Quantum Weak Parity Problem

Mohammad Bavarian (joint with S. Aaronson)
bavarian@mit.edu

Quantum Complexity Project   Dec 12^{th} 2012

1. Introduction
2. Lower Bounds
3. Upper Bounds
4. The Gap and the Case $k \ll \sqrt{n}$

Origin of the Problem

Only thing I will for sure remember from this course in two years:
PARITY needs $\Omega(n)$ queries in a black box-model !
Is this end of PARITY's story? NO!

Question

Imagine given access to a black-box $X = (x_1, x_2, \ldots, x_n)$ and still want to compute $PARITY(x_1, x_2, \ldots, x_n)$.

Problem? allowed to make only k queries.

Maybe box becomes untrustable after k queries or explodes or something !
Can you do something intelligent regarding PARITY when $k \ll n$?

Hope: we compute PARITY on large number of inputs ?!

Definition of Weak Parity Problem

Problem (Weak PARITY Problem)

What is the maximum size of a subset $A \subseteq \{0,1\}^n$ such that there exists a (bounded error) quantum algorithm U that makes at most k queries to $X = (x_1, x_2, \ldots, x_n)$ and satisfies for all $x \in A$

$$\Pr[U(x) = PARITY(x)] \geq \frac{2}{3} \qquad \forall x \in A$$

Observation

A Classical randomized machine restricted to make $k < n$ queries might as well not bother to query the box at all and just output zero !

Classical Machines seem too weak for this problem. What about quantum? Quantum, this work.

Weak PARITY Recast

We defined Weak Parity as a maximization problem on the size of good set, i.e. where we can compute PARITY.

But our lower bound techniques work in the framework of minimizing query complexity.

A new definition:

Problem (Weak PARITY Recast)

What is the minimum query complexity of a quantum algorithm U that outputs PARITY with bounded error on a set of fractional size $\frac{1}{2} + \epsilon$ of $Q_n = \{0, 1\}^n$.

Lower Bound Using Polynomial Method

Theorem

Any quantum algorithm U computing PARITY on a set A of size $(\frac{1}{2}+\epsilon)2^n$ requires at least $\Omega(\frac{n}{\log(1/\epsilon)})$.

Sketch of Proof

- Create an algorithm U' that uses U to compute PARITY on every input w.p $> 1/2$.
- Polynomial Method $\longrightarrow$ U' needs $\Omega(n)$ queries $\longrightarrow$ Lower bound on U.

The key is self-reducibility of PARITY.

- Pick a random vector $Y = (y_1, y_2, \ldots, y_n)$. Computes PARITY of $Z = X + Y$. We know $PARITY(Y)$ because we generated it.
- Compute PARITY of Z: Run U on Z for $O(\log(1/\epsilon))$ times. Take majority of answer. Will succeed w.p. $> 1/2$.

An Upper Bound

Theorem

There exist an algorithm U that makes only $O(\frac{n}{\sqrt{\log(1/\epsilon)}})$ queries to $X = (x_1, x_2, \ldots, x_n)$ and computes PARITY on A a set of size $(\frac{1}{2} + \epsilon)2^n$.

Sketch of Proof

- The key is the case $\epsilon = 2^{-n}$. Observation: $OR_n = PARITY_n$ for $2^{n-1} + 1$ inputs.
- Conclude the general case: Partition the coordinates $\{x_i\}_{i=1}^n$ into $m \approx \log(1/\epsilon)$ groups of size roughly $\frac{n}{m}$.
- Output $OR_m(y_1, y_2, \ldots, y_m)$ where each y_i is the PARITY of the corresponding i-th group out of total m groups.

□

How About This Gap?

The gap looks small. Actually it is not so.

Back to original formulation of problem

Corollary (Gap Recast)

A quantum machine restricted to make only k queries to a black box can decide PARITY on a set A of size

$$\frac{1}{2} + 2^{-O(n^{2(1-c)})} \leq \frac{|A|}{2^n} \leq \frac{1}{2} + 2^{-\Omega(n^{1-c})}$$

Important Case

- Our lowest complexity algorithm required $\Omega(\sqrt{n})$ queries.
- Don't know any non-trivial algorithm for $k \ll \sqrt{n}$. However, we cannot rule out algorithms succeeding on $\frac{1}{2} + 2^{-n^{0.4}}$ fraction say.
- So a big gap in some sense.

Weak Parity With Constant Queries?

Question

Can we do anything non-trivial using only $O(1)$ queries to the box?

Weak Parity With Constant Queries?

Question

Can we do anything non-trivial using only $O(1)$ queries to the box?

The answer is No.

Theorem

We at least need $\sqrt{\alpha(n)}$ queries to compute PARITY on a set of size $2^{n-1} + 1$

$$\alpha(n) = \frac{1}{2}\log n - \frac{1}{2}\log\log(n) + \frac{1}{2}$$

Proof Idea Extremal Graph theory over the hypercube. Lower Bound follows by showing *sensitivity* is at least $\alpha(n)$. □

Last Words: Improvements and Conjectures

Conjecture

We need $\Omega(\sqrt{n})$ queries for Weak Parity for $2^{n-1}+1$ size.

More generally we expect that the algorithm presented to be optimal. Improving the lower bound to $\Omega(n^{\delta})$ might be hard. How do I know?

Last Words: Improvements and Conjectures

Conjecture

We need $\Omega(\sqrt{n})$ queries for Weak Parity for $2^{n-1}+1$ size.

More generally we expect that the algorithm presented to be optimal. Improving the lower bound to $\Omega(n^{\delta})$ might be hard. How do I know? Relations to sensitivity conjecture.

Hence we restrict to logarithmic regime. We get some improvements. As corollary we have,

Theorem

For any $\delta > 0$ there exist $\beta > 0$ such that for $f : \{0,1\}^n \to \{0,1\}$,

$$2^{s(f)} \geq \beta \deg(f)^{1-\delta}$$

This might be be the best upper bound known on $\deg(f)$ in terms of $s(f)$.

Summary

- Introduced Weak Parity problem.
- Upper bound of $O(\frac{n}{\sqrt{\log(1/\epsilon)}})$ and lower bound of $\Omega(\frac{n}{\log(1/\epsilon)})$ for query complexity $PARITY_n$ on a set of fractional size $\frac{1}{2} + \epsilon$.
- Briefly mentioned the conjectures and theorems regarding the case $k \ll \sqrt{n}$.