A Quantum Compression No-Go Theorem

Samuel Epstein
samepst@jptheorygroup.org

January 16, 2024

Abstract

This paper provides a resolution to an open problem from 2001 in [BvL01], which states the Kolmogorov complexity of a string is not more than its quantum Kolmogorov complexity. Thus there are no benefits to using quantum mechanics to compress classical information. The quantitative amount of information in classical sources is invariant to the physical model used.

1 Introduction

A central topic of investigation in computer science is whether leveraging different physical models can change computability and complexity properties of constructs. In a remarkable result, Shor's factoring algorithm uses quantum mechanics to perform factoring in polynomial time. One question is whether quantum mechanics provides benefits to compressing classical information. In this paper, a negative answer is given. This solves open problem 1 in [BvL01]. The (prefix-free) Kolmogorov complexity of a string $x \in \{0,1\}^n$ conditioned on its length is $\mathbf{K}(x|n)$, the size of the smallest program to a classical universal Turing machine that can produce x given n on an auxilliary tape. The quantum Kolmogorov complexity of an n qubit state $|\psi\rangle$, which we call BvL complexity (named after its originators), is $\mathbf{Hbvl}(|\psi\rangle)$, the size of the smallest mixed quantum state input to a universal quantum Turing machine (conditioned on n) that produces $|\psi\rangle$ up to arbitrary fidelity. We first prove the result assuming elementary inputs. Then we prove the harder result, generalizing to arbitrary inputs. The main result is as follows. As shown later in the paper, the inequality is tight.

Theorem. For $x \in \{0,1\}^n$, $\mathbf{K}(x|n) <^+ \mathbf{Hbvl}(|x\rangle \langle x|) + \mathbf{K}(\mathbf{Hbvl}(|x\rangle \langle x|)|n)$.

2 Conventions

We use $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\{0,1\}$, and $\{0,1\}^*$ to denote natural numbers, rational numbers, reals, complex numbers, bits, and finite strings. Let $X_{\geq 0}$ and $X_{>0}$ be the sets of non-negative and of positive elements of X. When it is clear from the context, we will use natural numbers and other finite objects interchangeably with their binary representations. For positive real functions f, by $<^+ f$, $>^+ f$, $=^+ f$, we denote $\leq f + O(1)$, $\geq f - O(1)$, $= f \pm O(1)$. Furthermore, $\stackrel{*}{<} f$, $\stackrel{*}{>} f$ denotes $< O(1) f$ and $> f/O(1)$. The term and $\stackrel{*}{=} f$ is used to denote $\stackrel{*}{>} f$ and $\stackrel{*}{<} f$. $\mathbf{K}(x|y)$ is the prefix free Kolmogorov complexity and $\mathbf{C}(x|y)$ is the plain Kolmogorov complexity.

We use the standard model of qubits used throughout quantum information theory. We deal with finite N dimensional Hilbert spaces $\mathcal{H}_N$, with bases $|\alpha_1\rangle, |\alpha_2\rangle, \ldots, |\alpha_n\rangle$. We assume $\mathcal{H}_{n+1} \supseteq \mathcal{H}_n$ and the bases for $\mathcal{H}_n$ are the beginning of that of $\mathcal{H}_{n+1}$. An n qubit space is denoted by

$\mathcal{Q}_n = \bigotimes_{i=1}^n \mathcal{Q}_1$, where qubit space $\mathcal{Q}_1$ has bases $|0\rangle$ and $|1\rangle$. For $x \in \Sigma^n$ we use $|x\rangle \in \mathcal{Q}_n$ to denote $\bigotimes_{i=1}^n |x[i]\rangle$. The space $\mathcal{Q}_n$ has 2^n dimensions and we identify it with $\mathcal{H}_{2^n}$.

A pure quantum state $|\phi\rangle$ of length n is represented as a unit vector in $\mathcal{Q}_n$. Its corresponding element in the dual space is denoted by $\langle\phi|$. The tensor product of two vectors is denoted by $|\phi\rangle \otimes |\psi\rangle = |\phi\rangle\,|\psi\rangle = |\phi\psi\rangle$. The inner product of $|\psi\rangle$ and $\langle\phi|$ is denoted by $\langle\psi|\phi\rangle$.

The symbol Tr denotes the trace operation. The conjugate transpose of a matrix M is denoted by M^*. Projection matrices are Hermitian matrices with eigenvalues in $\{0, 1\}$. For positive semidefinite matrices, σ and ρ we say $\sigma \leq \rho$ if $\rho - \sigma$ is positive semidefinite. For positive semidefinite matrices A, B, C, if $A \leq B$ then $\mathrm{Tr}AC \leq \mathrm{Tr}BC$. Mixed states are represented by density matrices, which are, self adjoint, positive semidefinite, operators of trace 1. A semi-density matrix has non-negative trace less than or equal to 1.

A number is *algebraic* if it is a root of a polynomial with rational coefficients. A pure quantum state $|\phi\rangle$ and (semi)density matrix σ are called *elementary* if their real and imaginary components have algebraic coefficients. Elementary objects can be encoded into strings or integers and be the output of halting programs. Therefore one can use the terminology $\mathbf{K}(|\phi\rangle)$ and $\mathbf{K}(\sigma)$, and also $\mathbf{m}(|\phi\rangle)$ and $\mathbf{m}(\sigma)$.

We say program $q \in \{0,1\}^*$ lower computes positive semidefinite matrix σ if, given as input to universal Turing machine U, the machine U reads $\leq \|q\|$ bits and outputs, with or without halting, a sequence of elementary semi-density matrices $\{\sigma_i\}$ such that $\sigma_i \leq \sigma_{i+1}$ and $\lim_{i\to\infty} \sigma_i = \sigma$. A matrix is lower computable if there is a program that lower computes it.

3 Gács Complexity

Gács complexity, introduced in [GÓ1], is a construct that will be used in the proof of the main theorem. The Kolmogorov complexity of a string x is equal to, up to an additive factor, $-\log \mathbf{m}(x)$, where $\mathbf{m}$ is the universal lower computable semi-measure. Similarly Gács complexity is defined using the following universal lower computable semi-density matrix, with

$$\boldsymbol{\mu} = \sum_{\text{Eementary } |\phi\rangle \in \mathcal{Q}_n} \mathbf{m}(|\phi\rangle\,|n)\,|\phi\rangle\langle\phi|.$$

The parameter n represents number of qubits used. The Gács complexity of a mixed state σ is defined by

$$\mathbf{Hv}(\sigma) = \lceil -\log \mathrm{Tr}\boldsymbol{\mu}\sigma \rceil.$$

This generalizes the definition $\underline{H}$ in [GÓ1], which was solely over pure states. We use the following notation for pure states, with $\mathbf{Hg}(|\phi\rangle) = \mathbf{Hg}(\,|\phi\rangle\langle\phi|\,)$.

Theorem 1 ([GÓ1]) *Let $q \in \{0,1\}^*$ lower compute semi-density matrix A, relativized to the number of qubits n,. Then $\boldsymbol{\mu} \stackrel{*}{>} \mathbf{m}(q|n)A$.*

Proof. A can be composed into a sum $\sum_i p(i)\,|\psi_i\rangle\,\langle\psi_i|$, where each $|\psi_i\rangle$ is elementary, p is a semi-measure, with $\sum_i p(i) \leq 1$, and p is lower computable from q and n. Thus,

$$A = \sum_i p(i)\,|\psi_i\rangle\,\langle\psi_i| \stackrel{*}{<} \mathbf{m}(p|n)^{-1} \sum_i \mathbf{m}(i|n)\,|\psi_i\rangle\,\langle\psi_i| \stackrel{*}{<} \mathbf{m}(q|n)^{-1} \sum_i \mathbf{m}(i|n)\,|\psi_i\rangle\,\langle\psi_i| \stackrel{*}{<} \boldsymbol{\mu}/\mathbf{m}(q|n).$$

□

Theorem 2 ([Gác01]) $\boldsymbol{\mu}_{ii} \stackrel{*}{=} \mathbf{m}(i|n)$.

Proof. The matrix $\rho = \sum_i \mathbf{m}(i|n) |i\rangle \langle i|$ is lower computable, so $\rho \stackrel{*}{<} \boldsymbol{\mu}$ so $\boldsymbol{\mu}_{ii} \stackrel{*}{>} \mathbf{m}(i|n)$. Furthermore, $f(i) = \langle i| \boldsymbol{\mu} |i\rangle$ is a lower computable semi-measure, so $\mathbf{m}(i|n) \stackrel{*}{>} \boldsymbol{\mu}_{ii}$. □

4 BvL Complexity

In this section, we introduce quantum Kolmogorov complexity, which we call BvL complexity, after its originators. Kolmogorov complexity measures the smallest program to a universal Turing machine that produces a string. Thus it is natural to adapt this notion to defining the complexity of a pure or mixed quantum state ρ to be the shortest program to a universal quantum Turing machine that approximates or produces ρ. This definition was introduced in [BvL01]. Whereas Gács complexity can be thought of as a score of the algorithmic entropy of a state, BvL complexity enjoys a direct interpretation of the amount of resources in quantum mechanics needed to approximate or produce a state.

In this paper, BvL complexity is defined with respect to a universal quantum Turing machine introduced in [Mul08]. This is different than the work in [BvL01], which uses the universal quantum machine from [BV93]. The operation of a quantum Turing machine M can be found in [BV93].

The input and auxilliary tape of M consists of symbols of the type $\Sigma = \{0, 1, \#\}$. The input is an ensemble $\{p_i\}$ of pure states $|\psi_i\rangle$ of the same length n, where $p_i \geq 0$, $\sum_i p_i = 1$, and $p_i \in Q_{\geq 0}$. Each pure state $|\psi_i\rangle$ is a complex linear superposition over all inputs of length n. We first prove the main theorem assuming the inputs are elementary, and then prove the more difficult theorerm with this assumption lifted. Thus the input can be seen as an ensemble of states $|\psi_i \# 000 \ldots\rangle$. This ensemble can be represented as a mixed state ρ of n qubits. The auxilliary tape can contain quantum or classical information. The output tape consists solely of $\{0, 1\}$. The quantum transition function is

$$\delta : Q \times \Sigma^2 \times \{0, 1\} \to \mathbb{C}^{Q \times \Sigma^2 \times \{0,1\} \times \{L,R\}^3}.$$

Note that each complex number must be *computable*. That is the real and imaginary components are computable up to precision 2^{-n} given n. Q is the set of states, Σ is the alphabets on the auxilliary and input tapes, $\{0, 1\}$ is alphabet on the output tape and $\{L, R\}^3$ is the action taken by the three heads. The evolution of M is a computable unitary matrix u_M.

There is a start state $|s_C\rangle$ and a final state $|f_C\rangle$. If there exists a $t \in \mathbb{N}$, where during the operation of M input ρ, the control state $M_C^{t'}(\rho)$ is orthogonal to the final state $|f_C\rangle$ for all $t' < t$, with $\langle f_C| M_C^{t'}(\rho) |f_C\rangle = 0$, and $\langle f_C| M_C^{t}(\rho) |f_C\rangle = 1$, and all the heads of the superpositions are at position n then $M(\rho)$ is defined to be the n qubit mixed state on the output tape. Otherwise it is undefined. Quantum machines are not expected to produce the target states exactly, only an approximation. To measure the closeness of states, the *trace distance* function is used.

Definition 1 (Trace Distance of Quantum States) $D(\sigma, \rho) = \frac{1}{2}\|\sigma - \rho\|_1$, *where* $\|A\|_1 = \mathrm{Tr}\sqrt{A^* A}$. *The trace distance obeys the triangle inequality. Fidelity is* $F(\sigma, \rho) = \left(\mathrm{Tr}\sqrt{\sqrt{\sigma}\rho\sqrt{\rho}}\right)^2$, *With* $F(|\psi\rangle, \sigma) = \langle\psi| \sigma |\psi\rangle$. $1 - \sqrt{F(\rho, \sigma)} \leq D(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)}$.

Theorem 3 ([Mul08]) *There is quantum Turing machine* $\mathfrak{U}$ *such that for every QTM* M *and mixed state* σ *for which* $M(\sigma)$ *is defined, there is mixed state* σ_M *such that*

$$D\left(\mathfrak{U}(\sigma_M, \delta), M(\sigma)\right) < \delta,$$

for every $\delta \in \mathbb{Q}_{>0}$ where the length of σ_M is bounded by $\|\sigma_M\| \leq \|\sigma\| + c_M$, where $c_M \in \mathbb{N}$ is a constant dependent only on M.

One can define the complexity of a state σ with respect to an arbitrary quantum Turing machine.

Definition 2 (BvL Complexity [BvL01]) *The BvL Complexity of mixed state ρ with respect to QTM M and trace distance ϵ is*

$$\mathbf{Hbvl}_M[\epsilon](\rho) = \min_{\sigma}\{\|\sigma\| : D(M(\sigma, n), \rho) < \epsilon\}.$$

The BvL Complexity of mixed state ρ with respect to QTM M is

$$\mathbf{Hbvl}_M(\rho) = \min_{\sigma}\left\{\|\sigma\| : \forall_k, D\left(M\left(\sigma, n, k\right), \rho\right) < \frac{1}{k}\right\}.$$

Due to Theorem 3 and the fact that the trace distance D follows the triangle inequality, using the universal quantum Turing machine $\mathfrak{U}$, one can define the BvL complexity of a quantum state. This differs from the original definition in [BvL01] where the program must achieve any degree of precision.

Theorem 4 ([Mul08]) *For $\delta < \epsilon \in \mathbb{Q}_{>0}$, universal QTM $\mathfrak{U}$, for every QTM M, there is a constant c_M where*

- $\mathbf{Hbvl}_{\mathfrak{U}}[\epsilon](\sigma) < \mathbf{Hbvl}_M[\delta](\sigma) + \mathbf{K}(\epsilon - \delta) + c_M$.
- $\mathbf{Hbvl}_{\mathfrak{U}}(\sigma) < \mathbf{Hbvl}_M(\sigma) + c_M$.

Definition 3 (BvL Complexity)

- $\mathbf{Hbvl}[\epsilon](\sigma) = \mathbf{Hbvl}_{\mathfrak{U}}[\epsilon](\sigma)$.
- $\mathbf{Hbvl}(\sigma) = \mathbf{Hbvl}_{\mathfrak{U}}(\sigma)$.

Proposition 1 *For $k \in \mathbb{N}$, $\mathbf{Hbvl}\left[\frac{1}{k}\right](\sigma|k) \leq \mathbf{Hbvl}(\sigma)$.*

Proof. Let $\mathcal{M}$ be the set of inputs to $\mathfrak{U}$ that realize $\mathbf{Hbvl}\left[\frac{1}{k}\right](\sigma|k)$. Let $\mathcal{N}$ be the set of inputs to $\mathfrak{U}$ that realize $\mathbf{Hbvl}(\sigma)$. Clearly $\mathcal{N} \subseteq \mathcal{M}$. □

5 Elementary Inputs

This section proves the main inequality of the paper assumming the inputs are elementary inputs, that is the coefficients are algebraic. We first lower bound the BvL complexity by Gács complexity. Then we leverage the fact that over strings, Gács complexity is equal to Kolmogorov complexity.

Definition 4 ([BvL01]) *Let $\mathcal{H}^t_{k,n}$ be the smallest linear subspace spanning inputs of size k to $\mathfrak{U}$ (conditioned on n), that produce an output of length n in time t. If $t \neq t'$, then $\mathcal{H}^t_{k,n} \perp \mathcal{H}^{t'}_{k,n}$.*

Proposition 2 *There is a computable trace preserving completely positive map $\Psi^t_{k,n}$ such that for all $|\psi\rangle \in \mathcal{H}^t_{k,n}$, $\mathfrak{U}(|\psi\rangle, n) = \Psi^t_{k,n}(|\psi\rangle)$.*

Proof. The map $\Psi^t_{k,n}$ appends $3t$ 0s to the input tape, and creates an auxilliary and output tape consisting $3t$ 0s. The input, auxilliary, and output tapes are treated as loops. It applies $u_{\mathfrak{U}}$, restricted to the finite tapes, t times to the initial configuration and then performs a partial trace on all but n qubits of the output tape. □

Theorem 5 *Assume the universal quantum Turing machine $\mathfrak{U}$ is restricted to elementary inputs. For pure state $|\psi\rangle \in \mathcal{Q}_n$,* $\mathbf{Hg}(|\psi\rangle) <^+ \mathbf{Hbvl}[\epsilon](|\psi\rangle) + \mathbf{K}(\mathbf{Hbvl}[\epsilon](|\psi\rangle)|n) - 2\log(1-\epsilon)$.

Proof. The proof is a reworking of Theorem 9 in [GÓ1] from definitions $\overline{H}$ and QC to definitions **Hg** and **Hbvl**. It is a more detailed exposition of the proof of Theorem 2 in [Eps20]. We start by noting, without loss of generality, due to [Mul08, ADH97], the coefficients of the transistion function of $\mathfrak{U}$ are all elementary.

For each k, t, and n in $\mathbb{N}$, let $\mathcal{H}^t_{k,n}$ as defined in Definition 4. Let $\mathcal{S}^t_{k,n}$ be the elementary elements of $\mathcal{H}^t_{k,n}$. Let $P^t_{k,n}$ be the projection of minimum rank such that for all $|\phi\rangle \in \mathcal{S}^t_{k,n}$, $\langle\phi| P^t_{k,n} |\phi\rangle = \langle\phi|\phi\rangle$. By definition, $P^t_{k,n}$ is lower computable, uniformly in k, t. This by enumerating $\mathcal{S}^t_{k,n}$ by simulating all elementary inputs $|\phi\rangle$ into $\mathfrak{U}$ and then determining if $|\phi\rangle \in \mathcal{H}^t_{k,n}$ and if so then applying the Gram-Schmidt procedure.

For each k, n, and t, by Proposition 2, there is a completely positive trace preserving map $\Psi^t_{k,n}$, such that for all $|\psi\rangle \in \mathcal{H}^t_{k,n}$, $\Psi^t_{k,n}(|\psi\rangle) = \mathfrak{U}(|\psi\rangle, n)$. Let ρ be a k qubit mixed state consisting of elementary pure states that minimizes $k = \mathbf{Hbvl}[\epsilon](|\psi\rangle)$ in time t, with $\rho \leq P^t_{k,n}$ and $D(\Psi^t_{k,n}(\rho), |\psi\rangle) < \epsilon$. By the definition of trace distance and fidelity, $\langle\psi| \Psi^t_{k,n}(\rho) |\psi\rangle > (1-\epsilon)^2$.

$$\begin{aligned}
\rho &\leq P^t_{k,n} \\
2^{-k}\rho &\leq 2^{-k} P^t_{k,n} \\
\Psi^t_{k,n} 2^{-k}\rho &\leq \Psi^t_{k,n} 2^{-k} P^t_{k,n} \\
\Psi^t_{k,n} 2^{-k}\rho &\leq \sum_t \Psi^t_{k,n} 2^{-k} P^t_{k,n}.
\end{aligned}$$

The semi-density matrix $\sum_t \Psi^t_{k,n} 2^{-k-1} P^t_{k,n}$ is lower computable relative to k, so using Theorem 1,

$$\begin{aligned}
\mathbf{m}(k|n) 2^{-k} \Psi^t_{k,n}\rho \leq \mathbf{m}(k|n) \sum_t \Psi^t_{k,n} 2^{-k} P^t_{k,n} &\stackrel{*}{<} \boldsymbol{\mu} \\
\mathbf{m}(k|n) 2^{-k} \langle\psi| \Psi^t_{k,n}(\rho) |\psi\rangle &\stackrel{*}{<} \langle\psi| \boldsymbol{\mu} |\psi\rangle \\
k + \mathbf{K}(k|n) - 2\log(1-\epsilon) &>^+ \mathbf{Hg}(|\psi\rangle).
\end{aligned}$$

□

Corollary 1 *Assume the universal quantum Turing machine $\mathfrak{U}$ is restricted to elementary inputs.* $\mathbf{Hg}(|\psi\rangle) <^+ \mathbf{Hbvl}(|\psi\rangle) + \mathbf{K}(\mathbf{Hbvl}(|\psi\rangle)|n)$.

Proof. From Theorem 5,

$$\mathbf{Hg}(|\psi\rangle\,|2) <^+ \mathbf{Hbvl}[1/2](|\psi\rangle) + \mathbf{K}(\mathbf{Hbvl}[1/2](|\psi\rangle), 1/2|n, 2).$$

From Propositions 1 and 3,

$$\mathbf{Hg}(|\psi\rangle) <^+ \mathbf{Hbvl}(|\psi\rangle) + \mathbf{K}(\mathbf{Hbvl}(|\psi\rangle)|n).$$

□

Proposition 3 *For every c, there is a c' such that if $a < b + c$ then $a + \mathbf{K}(a) < b + \mathbf{K}(b) + c'$.*

Proof. So $\mathbf{K}(a - b) < 2\log c + O(1)$. So $\mathbf{K}(a) < \mathbf{K}(b) + 2\log c + O(1)$. Assume not, then $b - a + c' < \mathbf{K}(a) - \mathbf{K}(b) + O(1) < 2\log c + O(1)$, which is a contradiction for $c' > 2\log c + O(1)$.□

Up to logarithmic precision, the Kolmogorov complexity of a string is equal to its BvL complexity. Note that the lower and upper bounds are tight because $\mathbf{Hbvl}(|x\rangle\langle x|) <^+ \mathbf{C}(x|n)$ and the bound $\mathbf{K}(x|n) <^+ \mathbf{C}(x|n) + \mathbf{K}(\mathbf{C}(x|n)|n)$ is tight.

Theorem 6 *Assume the universal quantum Turing machine $\mathfrak{U}$ is restricted to elementary inputs. For $x \in \{0,1\}^n$,*

$$\begin{aligned}\mathbf{Hbvl}(|x\rangle\langle x|) &<^+ \mathbf{C}(x|n),\\ \mathbf{K}(x|n) &<^+ \mathbf{Hbvl}(|x\rangle\langle x|) + \mathbf{K}(\mathbf{Hbvl}(|x\rangle\langle x|)|n).\end{aligned}$$

Proof. The lower bound comes from [BvL01] which noted the fact that the universal quantum Turing machine $\mathfrak{U}$ can simulate any classical (non-prefix) Turing machine. For the upper bound, by Theorem 2 and Corollary 1,

$$\mathbf{K}(x|n) =^+ \mathbf{Hg}(|x\rangle\langle x|) <^+ \mathbf{Hbvl}(|x\rangle\langle x|) + \mathbf{K}(\mathbf{Hbvl}(|x\rangle\langle x|)|n).$$

□

6 Arbitrary Inputs

This section proves the results of Section 5 with the elementary input restriction lifted. However while Section 5 treats the universal quantum Turing machine $\mathfrak{U}$ as a black box, this section leverages properties of $\mathfrak{U}$, adding to the complexity of the main proof. Thus, instead of copying large sections of the text, the reader is assumed to be familiar with the contents of [Mul08], and terms from that paper will be directly referenced in this section.

Generally speaking, valid inputs of size m to $\mathfrak{U}$ are of the form $|x\rangle\langle x| \otimes \mathcal{Q}_k$. The classical portion consists of two parts $x = yz$. The first part y is an input to a fixed classical universal Turing machine which is expected to output (M, δ) a classical description of the QTM M to simulate, and a precision parameter $\delta \in \mathbb{Q}_{>0}$. The description of M contains a collection of algorithms that compute the transistion amplitudes. The second part z is a prefix free coding of a time amount τ.

After the classical portion, there is an arbitrary pure state $|\psi\rangle$ of size $n = m - \|x\|$. The QTM $\mathfrak{U}$ expects inputs of thus form. Such inputs are considered *valid*. We do not consider inputs that are not valid. Invalid inputs are not considered with respect to BvL complexity, **Hbvl**.

The universal QTM $\mathfrak{U}$ performs an approximation of a unitary transform on $|\psi\rangle$ producing $|\phi\rangle$ then, using results from [BV93], simulates $|\phi\rangle$ on M for τ steps then outputs its results. Note that in the following theorem m is the length of the pure state, not n.

Theorem 7 *For $|\psi\rangle \in \mathcal{Q}_m$, $\mathbf{Hg}(|\psi\rangle) <^+ \mathbf{Hbvl}[\epsilon](|\psi\rangle) + \mathbf{K}(\mathbf{Hbvl}[\epsilon](|\psi\rangle)|m) - 2\log(1-\epsilon)$.*

Proof. Let $k = \mathbf{Hbvl}[\epsilon](|\psi\rangle)$. We define the following algorithm A that on input (k, m), lower computes an m qubit semi-density matrix. It iterates over all strings x not greater than k and send (x, k, m) to algorithm B and simulates B on all the inputs in parallel. Algorithm B is possibly non-halting, but if it does halt then it will return (Ψ_x, P_x), where P_x is a k qubit projection matrix

and Ψ_x is a trace-preserving quantum operation taking k qubit inputs to m qubit inputs. When B halts on an input, algorithm A adds $2^{-k}\Psi_x(P_x)$ to a sum. Thus A lower computes a semi-density matrix.

Algorithm B first feeds x to a classical prefix-free universal Turing machine U. If some prefix of $y \sqsubset x$ causes U to output (M, δ), where M is a well formed QTM M, and $\delta \in \mathbb{Q}_{>0}$ then let $n = k - \|y\|$, which is the length of the input to send to M after some operations are performed. Let $yz = x$. The precision parameter δ is the same as the one specified as input to the algorithm of $\mathfrak{U}$ in [Mul08].

For all t, starting at $t = 1$ and $i = 1$ compute a description of $\mathcal{H}_M^{(n,\epsilon_0)}(t)$. If $\mathrm{Dim}\left(\mathcal{H}_M^{(n,\epsilon_0)}(t)\right) = 0$ then increment t and start again. Determine the length of its associated codeword $\ell_i^{(M,n)}$ and its corresponding "blind prefix code word" $c_i^{(M,n)}$. If $c_i^{(M,n)} = z$, then set the number of steps $\tau = t$, otherwise increment t and i and start again. Note that this process is potentially non-halting for certain z.

Set $P_x = |x\rangle\langle x| \otimes \mathcal{Q}_{k-\|x\|}$. Now what remains is to determine Ψ_x. Ψ_x starts off with a partial trace, removing the first part of the input of size $\|x\|$. Then it performs an elementary operation $\mathcal{D}$ defined in the following way. Let $\{|u_i\rangle\}$ be the basis vectors of $\mathcal{H}_M^{(n,\epsilon_0)}(\tau)$ and $\{|v_i\rangle\}$ be the canonical basis vectors of $\mathcal{Q}_{\lceil \log \mathrm{Dim}(\mathcal{H}_M^{(n,\epsilon_0)})\rceil}$. Then $\mathcal{D}$ is an elementary operation defined by linear extension of $\mathcal{D}|v_i\rangle = |u_i\rangle$. Add the $\mathcal{D}$ operation to the end of the map Ψ_x.

Compute an elementary unitary transform V that has the same properties as the unitary approximation V in the proof of Theorem 1.1 in [Mul08]. The reason that a full unitary operation can be used is that algebraic coefficients are being used, whereas in [Mul08], rational coefficients are used. Append V to the end of Ψ.

The last part is to simulate M for τ time steps by using an approximation of the unitary matrix u_M. We first describe an algorithm C that given M, $\gamma \in \mathbb{Q}_{>0}$, constructs an approximation $\tilde{u}_M$ such that for all $|\psi\rangle \in \mathcal{Q}_n$, $D(u_M|\psi\rangle, \tilde{u}_M|\psi\rangle) < \gamma$. Note that if the algorithms to compute the amplitudes of the transistion functions of M are not halting then algorithm C will be non-halting. First cover $\mathbb{Q}_n$ by elementary pure states $|\phi\rangle \in Q$, such that $\max_{|\psi\rangle\in\mathcal{Q}_n} \min_{|\phi\rangle\in Q} D(|\psi\rangle, |\phi\rangle) < \gamma/3$. Next run the algorithms to compute the transistion functions long enough to produce unitary matrix $\tilde{u}_M$ such that for all $|\phi\rangle \in Q$, $D(u_M|\phi\rangle, \tilde{u}_M|\phi\rangle) < \gamma/3$. This is possible because the amplitudes of the transition function can be computed to any accuracy. Thus for any $|\psi\rangle \in \mathcal{Q}_n$, for proper choice of $|\phi\rangle \in Q$

$$\begin{aligned} D(u_M|\psi\rangle, \tilde{u}_M|\psi\rangle) &< D(u_M|\psi\rangle, u_M|\phi\rangle) + D(u_M|\phi\rangle, \tilde{u}_M|\phi\rangle) + D(\tilde{u}_M|\phi\rangle, \tilde{u}_M|\psi\rangle) \\ &< D(|\psi\rangle, |\phi\rangle) + \gamma/3 + D(|\phi\rangle, |\psi\rangle) \\ &< \gamma. \end{aligned}$$

If $\tilde{u}_M$ is run twice with any input $|\psi\rangle \in \mathcal{Q}_n$, the error is bounded by

$$\begin{aligned} D(\tilde{u}_M^2|\psi\rangle, u_M^2|\psi\rangle) &< D(\tilde{u}_M^2|\psi\rangle, \tilde{u}_M u_M|\psi\rangle) + D(\tilde{u}_M u_M|\psi\rangle, \tilde{u}_M^2|\psi\rangle) \\ &< \gamma + D(u_M|\psi\rangle, \tilde{u}_M|\psi\rangle) \\ &< 2\gamma. \end{aligned}$$

With similar reasoning, one can see that running $\tilde{u}_M$ a total of ℓ times will produce a maximum error of $\gamma\ell$. Thus algorithm B uses algorithm C with parameters M, $\delta/3\tau$ to produce an elementary unitary approximation $\tilde{u}_M$. Using the same arguments in Proposition 2, we construct an τ-time simulation of M, using unitary transform $\tilde{u}_M$ as the approximation of the transistion function. This

simulation unitary transform is added to the end of the output. Finally a partial trace is added, factoring all but m qubits from the output. This is added to the end of the output.

So the output of algorithm A can be seen as $2^{-k}\sum_{x,\|x\|<m}\Psi_x(P_x)$. Let mixed state σ realize $\mathbf{Hbvl}[\epsilon](|\psi\rangle)$. Assuming the input is valid, σ can rewritten as $\sum_x a_x\sigma_x$ where $\sigma_x \leq P_x$, where all but finitely many a_x are zero. By the definition of trace distance and fidelity, $\langle\psi|\sum_x a_x\Psi_x(\sigma_x)|\psi\rangle > (1-\epsilon)^2$. So we get, similarly to the proof of Theorem 6,

$$\begin{aligned}
\mathbf{m}(k|m)\sum_x 2^{-k}\Psi_x(P_x) &\overset{*}{<} \boldsymbol{\mu}\\
\mathbf{m}(k|m)2^{-k}\sum_x a_x\Psi_x(\sigma_x) &\overset{*}{<} \boldsymbol{\mu}\\
\mathbf{m}(k|m)2^{-k}\langle\psi|\left(\sum_x a_x\Psi_x(\sigma_x)\right)|\psi\rangle &\overset{*}{<} \langle\psi|\boldsymbol{\mu}|\psi\rangle\\
k+\mathbf{K}(k|m)-2\log(1-\epsilon) &>^+ \mathbf{Hg}(|\psi\rangle).
\end{aligned}$$

□

Theorem 8 *For $x\in\{0,1\}^n$,*

$$\begin{aligned}
\mathbf{Hbvl}(|x\rangle\langle x|) &<^+ \mathbf{C}(x|n),\\
\mathbf{K}(x|n) &<^+ \mathbf{Hbvl}(|x\rangle\langle x|)+\mathbf{K}(\mathbf{Hbvl}(|x\rangle\langle x|)|n).
\end{aligned}$$

Proof. This is due to Theorem 7 and using the same reasoning in Theorem 6. □

References

[ADH97] L. Adleman, J. DeMarrais, and M. Huang. Quantum computability. *SIAM Journal on Computing*, 26(5):1524–1540, 1997.

[BV93] E. Bernstein and U. Vazirani. Quantum complexity theory. In *Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing*, page 11–20, New York, NY, USA, 1993. Association for Computing Machinery.

[BvL01] A. Berthiaume, W. van Dam, and S. Laplante. Quantum Kolmogorov Complexity. *Journal of Computer and System Sciences*, 63(2), 2001.

[Eps20] Samuel Epstein. An extended coding theorem with application to quantum complexities. *Information and Computation*, 275, 2020.

[GÓ1] P. Gács. Quantum Algorithmic Entropy. *Journal of Physics A Mathematical General*, 34(35), 2001.

[Mul08] M. Muller. Strongly Universal Quantum Turing Machines and Invariance of Kolmogorov Complexity. *IEEE Transactions on Information Theory*, 54(2), 2008.