Applications of
Kolmogorov complexity
to classical and quantum
computational complexity

Habilitation à diriger des recherches
Sophie Laplante
LRI, Université Paris-Sud XI
December 9, 2005
Summary

- Context and overview of contributions
- Part I  Foundations
  - Time bounded Kolmogorov complexity
  - Quantum Kolmogorov complexity
- Part II  Applications
  - Quantum query complexity lower bounds
  - Formula size lower bounds
- Research projects
Computational complexity
Computational complexity

- Shannon (1949)
  - defines circuits as a model of computation
  - proposes circuit size as a measure of complexity
  - poses the problem of finding an explicit function for which exponential size circuits are required.
Computational complexity

- Shannon (1949)
  - defines circuits as a model of computation
  - proposes circuit size as a measure of complexity
  - poses the problem of finding an explicit function for which exponential size circuits are required.

Current best lower bounds are $5n$ [LR01, IM02] (circuits) and $n^3$ [Hås98] (formulae)
Computational complexity

- Shannon (1949)
  - defines circuits as a model of computation
  - proposes circuit size as a measure of complexity
  - poses the problem of finding an explicit function for which exponential size circuits are required.

Current best lower bounds are $5n$ [LR01, IM02] (circuits) and $n^3$ [Hås98] (formulae)

- Asymptotic time complexity [HS65], P vs NP question [Edm65].
Computational complexity

• Shannon (1949)
  • defines circuits as a model of computation
  • proposes circuit size as a measure of complexity
  • poses the problem of finding an explicit function for which exponential size circuits are required.

  Current best lower bounds are 5n [LR01, IM02] (circuits) and n³ [Hås98] (formulae)

• Asymptotic time complexity [HS65], P vs NP question [Edm65].

  Despite much effort, still no separation in sight
Lower bound techniques

• Significant separations have been achieved by diagonalization

  “So many problems, so few machines...!”

• Many known techniques seem to be fundamentally information theoretic

  “So much information, so little time...!”
Kolmogorov complexity

Introduced by Solomonoff, Kolmogorov, and Chaitin (algorithmic information), in the 60s

\[ K(x) \] is the length of the shortest program that prints \( x \).

- \[ K(“0101010101010101 \ldots”) \approx \log(n) \]
- \[ K(“\text{\ding{51} \text{\ding{51} \text{\ding{51} \text{\ding{51} \ldots}}”) \approx n \]

\[ K(x|y) \] is the length of the shortest program that prints \( x \) when given string \( y \) as auxiliary input.
Incompressibility

Fundamental tool for proving lower bounds:

• For any finite set $A$, $\exists x \in A, K(x) \geq \log(#A)$
  (there are not enough short programs to describe all $x$ in $A$)

Corresponding upper bound:

• For any finite set $A$, $\forall x \in A, K(x) \leq \log(#A)$
  (suffices to give an index into the set $A$)
Classical decision tree model

To compute a boolean function $f : \{0,1\}^n \to \{0,1\}$,

Model: decision tree

Cost: Number of queries to input

Query complexity of $f$:

$DT(f)$ is depth of shallowest decision tree for $f$
Simple decision tree lower bound

**Proposition** \[ L \] If \( f(x) \neq f(y) \), then there exists \( i, x_i \neq y_i \):

\[
K(i|x) \leq \log(\text{depth}(T)) \\
K(i|y) \leq \log(\text{depth}(T))
\]

\[
\text{DT}(f) \geq \min_i \{ \max \{ 2K(i|x), 2K(i|y) \} \}
\]
Simple decision tree lower bound

**Proposition** [L] If \( f(x) \neq f(y) \), then there exists \( i, x_i \neq y_i \):

\[
K(i|x) \leq \log(\text{depth}(T))
\]

\[
K(i|y) \leq \log(\text{depth}(T))
\]

\[
\text{DT}(f) \geq \min_i \left\{ \max \{2K(i|x), 2K(i|y)\} \right\}
\]
Simple decision tree lower bound

**Proposition** [1] If \( f(x) \neq f(y) \), then there exists \( i, x_i \neq y_i \):

\[
K(i|x) \leq \log(\text{depth}(T))
\]

\[
K(i|y) \leq \log(\text{depth}(T))
\]

\[
\text{DT}(f) \geq \min_i \{ \max \{ 2K(i|x), 2K(i|y) \} \}
\]
Lower bounds for bounded depth circuits [Fortnow, L]

Extractors and language compression [Buhrman, Fortnow, L]

Quantum query lower bounds [L, Magniez]

Quantum Kolmogorov complexity [Berthiaume, van Dam, L]

Formula size lower bounds [L, Lee, Szegedy]

Approximate testing [L, Lassaigne, Magniez, Peyronnet, de Rougemont]

Lower bound on the language compression problem [Buhrman, L, Miltersen]

Adaptiveness and random-self-reducibility [Babai, L]

Adaptiveness and coherence [Feigenbaum, Fortnow, L, Naik]

Simulating quantum correlations [Degorre, L, Roland]

Lower bounds for bounded depth circuits [Fortnow, L]
Part I

Foundations

Time bounded Kolmogorov complexity

Quantum Kolmogorov complexity
Foundations: Time bounded complexity

- Lower bounds for bounded depth circuits [Fortnow, L]
- Extractors and language compression [Buhrman, Fortnow, L]
  - Approximate testing [L, Lassaigne, Magniez, Peyronnet, de Rougemont]
  - Lower bound on the language compression problem [Buhrman, L, Miltersen]
- Quantum query lower bounds [L, Magniez]
  - Adaptiveness and random-self-reducibility [Babai, L]
  - Adaptiveness and coherence [Feigenbaum, Fortnow, L, Naik]
- Formula size lower bounds [L, Lee, Szegedy]
- Simulating quantum correlations [Degorre, L, Roland]
- Quantum Kolmogorov complexity [Berthiaume, van Dam, L]
- Lower bounds for bounded depth circuits [Fortnow, L]
Time-bounded Kolmogorov complexity

\[ C^p(x) \] is the length of the shortest program that prints \( x \) in time \( p(|x|) \).

\[ CD^p(x) \] is the length of the shortest program that runs in time \( p(|z|) \) and accepts \( z \) if and only if \( z = x \).
Time-bounded Kolmogorov complexity

\[ C_p(x) \] is the length of the shortest program that prints \( x \) in time \( p(|x|) \).

\[ CD_p(x) \] is the length of the shortest program that runs in time \( p(|z|) \) and accepts \( z \) if and only if \( z = x \).

- In unbounded time, \( CD^\infty = C^\infty \).
- For any finite set \( A \), and \( x \in A \) \( CD^\infty (x) \leq \log (#A) \).
- The language compression problem [S83]:
  
  For any \( A \), \( x \in A \) \( CD^p(x) \leq ?? \) for polynomial \( p \).
Language compression problem

• For most \( r \), \( CD^p(x|r) \leq \log(\#A) \) [S83]

• \( CD^p(x) \leq 2\log(\#A) \) [BFL02]

• For all but \( \epsilon \) fraction of \( x \in A \),

\[
CD^p(x|r) \leq \log(\#A) + \text{polylog}(|x|/\epsilon) \quad \text{[BFL02]}
\]

• Exists \( A, x \in A \), \( CD^p(x) \geq 2\log(\#A) \) [BLM00]
Cover-free families of sets

- **Definition** $\mathcal{F}$ is $k$-cover free if for any $F_0,...,F_k$ in $\mathcal{F}$, $F_0 \not\subseteq \bigcup_i F_i$

- **Theorem** [DR82] Let $\mathcal{F}$ be a family of $N$ sets over a universe of $M$ elements. If $\mathcal{F}$ is $k$-cover free and $N > k^3$, then

$$M \geq \frac{N^2 \log(N)}{2 \log(k) + O(1)}$$

$F_0$ is covered by the other sets

$\mathcal{F}$ is 3-cover free
Lower bound on language compression

**Theorem [BLM00]** \( \exists A, x \in A, CD^p_A(x) \geq 2 \log(#A) \)
Lower bound on language compression

Theorem [BLM00] \( \exists A, x \in A, CD_{p,A}(x) \geq 2 \log(\#A) \)

Programs

\( F_x = \{ p: p \text{ accepts } x \} \)
Lower bound on language compression

**Theorem** [BLM00] \( \exists A, x \in A, CD_{p,A}(x) \geq 2 \log(\#A) \)

**Programs**

\[ F_x = \{ p: p \text{ accepts } x \} \]

\[ \mathcal{F} = \{ F_x | x \in A \} \text{ is } k\text{-cover free} \]
Lower bound on language compression

**Theorem** [BLM00] \( \exists A, x \in A, CD^{p,A}(x) \geq 2 \log(#A) \)

*Programs*

\[ F_x = \{ p: p \text{ accepts } x \} \]

\[ \mathcal{F} = \{ F_x \mid x \in A \} \text{ is } k \text{-cover free} \]

*Inputs (\#\mathcal{F} = r^{1/3})*

*Programs*

*Inputs (\#\mathcal{F} = r^{1/3})*

*Programs*
Foundations: Quantum Kolmogorov complexity

- Formula size lower bounds [L, Lee, Szegedy]
- Simulating quantum correlations [Degorre, L, Roland]
- Quantum query lower bounds [L, Magniez]
- Quantum Kolmogorov complexity [Berthiaume, van Dam, L]
- Lower bound on the language compression problem [Buhrman, L, Miltersen]
- Approximate testing [L, Lassaigne, Magniez, Peyronnet, de Rougemont]
- Adaptiveness and random-self-reducibility [Babai, L]
- Adaptiveness and coherence [Feigenbaum, Fortnow, L, Naik]
- Lower bounds for bounded depth circuits [Fortnow, L]
Quantum computation

- Computation acts on qubits
  - $n$-bit strings are vectors forming an orthonormal basis of $2^n$-dimensional Hilbert space, $\{|i\rangle = e_i\}_{1 \leq i \leq 2^n}$
  - Qubits are unit, complex combinations of basis states
- Quantum gates are unitary operations
  - $U^\dagger U = I$
  - Linear, invertible, norm-preserving
Quantum computation

• Computation acts on *qubits*

  • $n$-bit strings are vectors forming an orthonormal basis of $2^n$-dimensional Hilbert space, $\{|i\rangle = e_i\}_{1 \leq i \leq 2^n}$

  • Qubits are unit, complex combinations of basis states

• Quantum gates are unitary operations

  • $U^\dagger U = I$

  • Linear, invertible, norm-preserving

![Diagram showing quantum gate operations]

$|0\rangle \xrightarrow{\text{Unitary Gate}} |f(0)\rangle \xrightarrow{}$

$|1\rangle \xrightarrow{\text{Unitary Gate}} |f(1)\rangle \xrightarrow{}$
Quantum computation

- Computation acts on *qubits*
- $n$-bit strings are vectors forming an orthonormal basis of $2^n$-dimensional Hilbert space, $\{|i\rangle = e_i\}_{1 \leq i \leq 2^n}$
- Qubits are unit, complex combinations of basis states
- Quantum gates are unitary operations
  - $U^\dagger U = I$
  - Linear, invertible, norm-preserving

$$\alpha|0\rangle + \beta|1\rangle \xrightarrow{\text{Unitary Gate}} \alpha|f(0)\rangle + \beta|f(1)\rangle$$
Quantum Kolmogorov complexity

• Three definitions have been proposed
  • Classical description [V00]
  • Quantum description [BDL00]
  • Semi-density matrices [G01]

• We give a quantum description by means of universal quantum Turing machine $U$ [BV97]

• $QC(\lvert \phi \rangle) = \min\{\dim(\lvert \psi \rangle) : U\lvert \psi \rangle \approx \lvert \phi \rangle\}$

\textit{number of qubits}
Properties of quantum Kolmogorov complexity

- Properties of [BDL00] definition
  - Existence of incompressible quantum states
  - Strong connection to quantum information theory (von Neumann entropy)
  - Quantification of no-cloning of quantum states:
    \[ QC(|\phi\rangle^\otimes k | |\phi\rangle) \]
Part II

Applications

Quantum query complexity lower bounds

Formula size lower bounds
Applications: Quantum lower bounds

- Formula size lower bounds [L., Lee, Szegedy]
- Simulating quantum correlations [Degorze, L., Roland]
- Quantum query lower bounds [L., Magniez]
- Quantum Kolmogorov complexity [Berthiaume, van Dam, L.]
- Lower bound on the language compression problem [Buhrman, L., Miltersen]
- Adaptiveness and random-self-reducibility [Babai, L.]
- Adaptiveness and coherence [Feigenbaum, Fortnow, L., Naik]
- Approximate testing [L, Lassaigne, Magniez, Peyronnet, de Rougemont]
- Extractors and language compression [Buhrman, Fortnow, L.]
- Lower bounds for bounded depth circuits [Fortnow, L.]
Adversary method

\[ R \]
\[ \{ x : f(x) = 1 \} \quad \{ y : f(y) = 0 \} \]

\[ R_i = \{ (x,y) \in R : x_i \neq y_i \} \]
Adversary method

For any relation $R$, \( \forall i \ DT(f) \geq \deg_{\min}(R)/(\deg(R_i)) \)

Recall that
\( \forall i \ DT(f) \geq 2^{K(i|x)} \)

- \( K(x,y) \geq \log(_{\#f^{-1}(1)} \deg_{\min}(R)) \)
- \( K(x,y) \leq K(x) + K(i|x) + K(y|x,i) \)
- \( \#f^{-1}(1) \deg_{\min}(R) \leq \#f^{-1}(1) \cdot 2^{K(i|x)} \cdot \deg(R_i) \)
- \( 2^{K(i|x)} \geq \deg_{\min}(R)/(\deg(R_i)) \)
Quantum adversary lower bounds

**Theorem [LM04]**

\[ Q_\varepsilon(f) \geq \frac{c_\varepsilon}{2} \sum_{i: x_i \neq y_i} \frac{1}{\sqrt{2} - K(i|x) - K(i|y)} \]

Implies all previously known quantum adversary lower bounds

- Unweighted adversary [A02]
- Weighted adversary [A03]
- Spectral method [BSS03]

All these methods are equivalent [ŠS05]
Applications: Formula size lower bounds

- Simulating quantum correlations [Degorre, L, Roland]
- Quantum query lower bounds [L, Magniez]
- Quantum Kolmogorov complexity [Berthiaume, van Dam, L]
- Adaptiveness and random-self-reducibility [Babai, L]
- Adaptiveness and coherence [Feigenbaum, Fortnow, L, Naik]
- Lower bounds for bounded depth circuits [Fortnow, L]
- Lower bound on the language compression problem [Buhrman, L, Miltersen]
- Extractors and language compression [Buhrman, Fortnow, L]
- Approximate testing [L, Lassaigne, Magniez, Peyronnet, de Rougemont]
- Formula size lower bounds [L, Lee, Szegedy]
Boolean circuit and formula size

**Boolean circuit**

**Boolean formula**

Best lower bound: 5n  
[Lachish Raz 01,  
Iwama Morizumi 02]

Best lower bound: n³  
[Håstad 98]
Communication complexity

- $D(f) =$ amount of communication in the worst case, for the best protocol for $f$

- $d(f) = D(R_f)$ [KW88]

Given $x, y$ for which $f(x) \neq f(y)$, find $i$ s.t. $x_i \neq y_i$
Circuit depth lower bound

Proposition [LLS05]

\[ K(i|x) + K(i|y) \leq D(R_f) = d(f) \]

Proof

\[ K(i|x) \leq |m_2| + |m_4| + ... \]
\[ K(i|y) \leq |m_1| + |m_5| + ... \]
Background on communication complexity

\[ M_f = \begin{pmatrix} \end{pmatrix} \]
Background on communication complexity

\[ M_f = \]

A’s input \( x \)

B’s input \( y \)

\( f(x,y) \)
Background on communication complexity

\[ M_f = \begin{cases} 
A \text{ sends } 0 \\
A \text{ sends } 1 
\end{cases} \]
Background on communication complexity

\[ M_f = \]

\[
\begin{pmatrix}
B \text{ sends } 1 & B \text{ sends } 0 \\
A \text{ sends } 0 \\
A \text{ sends } 1
\end{pmatrix}
\]
Background on communication complexity

\[ M_f = \begin{pmatrix}
  B \text{ sends } 1 & B \text{ sends } 0 \\
  A \text{ sends } 0 \\
  A \text{ sends } 1
\end{pmatrix} \]
Background on communication complexity

- $D^{\text{Rect}}(f) =$ smallest number of disjoint monochromatic rectangles needed to cover $M_f$

- $L(f) \geq D^{\text{Rect}}(R_f)$ [KW88]

Given $x, y$ for which $f(x) \neq f(y)$, find $i$ s.t. $x_i \neq y_i$. 
Formula size lower bound, spectral formulation

**Theorem [LLS05]** Formula size lower bound

\[ L(f) \geq \max_A \frac{\|A\|^2}{\max_i \|A_i\|^2} \]

\[ M_f = \begin{pmatrix} \vdots \end{pmatrix} \]

\[ \|A\| = \max_{u,v} \frac{u^* A v}{|u||v|} \]
Formula size lower bound, spectral formulation

Theorem [LLS05] Formula size lower bound

\[ L(f) \geq \max_A \frac{\|A\|^2}{\max_i \|A_i\|^2} \]

\[ M_f = \begin{bmatrix} A \\ \end{bmatrix} \]

\[ \|A\| = \max_{u,v} \frac{u^* A v}{\|u\| \|v\|} \]
Theorem [LLS05] Formula size lower bound

\[ L(f) \geq \max_A \frac{\|A\|^2}{\max_i \|A_i\|^2} \]

\[ M_f = \begin{pmatrix} A & A_i \\ 0 & 0 \end{pmatrix} \]

\[ \|A\| = \max_{u,v} \frac{u^* A v}{\|u\| \|v\|} \]

\[ \alpha_i \neq y_i \]
Theorem [LLS05]

\[ L(f) \geq \max_A \frac{||A||^2}{\max_i ||A_i||^2} \]

\[ M_f = \]
Theorem [LLS05]

\[ L(f) \geq \max_A \frac{\|A\|^2}{\max_i \|A_i\|^2} \]

- If \( \mathcal{R} \) is an optimal partition \( R_1, \ldots, R_N \), then if \( \mu \) is subadditive
  \[ L(f) \geq D_{Rect}(R_f) = \#\mathcal{R} \geq \frac{\mu(X \times Y)}{\max_i \mu(R_i)} \]

- If \( \mathcal{S} \) is a covering with \( \mathcal{R} < \mathcal{S} \) (refinement) then if \( \mu \) is monotone,
  \[ L(f) \geq \frac{\mu(X \times Y)}{\max_{S \in \mathcal{S}} \mu(S)} \]

- **Key lemma** [LLS05] \( \|M\|^2 \) is subadditive and monotone
Formula size lower bound

**Theorem [LLS05]**

\[ L(f) \geq \max_A \frac{\|A\|^2}{\max_i \|A_i\|^2} \]

- If \( \mathcal{R} \) is an optimal partition \( R_1, \ldots, R_N \), then if \( \mu \) is subadditive,
  \[ L(f) \geq D_{Rect}(R_f) = \# \mathcal{R} \geq \frac{\mu(X \times Y)}{\max_i \mu(R_i)} \]

- If \( \mathcal{S} \) is a covering with \( \mathcal{R} < \mathcal{S} \) (refinement) then if \( \mu \) is monotone,
  \[ L(f) \geq \frac{\mu(X \times Y)}{\max_{S \in \mathcal{S}} \mu(S)} \]

- **Key lemma [LLS05]** \( \|M\|^2 \) is subadditive and monotone
Relation to other methods

- Closely related to the quantum spectral method

\[
L(f) \geq \max_A \frac{\|A\|^2}{\max_i \|A_i\|^2}
\]

\[
Q_\varepsilon(f) \geq \max_A \frac{\|A\|}{\max_i \|A_i\|}
\]

- Generalizes many previous methods
  - Khrapchenko’s combinatorial method [K71]
  - Koutsoupias’ spectral method [K93]
  - A key lemma of Håstad used to prove the current best formula size lower bound (random restrictions) [H98]
Research project
Current projects

- Continue to unify and extend classical and quantum lower bound techniques

- Combinatorial models
  - Communication complexity, circuits, formula size, decision trees

- Techniques
  - Fourier analysis
  - Information theory methods
Further projects

- Medium-term
  - Apply quantum Kolmogorov complexity to quantum lower bounds, e.g. quantum information theoretic methods

- Long-term
  - Use Kolmogorov complexity to study derandomization
Thank you