On the Quantum Complexity of Classical Words

Markus Müller

Technische Universität Berlin
Institut für Mathematik
Straße des 17. Juni 136
10623 Berlin

Max-Planck-Institut
für Mathematik in den Naturwissenschaften
Inselstraße 22
04103 Leipzig

ECCS 2007, Dresden

Outline

Outline

Motivation

Are quantum computers more powerful than classical computers?

- Quantum computers can solve some problems faster than classical computers ($\rightarrow$ Shor's factoring algorithm). Answer for *Computational Complexity*: Yes.
- What about description length (compression)? Can classical words be compressed further by allowing quantum descriptions? Answer for *Kolmogorov Complexity*: ???

For fixed classical words like $x = 00100010$, compare its classical and its quantum minimal description lengths.

Motivation

Are quantum computers more powerful than classical computers?

- Quantum computers can solve some problems faster than classical computers (→ Shor's factoring algorithm).
  Answer for *Computational Complexity*: Yes.
- What about description length (compression)?
  Can classical words be compressed further by allowing quantum descriptions?
  Answer for *Kolmogorov Complexity*: ???

For fixed classical words like $x = 00100010$, compare its classical and its quantum minimal description lengths.

Motivation

Are quantum computers more powerful than classical computers?

- Quantum computers can solve some problems faster than classical computers ($\longrightarrow$ Shor's factoring algorithm). Answer for *Computational Complexity*: Yes.
- What about description length (compression)? Can classical words be compressed further by allowing quantum descriptions? Answer for *Kolmogorov Complexity*: ???

For fixed classical words like $x = 00100010$, compare its classical and its quantum minimal description lengths.

Motivation

Are quantum computers more powerful than classical computers?

- Quantum computers can solve some problems faster than classical computers ($\longrightarrow$ Shor's factoring algorithm).
  Answer for *Computational Complexity*: Yes.
- What about description length (compression)?
  Can classical words be compressed further by allowing quantum descriptions?
  Answer for *Kolmogorov Complexity*: ???

For fixed classical words like $x = 00100010$, compare its classical and its quantum minimal description lengths.

Motivation

Are quantum computers more powerful than classical computers?

- Quantum computers can solve some problems faster than classical computers ($\longrightarrow$ Shor's factoring algorithm).
  Answer for *Computational Complexity*: Yes.
- What about description length (compression)?
  Can classical words be compressed further by allowing quantum descriptions?
  Answer for *Kolmogorov Complexity*: ???

For fixed classical words like $x = 00100010$, compare its classical and its quantum minimal description lengths.

Motivation

Are quantum computers more powerful than classical computers?

- Quantum computers can solve some problems faster than classical computers ($\to$ Shor's factoring algorithm). Answer for *Computational Complexity*: Yes.
- What about description length (compression)? Can classical words be compressed further by allowing quantum descriptions? Answer for *Kolmogorov Complexity*: ???

For fixed classical words like $x = 00100010$, compare its classical and its quantum minimal description lengths.

Motivation

Are quantum computers more powerful than classical computers?

- Quantum computers can solve some problems faster than classical computers ($\rightarrow$ Shor's factoring algorithm).
  Answer for *Computational Complexity*: Yes.
- What about description length (compression)?
  Can classical words be compressed further by allowing quantum descriptions?
  Answer for *Kolmogorov Complexity*: ???

For fixed classical words like $x = 00100010$, compare its classical and its quantum minimal description lengths.

Outline

Classical Kolmogorov Complexity

Finite binary words: $\{0,1\}^* := \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, \ldots\}$

A computer is a partial recursive function $U : \{0,1\}^* \to \{0,1\}^*$.

Definition of Kolmogorov Complexity

Let U be a (fixed, but arbitrary) universal computer. Then,

$$C(x) := \min\{\ell(p) \mid U(p) = x\} \qquad (x \in \{0,1\}^*).$$

Example

$$C(\underbrace{101010\ldots10}_{2n \text{ times "10"}}) \leq \log n + \mathcal{O}(\log\log n)$$

$C(x) \leq \ell(x) + \text{const.}$, $\qquad C(\underbrace{110111000011\ldots}_{n \text{ random bits}}) \approx n.$

Classical Kolmogorov Complexity

Finite binary words: $\{0,1\}^* := \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, \ldots\}$
A computer is a partial recursive function $U : \{0,1\}^* \to \{0,1\}^*$.

Definition of Kolmogorov Complexity

Let U be a (fixed, but arbitrary) universal computer. Then,

$$C(x) := \min\{\ell(p) \mid U(p) = x\} \qquad (x \in \{0,1\}^*).$$

Example

$$C(\underbrace{101010\ldots10}_{2n \text{ times } ``10"}) \leq \log n + \mathcal{O}(\log\log n)$$

$$C(x) \leq \ell(x) + \text{const.}, \qquad C(\underbrace{110111000011\ldots}_{n \text{ random bits}}) \approx n.$$

Classical Kolmogorov Complexity

Finite binary words: $\{0,1\}^* := \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, \ldots\}$
A computer is a partial recursive function $U : \{0,1\}^* \to \{0,1\}^*$.

Definition of Kolmogorov Complexity

Let U be a (fixed, but arbitrary) universal computer. Then,

$$C(x) := \min\{\ell(p) \mid U(p) = x\} \qquad (x \in \{0,1\}^*).$$

Example

$$C(\underbrace{101010\ldots10}_{2n \text{ times "10"}}) \leq \log n + \mathcal{O}(\log\log n)$$

$$C(x) \leq \ell(x) + \text{const.}, \qquad C(\underbrace{110111000011\ldots}_{n \text{ random bits}}) \approx n.$$

Classical Kolmogorov Complexity

Finite binary words: $\{0,1\}^* := \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, \ldots\}$
A computer is a partial recursive function $U : \{0,1\}^* \to \{0,1\}^*$.

Definition of Kolmogorov Complexity

Let U be a (fixed, but arbitrary) universal computer. Then,

$$C(x) := \min\{\ell(p) \mid U(p) = x\} \qquad (x \in \{0,1\}^*).$$

Example

$$C(\underbrace{101010\ldots10}_{2n \text{ times "}10\text{ "}}) \leq \log n + \mathcal{O}(\log\log n)$$

$$C(x) \leq \ell(x) + \text{const.}, \qquad C(\underbrace{110111000011\ldots}_{n \text{ random bits}}) \approx n.$$

Classical Kolmogorov Complexity

Finite binary words: $\{0,1\}^* := \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, \ldots\}$
A computer is a partial recursive function $U : \{0,1\}^* \to \{0,1\}^*$.

Definition of Kolmogorov Complexity

Let U be a (fixed, but arbitrary) universal computer. Then,

$$C(x) := \min\{\ell(p) \mid U(p) = x\} \qquad (x \in \{0,1\}^*).$$

Example

$$C(\underbrace{101010\ldots10}_{2n \text{ times "10"}}) \leq \log n + \mathcal{O}(\log\log n)$$

$$C(x) \leq \ell(x) + \text{const.}, \qquad C(\underbrace{110111000011\ldots}_{n \text{ random bits}}) \approx n.$$

Classical Kolmogorov Complexity

Finite binary words: $\{0,1\}^* := \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, \ldots\}$
A computer is a partial recursive function $U : \{0,1\}^* \to \{0,1\}^*$.

Definition of Kolmogorov Complexity

Let U be a (fixed, but arbitrary) universal computer. Then,

$$C(x) := \min\{\ell(p) \mid U(p) = x\} \qquad (x \in \{0,1\}^*).$$

Example

$$C(\underbrace{101010\ldots10}_{2n \text{ times "10 "}}) \leq \log n + \mathcal{O}(\log\log n)$$

$$C(x) \leq \ell(x) + \text{const.}, \qquad C(\underbrace{110111000011\ldots}_{n \text{ random bits}}) \approx n.$$

Qubit Strings

Quantum information theory: study superpositions like

$$|\psi\rangle := \frac{1}{\sqrt{2}}\left(|10\rangle + |0110\rangle\right).$$

Definition (Qubit Strings)

A qubit string σ is a state vector or density operator on $\mathcal{H}_{\{0,1\}^*}$, the Hilbert space with $\{0,1\}^*$ as orthonormal basis.

Qubit Strings

Quantum information theory: study superpositions like

$$|\psi\rangle := \frac{1}{\sqrt{2}}\left(|10\rangle + |0110\rangle\right).$$

Definition (Qubit Strings)

A qubit string σ is a state vector or density operator on $\mathcal{H}_{\{0,1\}^*}$, the Hilbert space with $\{0,1\}^*$ as orthonormal basis.

Thus, $|\psi\rangle$ is a qubit string, and so is $\sigma := \frac{2}{3}|\psi\rangle\langle\psi| + \frac{1}{3}|00\rangle\langle 00|$.

Properties

- Distance measure: trace norm $\|\rho - \sigma\|_{\mathrm{Tr}} := \frac{1}{2}\mathrm{Tr}|\rho - \sigma|$
- Length: $\ell(\sigma) := \max\{\ell(s) \mid \langle s|\sigma|s\rangle > 0\}$.

For example $\ell(|\psi\rangle) = 4$, and $\| |\psi\rangle\langle\psi| - \sigma \|$ ...

Qubit Strings

Quantum information theory: study superpositions like

$$|\psi\rangle := \frac{1}{\sqrt{2}}\left(|10\rangle + |0110\rangle\right).$$

Definition (Qubit Strings)

A qubit string σ is a state vector or density operator on $\mathcal{H}_{\{0,1\}^*}$, the Hilbert space with $\{0,1\}^*$ as orthonormal basis.

Thus, $|\psi\rangle$ is a qubit string, and so is $\sigma := \frac{2}{3}|\psi\rangle\langle\psi| + \frac{1}{3}|00\rangle\langle 00|$.

Properties

- Distance measure: trace norm $\|\rho - \sigma\|_{\mathrm{Tr}} := \frac{1}{2}\mathrm{Tr}|\rho - \sigma|$
- Length: $\ell(\sigma) := \max\{\ell(s) \mid \langle s|\sigma|s\rangle > 0\}$.

Qubit Strings

Quantum information theory: study superpositions like

$$|\psi\rangle := \frac{1}{\sqrt{2}}\left(|10\rangle + |0110\rangle\right).$$

Definition (Qubit Strings)

A qubit string σ is a state vector or density operator on $\mathcal{H}_{\{0,1\}^*}$, the Hilbert space with $\{0,1\}^*$ as orthonormal basis.

Thus, $|\psi\rangle$ is a qubit string, and so is $\sigma := \frac{2}{3}|\psi\rangle\langle\psi| + \frac{1}{3}|00\rangle\langle 00|$.

Properties

- Distance measure: trace norm $\|\rho - \sigma\|_{\rm Tr} := \frac{1}{2}{\rm Tr}|\rho - \sigma|$
- Length: $\ell(\sigma) := \max\{\ell(s) \mid \langle s|\sigma|s\rangle > 0\}$.

For example $\ell(|\psi\rangle) = 4$, and $\||\psi\rangle\langle\psi| - \sigma\|_{\rm Tr} = \frac{1}{3}$.

Qubit Strings

Quantum information theory: study superpositions like

$$|\psi\rangle := \frac{1}{\sqrt{2}}\left(|10\rangle + |0110\rangle\right).$$

Definition (Qubit Strings)

A qubit string σ is a state vector or density operator on $\mathcal{H}_{\{0,1\}^*}$, the Hilbert space with $\{0,1\}^*$ as orthonormal basis.

Thus, $|\psi\rangle$ is a qubit string, and so is $\sigma := \frac{2}{3}|\psi\rangle\langle\psi| + \frac{1}{3}|00\rangle\langle 00|$.

Properties

- Distance measure: trace norm $\|\rho - \sigma\|_{\rm Tr} := \frac{1}{2}{\rm Tr}|\rho - \sigma|$
- Length: $\ell(\sigma) := \max\{\ell(s) \mid \langle s|\sigma|s\rangle > 0\}$.

For example $\ell(|\psi\rangle) = 4$, and $\|\,|\psi\rangle\langle\psi| - \sigma\|_{\rm Tr} = \frac{1}{3}$

Qubit Strings

Quantum information theory: study superpositions like

$$|\psi\rangle := \frac{1}{\sqrt{2}}\left(|10\rangle + |0110\rangle\right).$$

Definition (Qubit Strings)

A qubit string σ is a state vector or density operator on $\mathcal{H}_{\{0,1\}^*}$, the Hilbert space with $\{0,1\}^*$ as orthonormal basis.

Thus, $|\psi\rangle$ is a qubit string, and so is $\sigma := \frac{2}{3}|\psi\rangle\langle\psi| + \frac{1}{3}|00\rangle\langle 00|$.

Properties

- Distance measure: trace norm $\|\rho - \sigma\|_{\mathrm{Tr}} := \frac{1}{2}\mathrm{Tr}|\rho - \sigma|$
- Length: $\ell(\sigma) := \max\{\ell(s) \mid \langle s|\sigma|s\rangle > 0\}$.

For example $\ell(|\psi\rangle) = 4$, and $\| \, |\psi\rangle\langle\psi| - \sigma\|_{\mathrm{Tr}} = \frac{1}{3}$.

Quantum Kolmogorov Complexity

Similarly as classical computers, quantum computers are partial maps U : input qubit string $\sigma \mapsto$ output qubit string $U(\sigma)$.

Definition (≈ Berthiaume et al. 2001)

Let U be a universal quantum computer and $\delta > 0$. Then, for every qubit string ρ, define

$$QC^\delta(\rho) := \min\{\ell(\sigma) \mid \|\rho - U(\sigma)\|_{\mathrm{Tr}} \leq \delta\}.$$

Moreover, we set

$$QC(\rho) := \min\left\{\ell(\sigma) \mid \|\rho - U(\sigma, k)\|_{\mathrm{Tr}} \leq \frac{1}{k} \text{ for every } k \in \mathbb{N}\right\}.$$

As classically, $QC(\rho) \leq \ell(\rho) + \mathrm{const.}$

Quantum Kolmogorov Complexity

Similarly as classical computers, quantum computers are partial maps U : input qubit string $\sigma \mapsto$ output qubit string $U(\sigma)$.

Definition (≈ Berthiaume et al. 2001)

Let U be a universal quantum computer and $\delta > 0$. Then, for every qubit string ρ, define

$$QC^{\delta}(\rho) := \min\{\ell(\sigma) \mid \|\rho - U(\sigma)\|_{\mathrm{Tr}} \leq \delta\}.$$

Moreover, we set

$$QC(\rho) := \min\left\{\ell(\sigma) \mid \|\rho - U(\sigma, k)\|_{\mathrm{Tr}} \leq \frac{1}{k} \text{ for every } k \in \mathbb{N}\right\}.$$

As classically, $QC(\rho) \leq \ell(\rho) + \text{const.}$

Quantum Kolmogorov Complexity

Similarly as classical computers, quantum computers are partial maps U : input qubit string $\sigma \mapsto$ output qubit string $U(\sigma)$.

Definition (≈ Berthiaume et al. 2001)

Let U be a universal quantum computer and $\delta > 0$. Then, for every qubit string ρ, define

$$QC^{\delta}(\rho) := \min\{\ell(\sigma) \mid \|\rho - U(\sigma)\|_{\mathrm{Tr}} \leq \delta\}.$$

Moreover, we set

$$QC(\rho) := \min\left\{\ell(\sigma) \mid \|\rho - U(\sigma, k)\|_{\mathrm{Tr}} \leq \frac{1}{k} \text{ for every } k \in \mathbb{N}\right\}.$$

As classically, $QC(\rho) \leq \ell(\rho) + \mathrm{const.}$

Quantum Kolmogorov Complexity

Similarly as classical computers, quantum computers are partial maps U : input qubit string $\sigma \mapsto$ output qubit string $U(\sigma)$.

Definition (≈ Berthiaume et al. 2001)

Let U be a universal quantum computer and $\delta > 0$. Then, for every qubit string ρ, define

$$QC^{\delta}(\rho) := \min\{\ell(\sigma) \mid \|\rho - U(\sigma)\|_{\mathrm{Tr}} \leq \delta\}.$$

Moreover, we set

$$QC(\rho) := \min\left\{\ell(\sigma) \mid \|\rho - U(\sigma, k)\|_{\mathrm{Tr}} \leq \frac{1}{k} \text{ for every } k \in \mathbb{N}\right\}.$$

As classically, $QC(\rho) \leq \ell(\rho) + \mathrm{const.}$

Outline

Statement of the Theorem

Result: Concerning minimal description lengths, quantum computers are not more powerful than classical computers:

Theorem (Quantum Complexity of Classical Words)

For every classical word $x \in \{0,1\}^*$,

$$C(x) = QC(|x\rangle) + \mathcal{O}(1).$$

If $0 < \delta < \frac{1}{6}$, *then*

$$QC^\delta(|x\rangle) \leq C(x) + \text{const.} \leq \frac{QC^\delta(|x\rangle)}{1 - 4\delta} + \text{const}'.$$

Statement of the Theorem

Result: Concerning minimal description lengths, quantum computers are not more powerful than classical computers:

Theorem (Quantum Complexity of Classical Words)

For every classical word $x \in \{0,1\}^*$,

$$C(x) = QC(|x\rangle) + \mathcal{O}(1).$$

If $0 < \delta < \frac{1}{6}$, *then*

$$QC^\delta(|x\rangle) \leq C(x) + \text{const.} \leq \frac{QC^\delta(|x\rangle)}{1 - 4\delta} + \text{const}'.$$

Statement of the Theorem

Result: Concerning minimal description lengths, quantum computers are not more powerful than classical computers:

Theorem (Quantum Complexity of Classical Words)

For every classical word $x \in \{0,1\}^*$,

$$C(x) = QC(|x\rangle) + \mathcal{O}(1).$$

If $0 < \delta < \frac{1}{6}$, *then*

$$QC^{\delta}(|x\rangle) \leq C(x) + \text{const.} \leq \frac{QC^{\delta}(|x\rangle)}{1-4\delta} + \text{const}'.$$

Outline of Proof, Part 1

Equation (1) follows from (2) by an appropriate limit $\delta \to 0$.
It remains to show Equation (2).

Theorem (Quantum Complexity of Classical Words)

For every classical word $x \in \{0,1\}^*$,

$$C(x) = QC(|x\rangle) + \mathcal{O}(1). \tag{1}$$

If $0 < \delta < \frac{1}{6}$, *then*

$$QC^\delta(|x\rangle) \leq C(x) + \text{const.} \leq \frac{QC^\delta(|x\rangle)}{1 - 4\delta} + \text{const}'. \tag{2}$$

Outline of Proof, Part 1

Equation (1) follows from (2) by an appropriate limit $\delta \to 0$.
It remains to show Equation (2).

Theorem (Quantum Complexity of Classical Words)

For every classical word $x \in \{0,1\}^*$,

$$C(x) = QC(|x\rangle) + \mathcal{O}(1). \tag{1}$$

If $0 < \delta < \frac{1}{6}$, *then*

$$QC^{\delta}(|x\rangle) \leq C(x) + \text{const.} \leq \frac{QC^{\delta}(|x\rangle)}{1-4\delta} + \text{const}'. \tag{2}$$

Outline of Proof, Part 1

Equation (1) follows from (2) by an appropriate limit $\delta \to 0$.
It remains to show Equation (2).

Theorem (Quantum Complexity of Classical Words)

For every classical word $x \in \{0,1\}^*$,

$$C(x) = QC(|x\rangle) + \mathcal{O}(1). \tag{1}$$

If $0 < \delta < \frac{1}{6}$, then

$$QC^{\delta}(|x\rangle) \leq C(x) + \text{const.} \leq \frac{QC^{\delta}(|x\rangle)}{1 - 4\delta} + \text{const}'. \tag{2}$$

Outline of Proof, Part 1

Theorem (Quantum Complexity of Classical Words)

$$QC^{\delta}(|x\rangle) \leq C(x) + \text{const.} \leq \frac{QC^{\delta}(|x\rangle)}{1-4\delta} + \text{const}'.$$

Proof of $QC^{\delta}(|x\rangle) \leq C(x) + \text{const.}$:

- Bennett: Every classical computation can be done reversibly...
- ... and can thus be simulated by a universal quantum computer.
- Thus, quantum computers are at least as powerful in compression as classical computers. □

Outline of Proof, Part 1

Theorem (Quantum Complexity of Classical Words)

$$QC^{\delta}(|x\rangle) \leq C(x) + \text{const.} \leq \frac{QC^{\delta}(|x\rangle)}{1-4\delta} + \text{const}'.$$

Proof of $QC^{\delta}(|x\rangle) \leq C(x) + \text{const.}$:

- Bennett: Every classical computation can be done reversibly...
- ... and can thus be simulated by a universal quantum computer.
- Thus, quantum computers are at least as powerful in compression as classical computers. □

Outline of Proof, Part 1

Theorem (Quantum Complexity of Classical Words)

$$QC^{\delta}(|x\rangle) \leq C(x) + \text{const.} \leq \frac{QC^{\delta}(|x\rangle)}{1-4\delta} + \text{const}'.$$

Proof of $QC^{\delta}(|x\rangle) \leq C(x) + \text{const.}$:

- Bennett: Every classical computation can be done reversibly...
- ... and can thus be simulated by a universal quantum computer.
- Thus, quantum computers are at least as powerful in compression as classical computers. □

Outline of Proof, Part 1

Theorem (Quantum Complexity of Classical Words)

$$QC^{\delta}(|x\rangle) \leq C(x) + \text{const.} \leq \frac{QC^{\delta}(|x\rangle)}{1-4\delta} + \text{const}'.$$

Proof of $QC^{\delta}(|x\rangle) \leq C(x) + \text{const.}$:

- Bennett: Every classical computation can be done reversibly...
- ... and can thus be simulated by a universal quantum computer.
- Thus, quantum computers are at least as powerful in compression as classical computers. □

Outline of Proof, Part 1

Theorem (Quantum Complexity of Classical Words)

$$QC^{\delta}(|x\rangle) \leq C(x) + \text{const.} \leq \frac{QC^{\delta}(|x\rangle)}{1-4\delta} + \text{const}'.$$

Proof of $QC^{\delta}(|x\rangle) \leq C(x) + \text{const.}$:

- Bennett: Every classical computation can be done reversibly...
- ... and can thus be simulated by a universal quantum computer.
- Thus, quantum computers are at least as powerful in compression as classical computers. □

Outline of Proof, Part 1

Theorem (Quantum Complexity of Classical Words)

$$QC^{\delta}(|x\rangle) \leq C(x) + \text{const.} \leq \frac{QC^{\delta}(|x\rangle)}{1-4\delta} + \text{const}'.$$

Proof of $QC^{\delta}(|x\rangle) \leq C(x) + \text{const.}$:

- Bennett: Every classical computation can be done reversibly...
- ... and can thus be simulated by a universal quantum computer.
- Thus, quantum computers are at least as powerful in compression as classical computers. □

Outline of Proof, Part 2

Theorem (Quantum Complexity of Classical Words)

$$C(x) \leq \frac{QC^{\delta}(|x\rangle)}{1-4\delta} + \text{const.}$$

Outline of Proof:

- Classical words are mutually orthogonal qubit strings, i.e. $\langle s|t\rangle = 0$ if $s,t \in \{0,1\}^*$ with $s \neq t$.
- (Almost) orthogonal outputs must have (almost) orthogonal inputs. There are only few short orthogonal qubit strings.
- They can all be discovered by short classical computer programs that simulate the quantum computer with brute force. □

Outline of Proof, Part 2

Theorem (Quantum Complexity of Classical Words)

$$C(x) \leq \frac{QC^{\delta}(|x\rangle)}{1-4\delta} + \text{const.}$$

Outline of Proof:

- Classical words are mutually orthogonal qubit strings, i.e. $\langle s|t\rangle = 0$ if $s, t \in \{0,1\}^*$ with $s \neq t$.
- (Almost) orthogonal outputs must have (almost) orthogonal inputs. There are only few short orthogonal qubit strings.
- They can all be discovered by short classical computer programs that simulate the quantum computer with brute force. □

Outline of Proof, Part 2

Theorem (Quantum Complexity of Classical Words)

$$C(x) \leq \frac{QC^{\delta}(|x\rangle)}{1-4\delta} + \mathrm{const.}$$

Outline of Proof:

- Classical words are mutually orthogonal qubit strings, i.e. $\langle s|t\rangle = 0$ if $s, t \in \{0,1\}^*$ with $s \neq t$.
- (Almost) orthogonal outputs must have (almost) orthogonal inputs. There are only few short orthogonal qubit strings.
- They can all be discovered by short classical computer programs that simulate the quantum computer with brute force. □

Outline of Proof, Part 2

Theorem (Quantum Complexity of Classical Words)

$$C(x) \leq \frac{QC^{\delta}(|x\rangle)}{1-4\delta} + \text{const.}$$

Outline of Proof:

- Classical words are mutually orthogonal qubit strings, i.e. $\langle s|t\rangle = 0$ if $s, t \in \{0,1\}^*$ with $s \neq t$.
- (Almost) orthogonal outputs must have (almost) orthogonal inputs. There are only few short orthogonal qubit strings.
- They can all be discovered by short classical computer programs that simulate the quantum computer with brute force. □

Outline of Proof, Part 2

Theorem (Quantum Complexity of Classical Words)

$$C(x) \leq \frac{QC^{\delta}(|x\rangle)}{1-4\delta} + \text{const.}$$

Outline of Proof:

- Classical words are mutually orthogonal qubit strings, i.e. $\langle s|t\rangle = 0$ if $s, t \in \{0,1\}^*$ with $s \neq t$.
- (Almost) orthogonal outputs must have (almost) orthogonal inputs. There are only few short orthogonal qubit strings.
- They can all be discovered by short classical computer programs that simulate the quantum computer with brute force. □

Outline of Proof, Part 2

Theorem (Quantum Complexity of Classical Words)

$$C(x) \leq \frac{QC^{\delta}(|x\rangle)}{1-4\delta} + \mathrm{const.}$$

Outline of Proof:

- Classical words are mutually orthogonal qubit strings, i.e. $\langle s|t\rangle = 0$ if $s, t \in \{0,1\}^*$ with $s \neq t$.
- (Almost) orthogonal outputs must have (almost) orthogonal inputs. There are only few short orthogonal qubit strings.
- They can all be discovered by short classical computer programs that simulate the quantum computer with brute force. □

Conclusions

- Classical and quantum Kolmogorov complexities agree up to an additive constant on the classical words, e.g.

$$C(x) = QC(|x\rangle) + \mathcal{O}(1) \qquad \text{for every } x \in \{0,1\}^*.$$

- Concerning description length alone, quantum and classical computers are equally powerful.
- As C is a special case of QC, both complexities can thus be treated in a single mathematical framework.

Conclusions

- Classical and quantum Kolmogorov complexities agree up to an additive constant on the classical words, e.g.

$$C(x) = QC(|x\rangle) + \mathcal{O}(1) \qquad \text{for every } x \in \{0,1\}^*.$$

- Concerning description length alone, quantum and classical computers are equally powerful.
- As C is a special case of QC, both complexities can thus be treated in a single mathematical framework.

Conclusions

- Classical and quantum Kolmogorov complexities agree up to an additive constant on the classical words, e.g.

$$C(x) = QC(|x\rangle) + \mathcal{O}(1) \qquad \text{for every } x \in \{0,1\}^*.$$

- Concerning description length alone, quantum and classical computers are equally powerful.
- As C is a special case of QC, both complexities can thus be treated in a single mathematical framework.