All Quantum Adversaries Are Equivalent

Robert Špalek
joint work with Mario Szegedy

CWI
THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

Quantum query complexity

- Want to compute Boolean function f
- Input queried by oracle calls $O_x|i, b, z\rangle = |i, b \oplus x_i, z\rangle$
  Allow arbitrary unitary operations between
- Length of computation t is the number of oracle calls
  Final state $|\varphi_x^t\rangle = U_t O_x U_{t-1} \dots U_1 O_x U_0 |0\rangle$
  Measure the leftmost qubit $|q_x\rangle$ of $|\varphi_x^t\rangle$ to get the outcome
  Bounded-error $\Longleftrightarrow Pr[q_x = f(x)] \geq \frac{2}{3}$
- *quantum query complexity* $Q_2(f)$
  is the minimal length of computation of a bounded-error algorithm

Adversary lower bounds

- [Bennett, Bernstein, Brassard & Vazirani, 1997]

  Hybrid method

  - computation starts at a fixed state $|\varphi_x^0\rangle = |\varphi_y^0\rangle$
  - inner product $\langle\varphi_x^k|\varphi_y^k\rangle$ changes little after one query
  - output states $|\varphi_x^t\rangle$ and $|\varphi_y^t\rangle$ almost orthogonal if $f(x) \neq f(y)$

  $\Longrightarrow$ number of queries must be big

- [Ambainis, 2000]

  Quantum adversary

  - examine average over many input pairs

Example lower bound for parity

[Ambainis, 2000] *Unweighted quantum adversary*

- Let $A = f^{-1}(0)$ and $B = f^{-1}(1)$. Pick $R \subseteq A \times B$.
- Compute $m = \min_{x \in A} |\{y : (x,y) \in R\}|$, $m' = \min_{y \in B} |\{x : (x,y) \in R\}|$,
  $\ell = \max_{x \in A, i \in [n]} |\{y : (x,y) \in R \;\&\; x_i \neq y_i\}|$,
  $\ell' = \max_{y \in B, i \in [n]} |\{x : (x,y) \in R \;\&\; x_i \neq y_i\}|$.
- Then $Q_2(f) = \Omega(\sqrt{\frac{mm'}{\ell\ell'}})$

For parity:

- $R = \{(x,y) : |x| = \frac{n}{2}, |y| = \frac{n}{2} + 1, |y - x| = 1\}$
- $m = \frac{n}{2}$, $m' = \frac{n}{2} + 1$, $\ell = \ell' = 1$. Hence $Q_2(\text{parity}) = \Omega(n)$

Weighted adversary lower bounds

- [Høyer, Neerbek & Shi, 2001]
  - used spectral norm of weighted adversary matrix
  - *specialized* for binary search and sorting
- [Barnum, Saks & Szegedy, 2003]
  Spectral method
  - *general bound* in terms of spectral norms
  - one weighted adversary matrix
- [Ambainis, 2003]
  Weighted quantum adversary
  - weight scheme: $n+1$ adversary matrices

Dual adversary lower bounds

- [Laplante & Magniez, 2003]

  Kolmogorov complexity bound

  - general lower bound in terms of $K(x|y)$

    [conditional prefix-free Kolmogorov complexity $K(x|y)$ is the *length of the shortest program* P taken from a prefix-free set such that $P(y) = x$]

  - subsumes all known adversary bounds

- [Laplante & Magniez, 2003]

  "MiniMax" bound

  - combinatorial version of the Kolmogorov complexity bound

Our results

- Equality of bounds:
  - spectral [BSS03]
  - weighted [Ambainis, 2003]
  - “strong” weighted [Zhang, 2004]

  primal

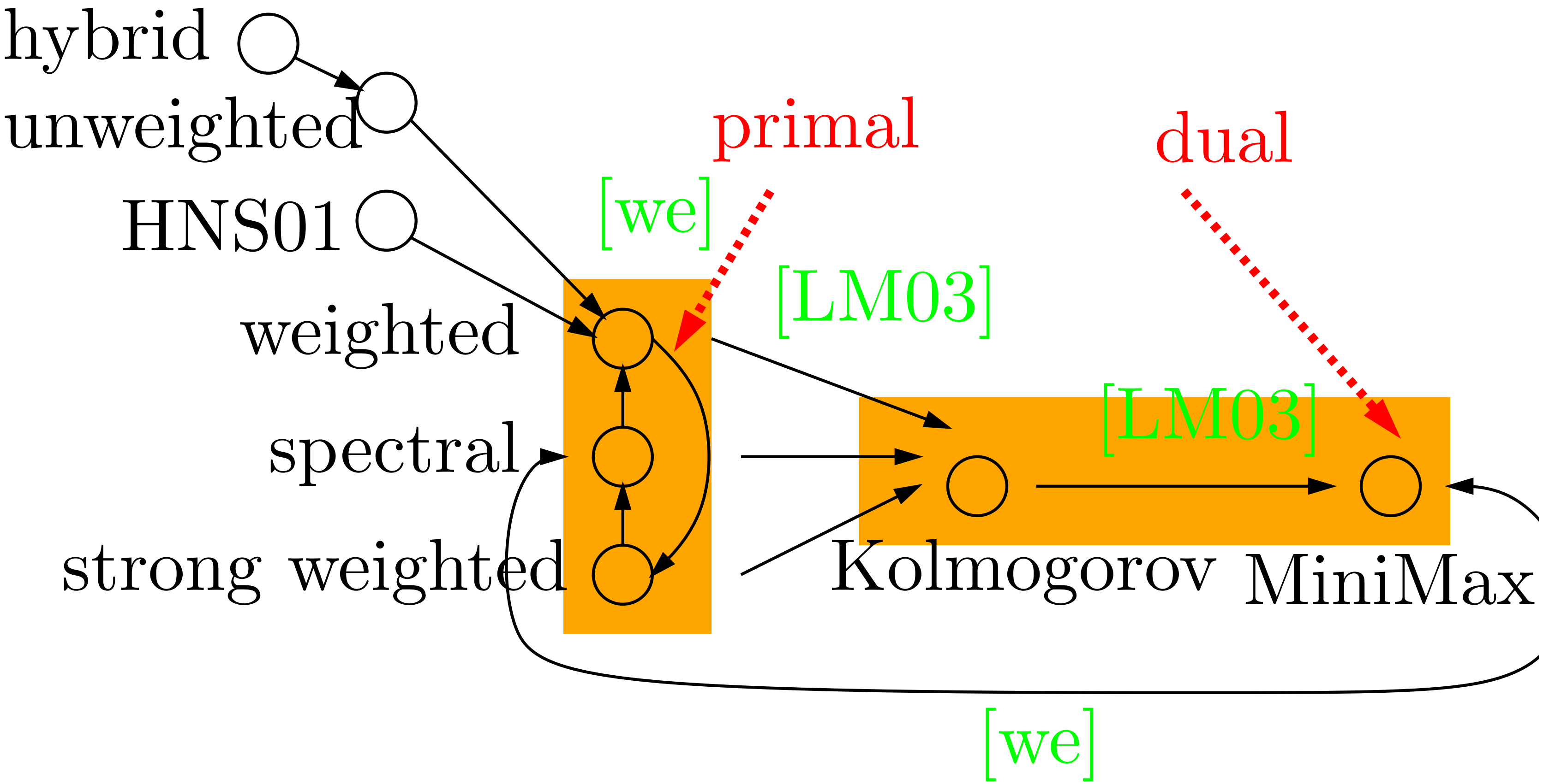
  - Kolmogorov [LM03]
  - MiniMax [LM03]

  dual

- Limitations of the method:
  - $\min(\sqrt{C_0(f)n}, \sqrt{C_1(f)n})$ for partial f
  - $\sqrt{C_0(f)C_1(f)}$ for total f

Some of them were known for some of the methods.

Inclusion of adversary lower bounds



Primal versus dual bounds

- [BSS03] *Spectral Adversary* $SA(f) = \max_{\Gamma} \frac{\lambda(\Gamma)}{\max_i \lambda(\Gamma_i)}$

  $\Gamma \geq 0$ symmetric with $\Gamma[x,y] = 0$ when $f(x) = f(y)$

  $\Gamma_i[x,y] = \Gamma[x,y]$ when $x_i \neq y_i$, otherwise 0

  $\lambda(\Gamma)$ spectral norm of Γ

- [LM03] *MiniMax* $MM(f) = \min_{p_x} \max_{\substack{x,y \\ f(x)\neq f(y)}} \frac{1}{\sum_{i:x_i\neq y_i} \sqrt{p_x(i)p_y(i)}}$

  p_x probability distribution on n bits

- [our paper] $SA(f) = MM(f)$
  - follows from duality in semidefinite programming
  - two non-trivial transformations needed

Reduce MiniMax to spectral 1/2

1. $MM(f) = 1/\mu_{\max} = 1 \Big/ \max_{p_x} \min_{\substack{x,y \\ f(x)\neq f(y)}} \sum_{i:x_i\neq y_i} \sqrt{p_x(i)p_y(i)}$

2. Define $R_i[x,y] = \sqrt{p_x(i)p_y(i)}$ and rewrite it as

$$\begin{aligned} &\text{maximize } \mu \\ &\text{subject to} \quad \forall i : \quad R_i \text{ is non-negative symmetric rank-1}, \\ &\qquad\qquad \textstyle\sum_i R_i \circ I = I, \\ &\qquad\qquad \textstyle\sum_i R_i \circ D_i \geq \mu F. \end{aligned}$$

3. Relax into $\forall i : R_i \succeq 0$.

   The best solution actually *is* rank-1.

Reduce MiniMax to spectral 2/2

4. By duality of semidefinite programming, $\mu_{\max} = \mu_{\min}$

$$\left[\begin{array}{ll} \text{maximize} & \mu \\ \text{subject to} & (\forall i) \quad R_i \succeq 0, \\ & \sum_i R_i \circ I = I, \\ & \sum_i R_i \circ D_i \geq \mu F. \end{array}\right] \Longleftrightarrow \left[\begin{array}{ll} \text{minimize} & \mu = \mathrm{Tr}\Delta \\ \text{subject to} & \Delta \text{ is diagonal} \\ & Z \geq 0 \\ & Z \cdot F = 1 \\ & (\forall i) \;\; \Delta - Z \circ D_i \succeq 0 \end{array}\right]$$

5. *(Simplified)* With a little calculation, w.l.o.g. $\Delta = I$ and

$$\begin{array}{ll} \text{maximize} & Z \cdot F \\ \text{subject to} & Z \geq 0 \\ & (\forall i) \;\; I - Z \circ D_i \succeq 0 \end{array}$$

which is exactly the *spectral bound*.

Tight bounds on spectral norm

- [Mathias, 1990] $\lambda(\Gamma) \leq \max_{\substack{x,y \\ \Gamma[x,y]>0}} r_x(M) c_y(N)$
  - $\Gamma[x, y] = M[x, y] \cdot N[x, y]$ symmetric, $M, N \geq 0$
    $r_x(M)$ the x-th row norm, $c_y(N)$ the y-th column norm
  - The bound is tight, i.e. there always exist M, N s.t. equality is reached.

  [our paper] We add conditioning on $\Gamma[x, y] > 0$, which was not there
- On the other hand, $\lambda(\Gamma) \geq \delta^T \Gamma \delta$ for every $|\delta| = 1$

- [our paper] (Strong) weighted adversary is the spectral adversary with bounds on $\lambda(\Gamma)$ and $\lambda(\Gamma_i)$ expanded using the inequalities above.

Spectral versus (strong) weighted adversary

[BSS03] *Spectral Adversary* $SA(f) = \max_{\Gamma} \frac{\lambda(\Gamma)}{\max_i \lambda(\Gamma_i)}$

[Amb03, Zha04] *Strong Weighted Adversary*

w like Γ, $w_i \geq 0$ with $w_i[x,y] = 0$ when $f(x) = f(y)$ or $x_i = y_i$
and $w_i[x,y]w_i[y,x] \geq w[x,y]^2$ for $x_i \neq y_i$

$$SWA(f) = \max_{w,w_i} \min_{\substack{x,y,i \\ w[x,y]>0,\ x_i \neq y_i}} \sqrt{\frac{\sum_{y^*} w[x,y^*] \sum_{x^*} w[y,x^*]}{\sum_{y^*} w_i[x,y^*] \sum_{x^*} w_i[y,x^*]}}$$

- $\Gamma \to w$: $w[x,y] := \Gamma[x,y]\delta[x]\delta[y]$ for $\delta =$ principal eigen-vector of Γ
- $w \to \Gamma$: $\Gamma[x,y] := \frac{w[x,y]}{\sqrt{wt(x)wt(y)}}$ for $wt(x) = \sum_{y^*} w[x,y^*]$

Limitation of all adversary methods

Easy to prove in the dual formulation! Let f be total.

- $MM(f) = 1 \Big/ \max_{p_x} \min_{\substack{x,y \\ f(x) \neq f(y)}} \sum_{i:x_i \neq y_i} \sqrt{p_x(i) p_y(i)}$
- Let $\mathcal{C}_f(x)$ be some *minimal certificate for $f(x)$*.
  Define $p_x(i) = 1/|\mathcal{C}_f(x)|$ if $i \in \mathcal{C}_f(x)$, otherwise 0.
- For every $f(x) \neq f(y)$, there is $j \in \mathcal{C}_f(x) \cap \mathcal{C}_f(y)$ with $x_j \neq y_j$

$$\sum_{i:x_i \neq y_i} \sqrt{p_x(i) p_y(i)} \geq \sqrt{p_x(j) p_y(j)} = \frac{1}{\sqrt{\mathcal{C}_f(x) \mathcal{C}_f(y)}} \geq \frac{1}{\sqrt{C_0(f) C_1(f)}}$$

Hence $MM(f) \leq \sqrt{C_0(f) C_1(f)}$.

Consequences of the limitation

Cannot prove good lower bounds on problems with small certificates:

- element distinctness: $C_0 = 2$, $C_1 = n$, hence limited by $\mathrm{O}(\sqrt{n})$
  tight bound $\Theta(n^{2/3})$ proved by the polynomial method [AS04]
- triangle finding: $C_0 = n^2$, $C_1 = 3$, hence limited by $\mathrm{O}(n)$
- verification of matrix multiplication: $C_0 = 2n$, $C_1 = n^2$, limited by $\mathrm{O}(n^{3/2})$
- binary And-Or trees: $C_0 = C_1 = \sqrt{n}$, hence limited by $\mathrm{O}(\sqrt{n})$

The complexities of the last 3 problems are open.

Conclusion

- Linear algebraic proof of equivalence of:
  - spectral
  - weighted
  - strong weighted
- Using semidefinite programming, equivalence with MiniMax
- With [LM03], Kolmogorov bound also fits there
- Simple proof of limitations of all bounds

Proof of spectral adversary

- Decompose the quantum state $|\varphi_x\rangle = \sum_i |i\rangle|\varphi_{x,i}\rangle$.

  Then $\langle\varphi_x|\varphi_y\rangle = \sum_i \langle\varphi_{x,i}|\varphi_{y,i}\rangle$.

- After one query $|\varphi'_x\rangle = \sum_i (-1)^{x_i}|i\rangle|\varphi_{x,i}\rangle$.

  Then $\langle\varphi'_x|\varphi'_y\rangle = \sum_i (-1)^{x_i+y_i}\langle\varphi_{x,i}|\varphi_{y,i}\rangle$.

  Hence $\langle\varphi'_x|\varphi'_y\rangle - \langle\varphi_x|\varphi_y\rangle = 2\sum_{i:x_i\neq y_i}\langle\varphi_{x,i}|\varphi_{y,i}\rangle$.

- Define progress function $\Psi^t = \sum_{x,y}\Gamma[x,y]\delta_x\delta_y \cdot \langle\varphi^t_x|\varphi^t_y\rangle$,

  where δ is the principal eigen-vector of Γ with $|\delta| = 1$.

- $\Psi^0 = \sum_{x,y}\Gamma[x,y]\delta_x\delta_y \cdot 1 = \lambda(\Gamma)$, $\qquad \Psi^T$ is constant times smaller.

  But $\Psi^{t+1} - \Psi^t \leq \max_i \lambda(\Gamma_i)$, hence $T \geq \frac{\lambda(\Gamma)}{\max_i \lambda(\Gamma_i)}$.

Recall $\Psi^t = \sum_{x,y} \Gamma[x,y]\delta_x\delta_y \cdot \langle \varphi_x^t | \varphi_y^t \rangle$
and $\langle \varphi_x^{t+1} | \varphi_y^{t+1} \rangle - \langle \varphi_x^t | \varphi_y^t \rangle = 2\sum_{i:x_i \neq y_i} \langle \varphi_{x,i} | \varphi_{y,i} \rangle$.
Define column vector $a_i[x] = \delta_x |\varphi_{x,i}|$

$$\begin{aligned}
\Psi^{t+1} - \Psi^t &= 2\sum_{x,y}\sum_{i:x_i \neq y_i} \Gamma[x,y]\delta_x\delta_y\langle \varphi_{x,i} | \varphi_{y,i} \rangle \\
&\leq 2\sum_{x,y}\sum_{i} \Gamma_i[x,y]\delta_x\delta_y \cdot |\varphi_{x,i}| \cdot |\varphi_{y,i}| \\
&= 2\sum_i a_i^T \Gamma_i a_i \leq 2\sum_i \lambda(\Gamma_i)|a_i|^2 \\
&\leq 2\max_i \lambda(\Gamma_i)\sum_i |a_i|^2 = 2\max_i \lambda(\Gamma_i)\sum_i\sum_x \delta_x^2 |\varphi_{x,i}|^2 \\
&= 2\max_i \lambda(\Gamma_i)\sum_x \delta_x^2 \sum_i |\varphi_{x,i}|^2 = 2\max_i \lambda(\Gamma_i)
\end{aligned}$$