# Quantum Turing machines

## Hiddensee meeting on BSS machines and computability

André Nies

August 15, 2016

# Kolmogorov complexity

We survey attempts to introduce an analog of Kolmogorov complexity in the setting of quantum computation. Here is a brief reminder of classical Kolmogorov complexity.

- Fix a universal system of descriptions; say, a universal Turing machine $M$ taking as input bit strings $\sigma$.
- The Kolmogorov complexity of a finite mathematical object $x$ (e.g. a string) is the length of a shortest description, i.e. $\min\{|\sigma| : M(\sigma) = x\}$

# Probabilistic computation

- A computation of a probabilistic TM can be seen as an infinite list of columns. The entries in the columns are labeled with possible configurations of a classic TM; all entries are in $[0, 1]$, with sum of columns 1, and almost all are zero. Column 0: the input configuration has probability 1.
- The transition function is give by a stochastic matrix (entries are probabilities, each row sums to 1) which specifies the distribution in the next column via a function $\delta \colon Q \times \Sigma \to \tilde{\mathbb{R}}^{Q \times \Sigma \times \{L,R\}}$ ($\tilde{\mathbb{R}} =$ polytime computable reals)

# Comparison of probabilistic computation and quantum computation

Taken from paper by Bernstein/Vazirani (1997)

- Computation of a QTM: the $t$-th column is now a vector $(\alpha_1, \alpha_2 \ldots,)$ in $\bigoplus_{\mathbb{N}} \mathbb{C}$ (almost all entries zero) with Euclidean length 1. Upon measurement, at stage $t$ obtain the probability $\alpha_i \bar{\alpha}_i$ for the configuration $i$.

$\tilde{\mathbb{C}}$ is the field of polytime computable complex numbers.

- Given sets $Q$ states, $\Sigma$ alphabet, $q_0, q_f \in Q$ initial/halting state
- Define configurations as usual, e.g. $01q_3110\sqcup$
- Transition function has the form

$$\delta \colon Q \times \Sigma \to \tilde{\mathbb{C}}^{\Sigma \times Q \times \{L,R\}}.$$

- $\mathcal{S}$ is Hilbert space generated by the configurations as an orthonormal base (i.e. a version of $\ell_2$).
- $U_M \colon \mathcal{S} \to \mathcal{S}$ defined in the canonical way (see below) is called time evolution operator.
- restriction on $\delta$ (they call it well-formed) ensures that $U_M$ is unitary. This is proved in the appendix of the paper from basic stuff in Hilbert space theory.

# Defining the time evolution operator $U_M$

We're given $\delta \colon Q \times \Sigma \to \tilde{\mathbb{C}}^{\Sigma \times Q \times \{L,R\}}$.

- Given configuration $c$ let $c_1, \ldots, c_n$ be the configs that can follow it.
- Define $U_M(|c\rangle) = |\sum_i \alpha_i\rangle$, where $c \to c_i$ via an entry $q, s, q', s', X$ in the format of a usual Turing table, and $\delta(q,s)(q',s',X) = \alpha_i$.

In the probabilistic case, do the same thing, now making convex combinations of the configurations.

# Wellformedness

In Lemma 5.3 B/V give three conditions that are necessary and sufficient to ensure that $U_M$ is unitary. Let $u, v$ range over $Q \times \Sigma$

- $\sum |\delta(u)|^2 = 1$ (length at base vectors is 1)
- for $u \neq v$ we have $\delta(u) \cdot \delta(v) = 0$ (orthogonality)
-

# Halting

- It might be that halting configuration could be reached at different steps in superpositions of configurations
- one says that a QTM $M$ halts at stage $t$ if at $t$ all configs with positive probability are in state $q_f$, and before, none is.
- also ask "well behaved": things such as that the head is in the leftmost position
- then the "output" is a probability distribution over various output words

# Quantum Kolmogorov complexity

There are lots of alternative approaches, all from about the time 2000-2008 (nothing after?)

- Berthiaume, van Dam, La Plante 2000: use approach based on QTM of Bernstein/Vazirani
- Vitanyi 2002- also in the 2008 edition of his book
- Gacs 2001: avoids machines altogether rather tries a quantum version of Levin's universal semimeasure. This supposedly combines the advantages of the two approaches above
- Müller 2007 thesis (Berlin): compares the various machine-based approaches, then settles for Berthiaume, except that strings can have indeterminate length.
- Rogers, Nagarajan, Vedral 2008 defines the "second quantized Kolmogorov complexity". Different bounds on $K(xx)$.

We go for Berthiaume et al.

# Fidelity $F(\rho, \tau)$

This is a way to measure the closeness of two states.

- For pure states (i.e., unit vectors in $\mathcal{H}_d$ it is $|\langle \rho, \tau \rangle|$. This is $|\cos \theta|$ where $\theta$ is the angle between $\rho$ and $\tau$.
- for mixed states (positive semidefinite self adjoint operators of trace 1, also called density matrices) it is the maximum fidelity of a pair of "purifications". Explicit formula is

$$F(\rho, \tau) = tr\sqrt{\sqrt{\rho} \cdot \tau \cdot \sqrt{\rho}}.$$

- Clearly $0 \leq F(\rho, \tau) \leq 1$. The quantity $D(\rho, \tau) = 1 - F(\rho, \tau)$ is like a distance, except we only have the weak triangle inequality $D(\rho, \nu) \leq 2(D(\rho, \tau) + D(\tau, \nu))$ (see Berthiaume Lemma 2 in section 3.6).

# Definition of quantum $QC_M^f$ according to Berthiaume et al.

The length of a qbit string $X$, denoted by $\ell(X)$, is the dimension of the smallest Hilbert space (with standard base) that $X$ is in.

For a QTM $M$, by $M(X, Y)$ (double input) one means that input tape is initialised to, say, $|0^{\ell(X)}1XY\$0^\infty\rangle$. Same for multiple.

The general definition for a QTM $M$ and fidelity bound $f$:

$$QC_M^f(X) = \min\{\ell(P) \colon \forall k\, F(X, M(P, 1^k)) \geq f(k)\}.$$

Various options are considered for $f$:

- Perfect: $f = 1$
- fixed $1 - \epsilon$ (constant fidelity)
- then they settle for $f(k) = 1 - 1/k$ because they can prove an invariance theorem in this case. Call this version $QC_M^{\uparrow 1}(X)$.

# Universal QTM according to Bernstein/Vazirani

In Thm. 4 they cite B/V. Use $M^T(X)$ for the result of $U_M$ on $X$ after $T$ steps (which is a state)

## Theorem (Universal QTM with fidelity)

*There is a universal QTM* $\mathbb{U}$ *(with finite classical description) such that: for any QTM* $M$ *with finite classical description* $\bar{M}$*, and any pure state* $X$*,*

$$\forall k \forall T \, [F(\mathbb{U}(\bar{M}, X, 1^k, T), M^T(X)) \geq 1 - 1/k].$$

# Invariance

Looking at the Bernstein/Vazirani proof for the existence of universal QTM they obtain the following (they may need to modify $\mathbb{U}$ a bit).

## Theorem

*For each quantum TM $M$ there is $c_M$ such that* $QC^{\uparrow 1}_{\mathbb{U}}(X) \leq QC^{\uparrow 1}_{M}(X) + c_M$.

Write $QC$ for $QC^{\uparrow 1}_{\mathbb{U}}$.

# Properties of $QC$

- $QC(x) \leq^+ C(x)$ for any classical string $x$. It is open whether the converse holds.
- Something on bounding $QC(xx)$ in terms of $QC(x)$.
- some result saying that lots of strings are incompressible. (This appears to be clearer in Vitanyi's version.)