The Quantum Kolmogorov Complexity of Strings Revisited

Samuel Epstein
samepst@jptheorygroup.org

January 25, 2024

Abstract

Due to [Mue07, Mul09], the Kolmogorov complexity of a string was shown to be equal to 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. These consequences make this theorem arguably the most important result in the intersection of algorithmic information theory and physics. The original proof is quite extensive. This paper contains a simpler proof of this theorem as well as new bounds relating Kolmogorov complexity and error bounded quantum Kolmogorov complexity.

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 [Mue07, Mul09], a negative answer was given, solving open problem 1 in [BvL01]. The (plain) Kolmogorov complexity of a string x is the size of the smallest program to a classical universal Turing machine that can produce x. The quantum Kolmogorov complexity of an pure state $|\psi\rangle$, which we call BvL complexity (named after its originators [BvL01]), is $\mathbf{Hbvl}(|\psi\rangle)$, the size of the smallest mixed quantum state input to a universal quantum Turing machine that produces $|\psi\rangle$ up to arbitrary fidelity. We provide a new simpler proof to the following main result, which is as follows

Theorem. ([Mue07, Mul09])

$$\mathbf{C}(x) =^+ \mathbf{Hbvl}(|x\rangle \langle x|).$$

The term $\mathbf{K}$ is the prefix-free Kolmogorov complexity. The complexity $\mathbf{Hbvl}[\epsilon](|\psi\rangle)$ is BvL complexity where the output is within trace distance ϵ to the target state. We also provide the following new result in this paper.

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

$$\mathbf{K}(x|n) <^+ \mathbf{Hbvl}[\epsilon](|x\rangle \langle x| \, |n) + \mathbf{K}(\mathbf{Hbvl}[\epsilon](|x\rangle \langle x| \, |n), \epsilon|n) - \log(1-4\epsilon).$$

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 score of the algorithmic entropy of a pure or mixed state. 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 ([GÓ1]) $\boldsymbol{\mu}_{ii} \stackrel{*}{=} \mathbf{m}(i|n)$.

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

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] and we call it BvL complexity. BvL complexity enjoys a direct interpretation of the amount of resources in quantum mechanics needed to approximate or produce a state.

All quantum Turing machines used in this paper are the well formed QTMs defined in [BV93]. Well formed QTM preserve length and their time evolution is unitary. In this manuscript, 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 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. 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. 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. One might argue that this definition with regard to the halting state is too restrictive, but as shown [Mue07], for every input σ to a QTM that almost halts, there is another state σ' such that $\|\sigma'\| <^+ \|\sigma\|$ that makes the universal QTM $\mathfrak{U}$ halt perfectly.

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 and Fidelity off Quantum States) *Trace distance is* $D(\sigma,\rho) = \frac{1}{2}\|\sigma-\rho\|_1$*, 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* $F(|\psi\rangle,\sigma) = \langle\psi|\,\sigma\,|\psi\rangle$*.* $1 - F(\rho,|\psi\rangle) \leq D(\rho,|\psi\rangle)$*.*

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*

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

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*

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

Definition 3 (BvL Complexity)

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

5 BvL Complexity and Gács Complexity

Lemma 1 ([BvL01]) *If $F(\sigma,\sigma) > 1-\delta$ and $F(\sigma',\sigma'') > 1-\epsilon$, then $F(\sigma,\sigma'') \geq 1-2\delta-2\epsilon$.*

Remark 1 *Let $\mathcal{H}_k^t$ be the linear subspace of k qubit inputs to the universal QTM $\mathfrak{U}$ that halts in time t. Due to [Mul08], if $t \neq t'$, then $\mathcal{H}_k^t \perp \mathcal{H}_k^{t'}$. Let $\mathcal{H}_{k,n}^t$ be the subspace of $\mathcal{H}_k^t$ whose outputs are of size n. If $n \neq n'$ then $\mathcal{H}_{k,n}^t \perp \mathcal{H}_{k,n'}^t$.*

Lemma 2 *Given t,k,n,δ one can compute an elementary quantum operation $\Psi_{k,n}^{t,\delta} : \mathcal{Q}_k \to \mathcal{Q}_n \oplus \mathcal{Q}_1$ such that if $\sigma \in \mathcal{H}_{k,n}^t$ then $F(\Psi_{k,n}^{t,\delta}(\sigma), \mathfrak{U}(\sigma)) > 1-\delta$. Let $|\psi\rangle$ be perpendicular to $\mathcal{H}_{k,n}^t$. Then $\mathrm{Tr}P\Psi_{k,n}^{t,\delta}(|\psi\rangle) \leq \delta$, where P projects out the $|\#\rangle$ subspace.*

Proof. Let $\Psi = \Psi_{k,n}^{t,\delta}$. The quantum operation Ψ starts by first applying quantum operation $\mathcal{E}_1$, which appends $2t$ spaces to the auxiliary, input, and output tape, and then treating the tapes as loops. Then it applies the approximating elementary unitary matrix $\tilde{u}$ corresponding to $\mathfrak{U}$ (with shortened tapes) t times. Then it applies quantum operation $\mathcal{E}_2$, which projects all configuratons in the halting state $|q_f\rangle$ with a head position at n to the first n output blocks and projects the rest to $|\#\rangle$. So $\Psi(\sigma) = \mathcal{E}_2(\tilde{u}^t\mathcal{E}_1(\sigma)\tilde{u}^{t*})$. It remains to determine the approximation matrix $\tilde{u}$.

Let $\mathcal{Q}$ be the finite configuration space. Let γ be a parameter to be determined later. First cover $\mathcal{Q}$ by elementary mixed states $\rho \in Q$, such that $\min_{\sigma\in\mathcal{Q}} \max_{\rho\in Q} F(\sigma,\rho) > 1-\gamma$. Next run the algorithm to compute the transistion function of $\mathfrak{U}$ long enough to produce unitary matrix $\tilde{u}$ such that for all $\rho \in Q$, $F(u\rho u^*, \tilde{u}\rho\tilde{u}^*) > 1-\gamma$. This is possible because the amplitudes of the transition function of $\mathfrak{U}$ can be computed to any accuracy. Thus for any $\sigma \in \mathcal{Q}$, for proper choice of $\rho \in Q$, due to Lemma 1,

$$\begin{aligned}
F(u\sigma u^*, \tilde{u}\rho\tilde{u}^*) &\geq 1 - 2(1 - F(u\sigma u^*, u\rho u^*)) - 2(1 - F(u\sigma u^*, \tilde{u}\rho\tilde{u}^*) \\
&\geq 1 - 2(1 - F(\sigma,\rho)) - 2(1 - F(u\rho u^*, \tilde{u}\,|\rho\rangle\,\tilde{u}^*) \\
&\geq 1 - 4\gamma. \\
F(u\sigma u^*, \tilde{u}\sigma\tilde{u}^*) &\geq 1 - 2(1 - F(u\sigma u^*, \tilde{u}\rho\tilde{u}^*)) - 2(1 - F(\tilde{u}\rho\tilde{u}^*, \tilde{u}\sigma\tilde{u}^*)) \\
&\geq 1 - 8\gamma - 2(1 - F(\rho,\sigma)) \\
&\geq 1 - 10\gamma.
\end{aligned}$$

Using this result, some tedious math shows how to pick γ such that for all $\sigma \in \mathcal{Q}_k$,

$$F(u^t\mathcal{E}_1(\sigma)u^{t*}, \tilde{u}^t\mathcal{E}_1(\sigma)\tilde{u}^{t*}) > 1-\delta. \tag{1}$$

If $\sigma \in \mathcal{H}_{k,n}^t$, then $\mathcal{E}_2(u^t\mathcal{E}_1(\sigma)u^{t*}) = \mathfrak{U}(\sigma)$, so

$$\begin{aligned}
1-\delta &\leq F(u^t\mathcal{E}_1(\sigma)u^{t*}, \tilde{u}^t\mathcal{E}_1(\sigma)\tilde{u}^{t*}) \\
&\leq F(\mathcal{E}_2(\tilde{u}^t\mathcal{E}_1(\sigma)\tilde{u}^{t*}), \mathcal{E}_2(u^t\mathcal{E}_1(\sigma)u^{t*})) \\
&= F(\Psi(\sigma), \mathfrak{U}(\sigma)).
\end{aligned}$$

Let $|\psi\rangle$ be perpendicular to $\mathcal{H}_{k,n}^t$ and $\rho = \Psi(|\psi\rangle\langle\psi|)$. Thus $\xi = u^t\mathcal{E}_1(|\psi\rangle\langle\psi|)u^{t*}$ will have no superpositions with a configuration in the halting state and the output head at n. From Equation 1 we have $F(\xi, \tilde{u}^t\mathcal{E}_1(|\psi\rangle\langle\psi|)\tilde{u}^{t*}) > 1-\delta$. So

$$1-\delta \leq F(\mathcal{E}_2(\xi),\rho) = F(|\#\rangle\langle\#|,\rho) = \langle\#|\,\rho\,|\#\rangle = 1 - \mathrm{Tr}P\rho,$$

where P projects out the subspace containing $|\#\rangle$. □

Corollary 1 $\mathrm{Tr}P\Psi^{t,\delta}_{k,n}(I_k) \leq \mathrm{Dim}\left(\mathcal{H}^t_{k,n}\right) + \delta 2^k$, *where* I_k *is the* 2^k *dimension identity matrix and* P *projects out* $|\#\rangle$.

Proof. Let Q be the projector onto $\mathcal{H}^t_{k,n}$. Let $R = I_k - Q$. Let $\sum_{i=1}^{\mathrm{Tr}R} |\psi_i\rangle$ be states that span the space perpendicular to $\mathcal{H}^t_{k,n}$. So, due to Lemma 2,

$$\begin{aligned}\mathrm{Tr}P\Psi^{t,\delta}_{k,n}(I_k) &\leq \mathrm{Tr}P\Psi^{t,\delta}_{k,n}(R) + \mathrm{Tr}P\Psi^{t,\delta}_{k,n}(Q)\\ &\leq \sum_i \mathrm{Tr}P\Psi^{t,\delta}_{k,n}(|\psi_i\rangle) + \mathrm{Tr}Q\\ &\leq \delta 2^k + \mathrm{Tr}Q.\end{aligned}$$

□

Theorem 5 *For* $|\psi\rangle \in \mathcal{Q}_m$, $\mathbf{Hg}(|\psi\rangle) <^+ \mathbf{Hbvl}^\epsilon(|\psi\rangle) + \mathbf{K}(\mathbf{Hbvl}^\epsilon(|\psi\rangle), \epsilon|n) - \log(1-4\epsilon)$.

Proof. Let $k = \mathbf{Hbvl}^\epsilon(|\psi\rangle)$. Let σ realize $\mathbf{Hbvl}^\epsilon(|\psi\rangle)$, where $\rho = \mathfrak{U}(\sigma)$ in s steps, and $D(\rho, |\psi\rangle) < \epsilon$. So $F(|\psi\rangle, \rho) = \langle\psi|\rho|\psi\rangle > 1-\epsilon$. Construct the following lower computable semi-density matrix, with $\nu = 2^{-k-1}\sum_t P\Psi^{t,\delta(t,\epsilon)}_{k,n}(I_k)P$, where P projects out the $|\#\rangle$ subspace, I_k is the k qubit identity matrix, and $\delta(t,\epsilon) = \min\{\epsilon, 2^{-t}\}$. So due to Corollary 1, $\mathrm{Tr}\nu \leq 2^{-k-1}(\sum_t \mathrm{Dim}(\mathcal{H}^t_{k,n}) + \min\{\epsilon, 2^{-t}\}2^k) \leq 1$. So due to Lemma 2, if $\xi = \Psi^{s,\delta(n,s,\epsilon)}_{k,n}(\sigma)$, then $F(\xi,\rho) > 1-\epsilon$. So, using reasoning analagous to Theorem 9 in [Gác01],

$$\begin{aligned}\mathbf{m}(k,\epsilon|n)\nu \overset{*}{<} \mathbf{m}(k,\epsilon|n)P\sum_{n,t} 2^{-k}P\Psi^{t,\delta(t,\epsilon)}_{k,n}(I_k)P &\overset{*}{<} \boldsymbol{\mu}\\ \mathbf{m}(k,\epsilon|n)2^{-k}P\Psi^{s,\delta(s,\epsilon)}_{k,n}(\sigma)P &\overset{*}{<} \boldsymbol{\mu}\\ \mathbf{m}(k,\epsilon|n)2^{-k}\langle\psi|P\xi P|\psi\rangle &\overset{*}{<} \langle\psi|\boldsymbol{\mu}|\psi\rangle.\end{aligned}$$

Since $|\langle\psi|\#\rangle^2| = 0$, $\langle\psi|P\xi P|\psi\rangle = \langle\psi|\xi|\psi\rangle$. Since $F(\xi,\rho) > 1-\delta$ and $F(\rho,|\psi\rangle) > 1-\delta$, by Lemma 1, $F(\xi,\psi) > 1-4\delta$. So

$$\begin{aligned}\mathbf{m}(k,\epsilon|n)2^{-k}(1-4\epsilon) &\overset{*}{<} \langle\psi|\boldsymbol{\mu}|\psi\rangle,\\ k + \mathbf{K}(k,\epsilon|n) - \log(1-4\epsilon) &>^+ \mathbf{Hg}(|\psi\rangle).\end{aligned}$$

□

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

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

Corollary 2 $\mathbf{Hg}(|\psi\rangle) <^+ \mathbf{Hbvl}(|\psi\rangle|n) + \mathbf{K}(\mathbf{Hbvl}(|\psi\rangle|n)|n)$.

Proof. From Theorem 5,

$$\mathbf{Hg}(|\psi\rangle\,|8) <^{+} \mathbf{Hbvl}^{\frac{1}{8}}(|\psi\rangle) + \mathbf{K}(\mathbf{Hbvl}^{\frac{1}{8}}(|\psi\rangle), 1/8|n, 8) - \log(1 - 4/8)$$

From Propositions 1 and 2,

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

□

Proposition 2 *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 $c' > 2\log c + O(1)$.□

6 BvL Complexity and Kolmogorov Complexity

One question is whether quantum mechanics provides benefits to compressing classical information. This section answers this question in the negative: there are no such benefits. The quantitative amount of information in classical sources is invariant to the physical model used. This section details the work of [Mue07, Mul09, Gác01], which proves that plain and prefix-free Kolmogorov complexity was shown to equal BvL complexity of classical strings. The proof to Theorem 6 in [Mue07, Mul09] is quite extensive; we present a shortened version.

6.1 Prefix Free Complexity

Corollary 3 *For $x \in \{0,1\}^n$,*

(1) $\mathbf{K}(x|n) <^{+} \mathbf{Hbvl}^{\epsilon}(|x\rangle\langle x|\,|n) + \mathbf{K}(\mathbf{Hbvl}^{\epsilon}(|x\rangle\langle x|\,, |n), \epsilon|n) - \log(1 - 4\epsilon)$,

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

Proof. (1) and (2) comes from Theorems 2, 5, and Corollary 2. □

6.2 Plain Complexity

The following proof is a shortening of the one found in [Mue07].

Theorem 6 ([Mue07, Mul09]) $\mathbf{C}(x) =^{+} \mathbf{Hbvl}(|x\rangle\langle x|)$.

Proof. $\mathbf{Hbvl}(|x\rangle) <^{+} \mathbf{C}(x)$ because a quantum Turing machine can simulate a Turing machine. Let $k = \mathbf{Hbvl}(|x\rangle\langle x|)$. Let the precision parameter be $j = 2^{k+6}$. Let $\Psi^{a,b}_{c,d}(\cdot|j)$ be equal to th definition of $\Psi^{a,b}_{c,d}(\cdot)$, except the universal QTM $\mathfrak{U}$ has j on the auxilliary tape. Let $N^t_n = \Psi^{t,\delta(t,n)}_{k,n}(I_k|j)$, where $\delta(t,n) = \min\{j^{-1}, 2^{-t-n}\}$. Let $O^t_n = QN^t_nQ$, where Q projects out the subspace containing $|\#\rangle$. So due to Corollary 1,

$$\sum_{t,n} \mathrm{Tr}O^t_n \leq \sum_{t,n} (\mathrm{Dim}(\mathcal{H}^t_{k,n}) + (2^{-t-n}2^k) \leq 2^{k+1}.$$

Assume there is some $|\psi\rangle \in \mathcal{Q}_n$, $\sigma \in \mathcal{H}^t_{k,n}$ such that $D(\rho, |\psi\rangle) < j^{-1}$, where $\rho = \mathfrak{U}(\sigma, j)$. Thus due to the definition of trace distances, $F(\rho, |\psi\rangle) = \langle\psi| \rho |\psi\rangle > 1 - j^{-1}$. Let $\xi = \Psi^{t,\delta(t,n)}_{k,n}(\sigma|j)$, where $\xi \leq N^t_n$ and $Q\xi Q \leq O^t_n$. Due to Lemma 2, $F(\rho, \xi) \geq 1 - j^{-1}$. Thus due to Lemma 1, $F(\xi, |\psi\rangle) = \langle\psi| \xi |\psi\rangle \geq 1 - 4j^{-1} = 1 - 2^{-k-4}$. Since $|\langle\psi|\#\rangle^2| = 0$, $\langle\psi| O^t_n |\psi\rangle \geq \langle\psi| Q\xi Q |\psi\rangle = \langle\psi| \xi |\psi\rangle \geq 1 - 2^{-k-4}$.

For each O^t_n we define a an n qubit projection P^t_n. If $O^t_n = \sum_i v_i |e_i\rangle \langle e_i|$ for some orthonormal basis $\{|e_i\rangle\}$ then $P^t_n = \sum_i [v_i \geq 1/2] |e_i\rangle \langle e_i|$. So $\sum_{t,n} \mathrm{Tr} P^t_n \leq 2^{k+2}$. Furthermore, some simple math shows that if $\langle\psi| O^t_n |\psi\rangle \geq 1 - 2^{-k-4}$ then $\langle\psi| P^t_n |\psi\rangle \geq 1 - 2^{-k-2}$.

So with $|\psi\rangle = |x\rangle$ we have $\langle x| P^t_n |x\rangle \geq 1 - 2^{-k-2}$. By Lemma 3, there are only at most $2\mathrm{Tr} P^t_n$ classical states $|y\rangle$, $y \in \{0,1\}^n$, with $\langle y| P^t_n |y\rangle \geq 1 - 2^{-k-2}$. Thus there only at most 2^{k+3} classical strings $|y\rangle$ such that there is a k qubit state, such that $D(\mathfrak{U}(\rho, j), |y\rangle) < j^{-1}$.

So we define an algorithm that takes in a $k+3$ bit number b. For all t and n, it enumerates N^t_n, O^t_n, and then P^t_n. Then it determines the set $\{|y\rangle\}$ for classical strings $y \in \{0,1\}^n$ such that $\langle y| P^t_n |y\rangle > 1 - 2^{-k-2}$. If $|y\rangle$ is the bth state discovered with this condition, then return y. By the definition of k, there is a k qubit input ρ such that $D(\mathfrak{U}(\rho, j), |x\rangle) < 1/j$, x will be returned for proper choice of b. So $\mathbf{C}(x) <^+ \mathbf{Hbvl}(|x\rangle)$. □

Proposition 3 ([Tao]) *Let $v_1, \ldots, v_m$ be unit vectors in an n dimensional complex linear subspace such that $|\langle v_i, v_j\rangle| \leq \frac{1}{2n^{1/2}}$ for all distinct i, j. Then $m < 2n$.*

Proof. Suppose for contradiction $m \geq 2n$. We consider the $2n \times 2n$ Gram matrix $(\langle v_i, v_j\rangle)$, $1 \leq i, j \leq 2n$. This matrix is positive semi-definite with rank at most n. Thus if one subtracts off the identity matrix, it has an eigenvalue of -1 with multiplicity at least n. Taking Hilbert-Schmidt norm, we conclude

$$\sum_{1 \leq i,j \leq 2n; i \neq j} |\langle v_i, v_j\rangle|^2 \geq n.$$

But by hypothesis, the left-hand side is at most $2n(2n-1)\frac{1}{4n} = n - \frac{1}{2}$, giving the desired contradiction. □

Lemma 3 *For a rank m projection matrix P in $\mathbb{C}^n$, assume there is a orthonormal set $\{|e_i\rangle\}_{i=1}^N$ such that $\langle e_i| P |e_i\rangle > 1 - 1/4m$ for all i. Then $N \leq 2m$.*

Proof. Let $Q = I_n - P$. So $\langle e_i| Q |e_i\rangle \leq 1/4m$. By the Cauchy Schwarz inequality $|\langle e_i|Q|e_j\rangle|^2 \leq \langle e_i| Q |e_i\rangle \langle e_j| Q |e_j\rangle \leq (1/4m)^2$. So $|\langle e_i|Q|e_j\rangle| \leq 1/4m$.

$$\begin{aligned} 0 = \langle e_i|e_j\rangle &= \langle e_i|P + Q|e_j\rangle \\ 0 &= \langle e_i|P|e_j\rangle + \langle e_i|Q|e_j\rangle \\ |\langle e_i|P|e_j\rangle| &\leq |\langle e_i|Q|e_j\rangle| \leq 1/4m. \end{aligned} \tag{2}$$

Let $c_i = (\langle e_i|P|e_i\rangle)^{1/2}$, where $c_i^2 \geq 1 - 1/4m$. Let $|f_i\rangle = c_i^{-1} P |e_i\rangle$. If $i \neq j$ then $|f_i\rangle \neq |f_j\rangle$. Otherwise, due to Equation 2, we get the contradiction,

$$\begin{aligned} |\langle e_i|P|e_j\rangle| &\leq |\langle e_i|Q|e_j\rangle| \\ c_i c_j |\langle f_i|f_i\rangle| &\leq 1/4m \\ 1 - 1/4m &\leq 1/4m. \end{aligned}$$

So for $i \neq j$,

$$|\langle f_i|f_j\rangle| \leq c_i c_j |\langle e_i|P|e_j\rangle| \leq (1/4m)/(1 - 1/4m) \leq m^{-1/2}/2.$$

Applying Proposition 3 on $\{|f_i\rangle\}_{i=1}^N$ proves that $N \leq 2m$. □

7 Discussion

Note that Corollary 3(1) can be improved to the bounds

$$\mathbf{K}(x|n) <^{+} \mathbf{Hbvl}^{\epsilon}(|x\rangle \langle x| |n) + \mathbf{K}(\mathbf{Hbvl}^{\epsilon}(|x\rangle \langle x| , |n), \epsilon|n) - \log(1-\epsilon),$$

with a difficult proof involving a complete reconstruction of the universal QTM $\mathfrak{U}$.

References

[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.

[Gác01] P. Gács. Quantum Algorithmic Entropy. *Journal of Physics A Mathematical General*, 34(35), 2001.

[Mue07] M. Mueller. Quantum kolmogorov complexity and the quantum turing machine. *CoRR*, abs/0712.4377, 2007.

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

[Mul09] M. Muller. On the quantum kolmogorov complexity og classical strings. *International Journal of Quantum Information*, 07(04):701–711, 2009.

[Tao] What's new: A cheap version of the kabatjanskii-levenstein bound for almost orthogonal vectors. https://terrytao.wordpress.com/2013/07/18/a-cheap-version-of-the-kabatjanskii-levenstein-bound-for-almost-orthogonal-vectors/. Accessed: 2024-01-11.