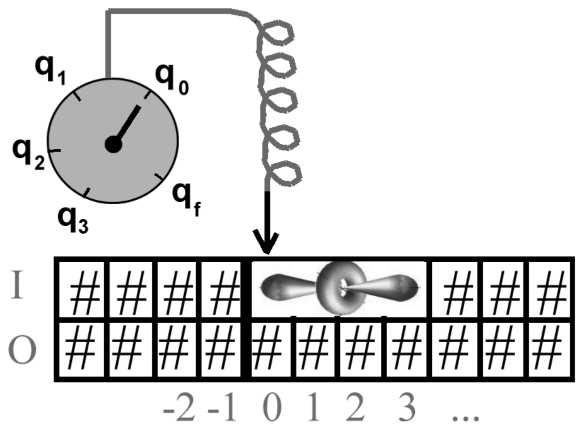
Strongly Universal Quantum Turing Machines & Invariance of Kolmogorov Complexity

Markus Müller

Technical University of Berlin

Institute for Mathematics MA 7-2

Straße des 17. Juni 136, 10623 Berlin, Germany



Overview

1. Classical Theory of Computation

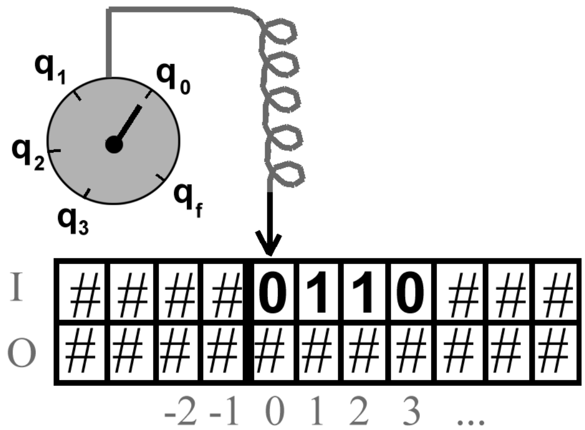
   – Universal Turing Machines
   – Kolmogorov Complexity and its Invariance

2. Quantum Computation

   – Quantum Turing Machines (QTMs)
   – Universality of QTMs (?)
   – Quantum Kolmogorov Complexity
   – A strongly universal QTM

3. Conclusions

1. Classical Theory of Computation: Universal Turing Machines



A Turing machine is a **mathematical model** of a computing device. It is a **triplet** (Σ, Q, δ), where

- Σ is the **alphabet**, e.g. $\Sigma = \underbrace{\{0,1,\#\}}_{\text{input tape}} \times \underbrace{\{0,1,\#\}}_{\text{output tape}}$,

- $Q = \left\{ \underbrace{q_0}_{\textit{start state}}, \; q_1, \; \ldots, \; q_N, \; \underbrace{q_f}_{\textit{final state}} \right\}$ is the set of **internal states**,

- $\delta : \Sigma \times Q \rightarrow \Sigma \times Q \times \{\text{left}, \text{right}\}$ is the **transition function**.

1. Classical Theory of Computation: Universal Turing Machines

- Start of computation: Head at cell 0, control in state q_0, **input** $x \in \{0,1\}^*$ written on input tape.

- Computation: determined by transition function δ

- Halting: Control is in state q_f. $\longrightarrow$ Read **output** $M(x)$ from output tape.

$\Rightarrow$ partial recursive function $M : \{0,1\}^* \to \{0,1\}^*$.

Theorem 1. [Universal Turing Machine] *There is a TM U such that for every TM M there is a constant c_M such that* **for every input** $x \in \{0,1\}^*$ **there is some** $\tilde{x} \in \{0,1\}^*$ *such that*

$$U(\tilde{x}) = M(x)$$

and $\ell(\tilde{x}) \leq \ell(x) + c_M$.

1. Classical Theory of Computation: Kolmogorov Complexity & Invariance

Definition 2. [Kolmogorov Complexity] *Let M be a TM and $s \in \{0,1\}^*$. Then,*

$$C_M(s) := \min\{\ell(x) \mid x \in \{0,1\}^*,\ M(x) = s\}.$$

- C is a measure of **randomness**: The smaller $C_M(s)$, the less random/ more regular is s.
- Important **proof tool**, large theory about C.

Theorem 3. [Invariance] *If U is a universal TM and M is an arbitrary TM, then*

$$C_U(s) \leq C_M(s) + \mathrm{const}_M \qquad (s \in \{0,1\}^*).$$

2. Quantum Computation: Quantum Turing Machines (QTMs)

E. Bernstein, U. Vazirani, "Quantum Complexity Theory", *SIAM Journal on Computing* **26** 1411-1473 (1997): A QTM is a **triplet** (Σ, Q, δ), where

- Σ is the **alphabet**, e.g. $\Sigma = \underbrace{\{0,1,\#\}}_{\text{input tape}} \times \underbrace{\{0,1,\#\}}_{\text{output tape}}$,
- $Q = \left\{ \underbrace{q_0}_{\textit{start state}}, q_1, \ldots, q_N, \underbrace{q_f}_{\textit{final state}} \right\}$ is the set of **internal states**,
- $\delta : \Sigma \times Q \times \Sigma \times Q \times \{\text{left}, \text{right}\} \to \mathbb{C}$ is the **transition amplitude**.

$$\delta(\underbrace{00, q_0}_{\textit{read}}, \underbrace{11, q_1}_{\textit{write}}, \textbf{left}) = \frac{1}{\sqrt{2}} = \delta(00, q_0, 11, q_1, \textbf{right})$$

means: In **superposition** turn **left** *and* **right**.

2. Quantum Computation: Quantum Turing Machines (QTMs)

Inputs and outputs are **qubit strings** $\mathcal{Q}$, i.e. density operators on the Hilbert space $\mathcal{H}_{\{0,1\}^*}$, i.e. on

$$\mathcal{H}_{\{0,1\}^*} = \ell^2(\{\underbrace{\varepsilon, 0, 1, 00, 01, \ldots}_{\textit{orthonormal basis}}\}) = \bigoplus_{n=0}^{\infty} \left(\mathbb{C}^2\right)^{\otimes n}.$$

Example: $\sigma = \frac{1}{2}(|0\rangle + |111\rangle)(\langle 0| + \langle 111|) \in \mathcal{Q}$ is a qubit string of **length** $\ell(\sigma) = 3$.

Definition 4. [Halting of a QTM] *We say that a QTM M* **halts** *at time $T \in \mathbb{N}$ on input $\sigma \in \mathcal{Q}$, iff*

$$\langle q_f | M_{\mathrm{C}}^t(\sigma) | q_f \rangle = \begin{cases} 0 & \textit{if } t < T, \\ 1 & \textit{if } t = T, \end{cases}$$

where $M_{\mathrm{C}}^t(\sigma)$ is the state of the control at time t.

$\Rightarrow$ QTMs are partial maps $M : \mathcal{Q} \to \mathcal{Q}$.

2. Quantum Computation: Universality of QTMs (?)

$$(*) \qquad \langle q_f | M_{\mathrm{C}}^t(\sigma) | q_f \rangle = \begin{cases} 0 & \text{if } t < T \\ 1 & \text{if } t = T \end{cases}$$

There are good reasons for **not** allowing **approximate halting**, i.e. $0 < \langle q_f | M_{\mathrm{C}}^t(\sigma) | q_f \rangle < 1$.

Serious problem:

- QTMs can simulate other QTMs only approximately.
- Thus, halting $(*)$ can **never** be simulated **perfectly**.
- So how can there be a **universal QTM**?

2. Quantum Computation: Universality of QTMs (?)

Bernstein and Vazirani: There is a QTM $\mathcal{U}$ such that for every QTM M there is a string s_M such that

$$\left\| \underbrace{M_{\mathbf{O}}^T(|\psi\rangle)}_{\textit{content of output tape}} - \mathcal{U}(s_M, T, \delta, |\psi\rangle) \right\|_{\mathrm{Tr}} < \delta$$

for every input $|\psi\rangle$, accurary $\delta > 0$ and time $T \in \mathbb{N}$.

- Number of time steps T **given** as input **in advance**.
- $\mathcal{U}$ simulates M **efficiently** (quickly).
- Aim of B&V: Study **computational complexity**: How "fast" are quantum algorithms?
  $\Rightarrow$ Time T known in advance. No problem.

2. Quantum Computation:
Quantum Kolmogorov Complexity

Definition 5. [$\approx$ Berthiaume et. al. 2001] *Let M be a QTM and $\rho \in \mathcal{Q}$ a qubit string.*

$$QC_M(\rho) := \min \left\{ \ell(\sigma) \;\middle|\; \|\rho - M(\sigma, k)\|_{\mathrm{Tr}} \leq \frac{1}{k} \; \forall k \in \mathbb{N} \right\}$$

Question: Is there a **"universal" QTM** U such that for every QTM M

$$QC_U(\rho) \leq QC_M(\rho) + \mathrm{const}_M \qquad (\rho \in \mathcal{Q}) \ ?$$

Bernstein-Vazirani universal QTM $\mathcal{U}$ is **not enough**:
Halting time T can be **very large**; giving T as input **makes the input very long**.
Can we do better?

2. Quantum Computation: A strongly universal QTM

Theorem 6. [M.M., quant-ph/0605030] *There is a QTM U such that for every QTM M and every qubit string $\sigma \in \mathcal{Q}$ there is a $\sigma_M \in \mathcal{Q}$ such that*

$$\|U(\sigma_M, \delta) - M(\sigma)\|_{\mathrm{Tr}} < \delta \qquad (\delta > 0)$$

while $\ell(\sigma_M) \leq \ell(\sigma) + \mathrm{const}_M$.

Corollary 7. [Invariance]
There is a QTM U such that for every QTM M there is a constant $c_M \in \mathbb{N}$ such that

$$QC_U(\rho) \leq QC_M(\rho) + c_M \qquad (\rho \in \mathcal{Q}).$$

Proof is based on thorough **analysis of the halting structure** of input qubit strings: Every input σ can be decomposed into **classical** and **quantum** part (in a non-trivial way).

3. Conclusions

- Turing Machines and Kolmogorov Complexity have **quantum counterparts**.

- There are **different notions of universality** for quantum Turing machines.

- What we have shown: There is a **"strongly universal"** QTM U such that for every QTM M and qubit string $\sigma \in \mathcal{Q}$ there is a $\sigma_M \in \mathcal{Q}$ such that

$$\|U(\sigma_M, \delta) - M(\sigma)\|_{\mathrm{Tr}} < \delta \qquad (\delta > 0)$$

  while $\ell(\sigma_M) \leq \ell(\sigma) + \mathrm{const}_M$.

- Thus, it makes sense to study **quantum Kolmogorov complexity**.

- More information: **quant-ph/0605030**.