Quadratically Tight Relations for Randomized Query Complexity

Rahul Jain Hartmut Klauck Srijita Kundu Troy Lee
Miklos Santha Swagato Sanyal Jevgēnijs Vihrovs

Centre for Quantum Technologies, National University of Singapore,
Centre for Quantum Computer Science, University of Latvia.

8th June, 2018

The 13th International Computer Science Symposium in Russia, CSR 2018

Outline

Query Complexity

- We want to compute some Boolean function $f : \{0,1\}^n \to \{0,1\}$.
- The input is $x = (x_1, \ldots, x_n)$.
- With a single query we can ask the value of any x_i.
- The cost of the computation is the number of queries made.

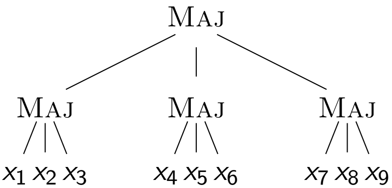
Query Complexity

- Determistic query complexity $\mathrm{D}(f)$ (minimum worst-case number of queries).
- Randomized query complexity $\mathrm{R}(f)$ (correct with probability $\geq 2/3$).
- Exact randomized query complexity $\mathrm{R}_0(f)$ (minimum worst-case expected number of queries).

$$\mathrm{R}(f) \leq \mathrm{R}_0(f) \leq \mathrm{D}(f).$$

Example: Recursive Majority

- $3\text{-}\textsc{Maj}(x_1, x_2, x_3) = 1 \iff x_1 + x_2 + x_3 \geq 2.$
- $\mathsf{D}(3\text{-}\textsc{Maj}_h) = 3^h.$
- $\mathsf{R}_0(3\text{-}\textsc{Maj}_h) \leq (8/3)^h.$



Query Complexity

- In this work, we study which measures $\mathrm{M}(f)$ can characterize $\mathrm{R}_0(f)$ or $\mathrm{R}(f)$ quadratically: $\mathrm{M}(f) \leq \mathrm{R}(f) \leq \mathrm{M}(f)^2$?
- We show two results:
  1. The *expectational certificate* complexity bounds $\mathrm{R}_0(f)$ quadratically:

$$\mathrm{EC}(f) \leq \mathrm{R}_0(f) \leq O(\mathrm{EC}(f)^2).$$

  2. The *partition bound* bounds $\mathrm{R}(f)$ quadratically for product distributions μ:

$$\mathrm{D}^{\mu}_{1/3}(f) \leq O(\mathrm{prt}_{1/3}(f)^2).$$

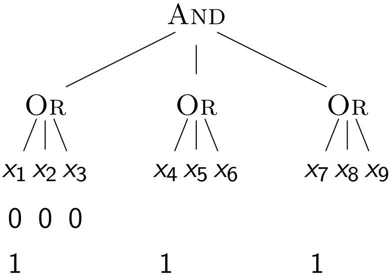
Outline

Certificate Complexity

- A *certificate* for an input x is a set of positions of x that have to be revealed to know the value of $f(x)$ with certainty.
- The *length* of a certificate is the number of positions revealed.
- A *minimal* certificate of x is a certificate of smallest length $\mathrm{C}(f,x)$.
- The *certificate complexity* of f is $\mathrm{C}(f) = \max_x \mathrm{C}(f,x)$.
- It is known that $\mathrm{C}(f) \leq \mathrm{R}_0(f) \leq \mathrm{C}(f)^2$.

Example: AND-OR

- $\mathrm{C}(\textsc{And-Or}_n) = \sqrt{n}$.



Fractional Certificate Complexity

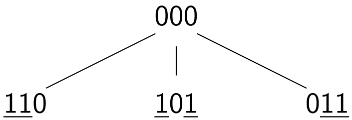
- Fractional certificate complexity $\mathrm{FC}(f)$ is given by the optimal value of the following LP: [Tal / Gilmer, Saks, Srinivasan]

$$\begin{array}{ll} \text{minimize} & \max\limits_{x} \sum\limits_{i \in [n]} w_x(i) \\ \text{subject to} & \forall x, y \text{ s.t. } f(x) \neq f(y) : \sum\limits_{i : x_i \neq y_i} w_x(i) \geq 1 \\ & \forall x, i : 0 \leq w_x(i) \leq 1. \end{array}$$

- $\mathrm{FC}(f) \leq \mathrm{C}(f)$.
- It is known that $\mathrm{FC}(f) \leq \mathrm{R}(f) \leq \mathrm{R}_0(f) \leq \mathrm{FC}(f)^3$.

Example: Majority

- $3\text{-}\mathrm{MAJ}(x_1, x_2, x_3) = 1 \iff x_1 + x_2 + x_3 \geq 2$.
- $\mathrm{C}(f, 000) = 2$.
- $\mathrm{FC}(f, 000) = 3/2$.
  Weights $w_1 = w_2 = w_3 = 1/2$.



Fractional Certificate Complexity

- Hypothesis: $\mathrm{R}_0(f) \leq \mathrm{FC}(f)^2$.
- If that is true, then $\mathrm{R}_0(f) \leq \mathrm{Q}(f)^4$. (Quantum query complexity.) Currently the best upper bound is $\mathrm{R}_0(f) \leq \mathrm{Q}(f)^6$.
- A quadratic separation is known, $\mathrm{R}(\textsc{And-Or}_n) = \Omega(n)$, $\mathrm{FC}(\textsc{And-Or}_n) = \sqrt{n}$.

Expectational Certificate Complexity

- Expectational certificate complexity $\mathrm{EC}(f)$ is given by the optimal value of the following program:

$$\begin{aligned} \text{minimize} \quad & \max_x \sum_{i \in [n]} w_x(i) \\ \text{subject to} \quad & \forall y \text{ s.t. } f(x) \neq f(y) : \sum_{i : x_i \neq y_i} w_x(i) w_y(i) \geq 1, \\ & \forall x, i : 0 \leq w_x(i) \leq 1. \end{aligned}$$

- Not a linear program anymore!

Expectational Certificate Complexity

$\mathrm{R}(f) = O(\mathrm{EC}(f)^2)$ algorithm:

- Repeat $O(\mathrm{EC}(f))$ times:
  - Pick any consistent (with previous queries) input z s.t. $f(z) = 1$;
  - If there is no such z, **return 0**.
  - Independently query each x_i with probability $w_z(i)$;
- **Return 1**.

Each round takes $\sum_{i=1}^{n} w_z(i) \leq \mathrm{EC}(f)$ queries on expectation; hence query complexity is $O(\mathrm{EC}(f)^2)$.

Expected amount of weight removed from w_x each round is $\sum_{i:x_i \neq z_i} w_x(i) w_z(i) \geq 1$; hence, $O(\mathrm{EC}(f))$ many rounds is enough.

Expectational Certificate Complexity

Properties:

- $\mathrm{FC}(f) \leq \mathrm{EC}(f) \leq \mathrm{C}(f)$.
- $\mathrm{EC}(f) \leq \mathrm{C}(f)^2$, tight!
- $\mathrm{EC}(f) \leq \mathrm{R}_0(f) \leq O(\mathrm{EC}(f)^2)$.
- $\mathrm{EC}(f) \leq O(\mathrm{FC}(f)^{3/2})$.
- $\mathrm{EC}(f)^{2/3} \leq \mathrm{R}(f) \leq O(\mathrm{EC}(f)^2)$.

Outline

1 Query Complexity

2 Expectational Certificate Complexity

3 Partition Bound

Partition Bound

- The ϵ-partition bound of f (denoted by $\mathrm{prt}_\epsilon(f)$), is given by the $\log_2$ of the optimal value of the following LP: [Jain, Klauck]

$$\text{minimize} \sum_{z,A} w_{z,A} \cdot 2^{|A|} \quad \text{subject to} \quad \begin{aligned} &\forall x : \sum_{A \ni x} w_{f(x),A} \geq 1 - \epsilon, \\ &\forall x : \sum_{z, A \ni x} w_{z,A} = 1, \\ &\forall z, A : w_{z,A} \geq 0. \end{aligned}$$

- Lower bound, $\frac{1}{2}\,\mathrm{prt}_\epsilon(f) \leq \mathrm{R}_\epsilon(f)$.

Partition Bound

- Example: $\mathrm{prt}(\textsc{And-Or}_n) = \Omega(n)$.
- Known that $\mathrm{R}(f) = O(\mathrm{prt}(f))^3$.
- Best separation is quadratic, $\mathrm{R}(f) = \Omega(\mathrm{prt}(f)^2)$. [Ambainis, Kokainis, Kothari]
- Is $\mathrm{prt}(f)$ quadratically tight for $\mathrm{R}(f)$?

Distributional Query Complexity

- Let μ be a probability distribution over inputs $\{0,1\}^n$.
- Distributional query complexity $\mathrm{D}_\epsilon^\mu(f)$ is the minimum worst-case cost of a deterministic algorithm $\mathcal{A}$ such that

$$\Pr_{x\sim\mu}[\mathcal{A}(x) = f(x)] \geq 1 - \epsilon.$$

- Yao's theorem:

$$\mathrm{R}_\epsilon(f) = \max_\mu \mathrm{D}_\epsilon^\mu(f).$$

Block Sensitivity

- An input x is *sensitive* on a subset of positions $B \subseteq [n]$, if $f(x) \neq f(x^B)$.
- The *block sensitivity* of x, denoted by $\mathrm{bs}(f, x)$, is the maximum number of disjoint sensitive blocks.
- The block sensitivity of f is $\max_x \mathrm{bs}(f, x)$.

Corruption Bound

- Let μ be a probability distribution over the inputs.
- Let A be an ϵ-error b-certificate under μ, if

$$\Pr_{x \sim \mu}[f(x) \neq b \mid x \in A] \leq \epsilon.$$

- Query corruption bound:

$$\mathrm{corr}_{\epsilon}^{b,\mu}(f) = \min\{|A| \mid A \text{ is an } \epsilon\text{-error } b\text{-certificate under } \mu\}.$$

- Query corruption bound:

$$\mathrm{corr}_{\epsilon}(f) = \max_{\mu} \max_{b} \mathrm{corr}_{\epsilon}^{b,\mu}(f).$$

Corruption Bound

- Minimum query corruption bound over product distributions:

$$\mathrm{corr}^{\times}_{\min,\epsilon}(f) = \max_{\mu} \min_{b} \mathrm{corr}^{b,\mu}_{\epsilon}(f),$$

  where μ is a product distribution.

- μ is a bit-wise product distribution if for all x,

$$\mu(x) = \prod_{i=1}^{n} \mu_i(x_i).$$

Corruption Bound

- We adapt the proof of $\mathrm{D}(f) \leq \mathrm{C}(f)\,\mathrm{bs}(f)$ to prove that

$$\mathrm{D}^{\mu}_{4\epsilon}(f) = O(\mathrm{corr}^{\times}_{\min,\epsilon}(f) \cdot \mathrm{bs}(f))$$

  for product distributions.

- Since $\mathrm{corr}^{\times}_{\min,\epsilon}(f) \leq \mathrm{corr}_{\epsilon}(f)$ and $\mathrm{bs}(f) \leq \mathrm{corr}_{\epsilon}(f)$, we get

$$\mathrm{D}^{\mu}_{4\epsilon}(f) = O(\mathrm{corr}_{\epsilon}(f)^2).$$

Partition Bound

- Since $\mathrm{bs}(f) = O(\frac{1}{\epsilon}\,\mathrm{prt}_\epsilon(f))$ and $\mathrm{corr}^{\times}_{\min,2\epsilon}(f) \le \mathrm{prt}_\epsilon(f)$, we get

$$\mathrm{D}^{\mu}_{8\epsilon}(f) = O\left(\frac{1}{\epsilon}\mathrm{prt}_\epsilon(f)^2\right).$$

- A polylogarithmic improvement over previous best upper bound; constant error instead of inverse polynomial error. [Harsha, Jain, Radhakrishnan]

Lower Bounds

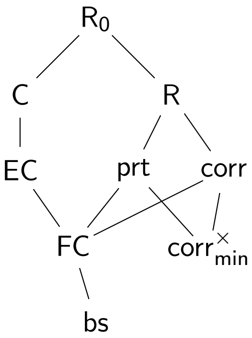


Figure: Lower bounds on $R_0(f)$ and $R(f)$.

Thank you!

Questions?