M_{x,S,z}\rangle$$

  where $|M_{x,S,z}\rangle$ satisfies the properties $|M_{x,S,0}\rangle = -|M_{x,S,1}\rangle$ and $\{|M_{x,S,0}\rangle\}_{x,S}$ is orthonormal.
- $|x\rangle|\chi_S\rangle|z + Par_n(x|_S)\rangle|0\rangle^{\otimes(w+1)}$:
  - Output of a coherent parity algorithm
  - Not necessarily orthogonal to $|M_{x,S,z}\rangle$

The quantum reduction for general algorithms

- Apply Hadamard gate, the above algorithm and another Hadamard gate: $|x\rangle|x\rangle|1\rangle|0\rangle^{\otimes(w+1)} + |\psi\rangle$

$$\||\psi\rangle\|_2^2 = \|\frac{1}{\sqrt{2^n}} \sum_{(z,\chi_S)\in\{0,1\}^{n+1}} (-1)^z b_{x,S}|M_{x,S,z}\rangle\|_2^2$$

$$= \frac{4}{2^n} \sum_{\chi_S\in\{0,1\}^n} p_{x|_S}(n)$$

The quantum reduction for general algorithms

- Apply Hadamard gate, the above algorithm and another Hadamard gate: $|x\rangle|x\rangle|1\rangle|0\rangle^{\otimes(w+1)} + |\psi\rangle$

$$\||\psi\rangle\|_2^2 = \|\frac{1}{\sqrt{2^n}} \sum_{(z,\chi_S)\in\{0,1\}^{n+1}} (-1)^z b_{x,S}|M_{x,S,z}\rangle\|_2^2$$

$$= \frac{4}{2^n} \sum_{\chi_S\in\{0,1\}^n} p_{x|S}(n)$$

- $Pr[\text{Obtaining } x] \geq 4q^2(n)$ whenever

$$\frac{1}{2^n} \sum_{S\subset\{0,1\}^n} p_{x|S}(n) \leq (\frac{1}{2} - q(n))$$

The quantum reduction for general algorithms

- Holevo's theorem ?

The quantum reduction for general algorithms

- Holevo's theorem ?
  - n queries to the oracle might give $n \log n$ classical bits of information.

The quantum reduction for general algorithms

- Holevo's theorem ?
  - n queries to the oracle might give $n \log n$ classical bits of information.
- The t-fold search problem
  - Given $x \in \{0,1\}^n$ and promised that $|x| = t$, find the subset $J \subset [n]$ of 1's of x.

The quantum reduction for general algorithms

- Holevo's theorem ?
  - n queries to the oracle might give $n \log n$ classical bits of information.
- The t-fold search problem
  - Given $x \in \{0,1\}^n$ and promised that $|x| = t$, find the subset $J \subset [n]$ of 1's of x.
- For every $t \leq \frac{n}{4e}$ and every $\epsilon = 1 - \Omega(e^{-t/8})$, $Q_\epsilon(t\text{-fold search}) = \Omega(\sqrt{tn})$.
  - Proof using the earliest version of the multiplicative adversary method(Ambianis 2005, Spalek 2007)

The quantum reduction for general algorithms

- Holevo's theorem ?
  - n queries to the oracle might give $n \log n$ classical bits of information.
- The t-fold search problem
  - Given $x \in \{0,1\}^n$ and promised that $|x| = t$, find the subset $J \subset [n]$ of 1's of x.
- For every $t \leq \frac{n}{4e}$ and every $\epsilon = 1 - \Omega(e^{-t/8})$, $Q_\epsilon(t\text{-fold search}) = \Omega(\sqrt{tn})$.
  - Proof using the earliest version of the multiplicative adversary method(Ambianis 2005, Spalek 2007)
- Conclude: The claim holds for all $q(n) = \Omega(e^{-t/16})$.