Quantum and randomized query complexity lower bounds using Kolmogorov adversary arguments

Sophie Laplante - LRI
Frédéric Magniez - CNRS LRI
Université Paris-Sud, Orsay
Query complexity: classical model

For any boolean function $f$:

- **Goal** compute $f(x)$
- **Cost** worst case number of queries to bits of $x$

$DT(f) = \text{depth of the shallowest decision tree that computes } f$
Query complexity: quantum model

- **Queries**: unitary transformation $O_x$ that maps $|i, b\rangle$ to $|i, b\oplus x_i\rangle$ (identity on remaining qubits)

- **Computation**: 
  $$|\psi_T\rangle = U_T O_x \cdots O_x U_0 |0\rangle$$

- **Output**: Measure first qubit of $|\psi_T\rangle$

- Error probability bounded by $1/3$

- Same model with **stochastic** matrices for randomized query complexity
Ambainis’ unweighted adversary method

\[ R \]

\[ R_i \ (x_i \neq y_i) \]

\[ X \subseteq f^{-1}(1) \quad Y \subseteq f^{-1}(0) \]

\[ \text{QQC} \geq \Omega \left( \sqrt{\frac{mm'}{ll'}} \right) \]
Quantum lower bound techniques

Semidefinite programming [BSS03]

Query complexity

Spectral method [BS02, BSS03]

Polynomial method [BBCMW]

Ad hoc for ordered search and sorting [HNS02]

This talk

Weighted adversary methods [Am03, Aa04]

Adversary method [Am02]
Kolmogorov complexity

**Defn** $K(x|y)$ is the length of the shortest program that prints $x$, given as input the string $y$

For any finite set of strings $A$,

- $\forall x \in A \ K(x|A) \leq \log(|A|)$
- $\exists x \in A \ K(x|A) \geq \log(|A|)$

Such a string $x$ is called *incompressible* with respect to $A$.

Incompressible strings are “typical”, behave like strings taken at random from $A$. 
Why use Kolmogorov complexity?

- Captures intuition of “not enough information to carry out computational task”.
- Similar to, but often easier to apply than:
  - Information theoretic techniques,
  - Probabilistic method.
Simple case: decision tree complexity

For any function \( f : \{0, 1\}^n \rightarrow D \) and any inputs \( x, y \) such that \( f(x) \neq f(y) \), if \( T \) decides \( f \), its deterministic decision tree complexity is

\[
DT(f) \geq \min_{i: x_i \neq y_i} \{\max\{2K(i|x,T), 2K(i|y,T)\}\}
\]

Claim:

\[ \exists i : x_i \neq y_i \ (i = 3) \]

\[
K(i|x,T) \leq \log(DT(f)) \quad K(i|y,T) \leq \log(DT(f))
\]

\[ x = 01011 \]
\[ y = 01101 \]
Main Theorem

For any function $f : \{0, 1\}^n \rightarrow D$ and any inputs $x, y$ such that $f(x) \neq f(y)$ if $A$ decides $f$,

- The quantum query complexity is
  \[
  \text{QQC} \geq \Omega \left( \frac{1}{\sum_{i : x_i \neq y_i} \sqrt{2^{-K(i|x,A)} - K(i|y,A)}} \right)
  \]

- The randomized query complexity is
  \[
  \text{RQC} \geq \Omega \left( \frac{1}{\sum_{i : x_i \neq y_i} \min\{2^{-K(i|x,A)}, 2^{-K(i|y,A)}\}} \right)
  \]
Example: Lower bound for parity

Pick an incompressible string of length \( n + \log(n) \)

- \( K(i|x) \geq \log(n) \)
- \( n + \log(n) \leq K(i, x) \leq K(i, y) \), so
- \( K(i|y) \geq \log(n) \)

Therefore

\[ \text{QQC(Parity)} \geq \Omega \left( \sqrt{2^{2\log(n)}} \right) = \Omega(n) \]
Sketch of proof (1/2)

1. Model-dependent part

- Quantum case:
  \[ 2T \sum_{i: x_i \neq y_i} \sqrt{p^x(i)p^y(i)} \geq \Omega(1) \]

- Randomized case:
  \[ 2T \sum_{i: x_i \neq y_i} \min(\overline{p}^x(i), \overline{p}^y(i)) \geq \Omega(1) \]

---

\( p^x_t(i) \) = probability of querying \( i \) at step \( t \) on input \( x \).

\( \overline{p}^x(i) = \frac{1}{T} \sum_t p^x_t(i) \)
2. Model-independent part

Using the Shannon-Fano code for the probability distribution on queries,

\[ K(i|x, A) \leq \log \left( \frac{1}{p^x(i)} \right) \]

Therefore,

- **Quantum case:**
  \[
  2T \sum_{i: x_i \neq y_i} \sqrt{2^{-K(i|x, A)} - K(i|x, A)} \geq \Omega(1)
  \]

- **Randomized case:**
  \[
  2T \sum_{i: x_i \neq y_i} \min \{2^{-K(i|x, A)}, 2^{-K(i|y, A)} \} \geq \Omega(1)
  \]

\[ \text{QED} \]
Ambainis’ unweighted adversary method

\[ R \]

\[ \geq m \]

\[ \geq m' \]

\[ X \subseteq f^{-1}(1) \quad Y \subseteq f^{-1}(0) \]

\[ R_i \ (x_i \neq y_i) \]

\[ \leq l \]

\[ \leq l' \]

\[ \text{QQC} \geq \Omega \left( \sqrt{\frac{mm'}{ll'}} \right) \]
Main theorem implies unweighted adversary method

\[ K(i|x) \geq K(x, y) - K(x) - K(y|i, x) + K(i|x, y, K(x, y)) \]

\[ \exists x, y \quad K(x, y) \geq \log |R| \geq \log m + \log |X| \]

\[ \forall x \quad K(x) \leq \log |X| \]

\[ \forall x, y, i \quad K(y|x, i) \leq \log l \]

\[ \geq \log \left( \frac{m}{l} \right) + K(i|x, y, K(x, y)) \]
Main theorem implies unweighted adversary method

We have shown \( \exists x, y \ \forall i \ s.t. \ x_i \neq y_i \)

\[
K(i|x) \geq \log\left(\frac{m}{l}\right) + K(i|x, y, K(x, y))
\]

\[
K(i|y) \geq \log\left(\frac{m'}{l'}\right) + K(i|x, y, K(x, y))
\]

Recall the general theorem:

\[
QQC \geq \Omega \left( \frac{1}{\sum_{i: x_i \neq y_i} \sqrt{2 - K(i|x) - K(i|y)}} \right)
\]

and apply Kraft’s inequality:

\[
QQC \geq \Omega \left( \sqrt{\frac{mm'}{ll'}} \right)
\]
A \textit{b-certificate of size m for f} is a partial assignment of \( m \) bits of the input, which forces the value of a function \( f \) to \( b \) (\( b=0,1 \)).

0-certificate: \( f(*0*11**0*0***) = 0 \)

1-certificate: \( f(*0*1***1*0*0*) = 1 \)

The \textit{b-certificate complexity,} \( C_b(f) \), is the size of the largest minimal \( b \)-certificate for \( f \).

- Bipartiteness: an odd cycle is a 0-certificate.
- Connectivity: a spanning tree is a 1-certificate.
Limits of adversary methods

[Troy Lee] Consider \( x, y \) with \( f(x) = 0 \) and \( f(y) = 1 \).

**0-certificate consistent with** \( x \):

\[
f(*0*1l**0*0**...0) = 0
\]

\( f(y) = 1 \)

So there exists \( i \) with \( x_i \neq y_i \), such that

\[
K(i|x) \leq \log(C_0(f))
\]

Similarly, there exists \( j \) with \( x_j \neq y_j \)

\[
K(j|y) \leq \log(C_1(f))
\]

\[
\frac{1}{\sqrt{2-K(i|x,A)-K(i|y,A)}} \leq \sqrt{nC_0(f)}, \sqrt{nC_1(f)}
\]

(Indep. S. Zhang, for weighted method, ICALP 2004)
Limits of adversary methods

R. Špalek

[Troy Lee] For any function \( f \), and inputs \( x, y \) with \( f(x) = 0 \) and \( f(y) = 1 \), there exist \( i, j \) with \( x_i = y_i, x_j = y_j \).

\[
K(i | x) \leq \log(C_0(f))
\]

\[
K(i | y) \leq \log(C_1(f))
\]

\[
\sum_{i: x_i \neq y_i} \frac{1}{\sqrt{2 - K(i | x, A) - K(i | y, A)}} \leq \sqrt{nC_0(f)}, \sqrt{nC_1(f)}
\]

\[
\sum_{i: x_i \neq y_i} \frac{1}{\sqrt{2 - K(i | x, A) - K(i | y, A)}} \leq \sqrt{C_0(f)C_1(f)}
\]
Summary of results

- New framework to prove lower bounds in query complexity.
- Unified proofs for quantum and randomized lower bounds.
- Generalizes previous adversary methods.
- Applies to boolean as well as non-boolean functions.
- Easy-to-prove limits of adversary methods in terms of certificate complexity.
Directions for future work

- Lower bounds for bounded rounds (adaptive vs nonadaptive queries).
- Similar techniques involving $K(i|x)$ may apply to other models, such as communication complexity, time/space tradeoffs.
- Quantum Kolmogorov complexity might be necessary to handle these models.