# A Simple Proof of Müller's Theorem

Samuel Epstein
samepst@jptheorygroup.org

February 2, 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 simple proof of this theorem.

## 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 simple proof to the following main result, which is as follows.

**Theorem**. ([Mue07, Mul09])

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

## 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. We use $[A]$ to equal 1 if the mathematical statement $A$ is true and 0 otherwise.

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 $\mathcal{H}_{2^n}$.

**Definition 1 (Indeterminate Length Quantum States)** *The separable Hilbert space $\mathcal{Q} = \bigoplus_{n\in\mathbb{W}} \mathcal{Q}_n$ is the space of indeterminate length quantum states.*

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, $\sigma$ and $\rho$ 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 $\sigma$ 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 $\mathbf{m}(\sigma)$. A quantum operation is elementary if its corresponding Kraus operators are elementary.

We say program $q \in \{0, 1\}^*$ lower computes positive semidefinite matrix $\sigma$ 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 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 $\rho$ to be the shortest program to a universal quantum Turing machine that approximates or produces $\rho$. This definition was introduced in [BvL01] and we call it BvL complexity.

All quantum Turing machines used in this manuscript 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].

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 $\rho$ 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, $\Sigma$ 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 $\rho$, 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 $\langle f_C| M_C^{t}(\rho) |f_C\rangle = 1$, then $M(\rho)$ is defined to be the qubit mixed state $\sigma$ corresponding to at ensemble of pure states determined by the pointer positions on the output tape at the time of halting. Otherwise $M$ is undefined. Thus the output can be a superposition of pure states of different lengths, indeterminate length quantum states. Thus QTMs $M$ can be thought of as partial functions of the following form.

$$M : \bigcup_n \mathcal{Q}_n \to \mathcal{Q}.$$

Thus we only consider *fixed-length* inputs to QTMs $M$. This consists of elements of $\mathcal{Q}$ that are superpositions of basis quantum states $|e_i\rangle$ of the same length.

One might argue that this definition with regard to the halting state is too restrictive, but as shown [Mue07], for every input $\sigma$ to a QTM that almost halts within a certain computable level of precision, there is another state $\sigma'$ 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 is required. To measure the closeness of states, the *trace distance* function is used.

**Definition 2 (Trace Distance and Fidelityt 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* $F(|\psi\rangle,\sigma) = \langle\psi|\sigma|\psi\rangle$ *and* $1 - D(\rho,|\psi\rangle) < F(\rho,|\psi\rangle)$.

**Theorem 1 ([Mul08])** *There is quantum Turing machine* $\mathfrak{U}$ *such that for every QTM* $M$ *and mixed state* $\sigma$ *for which* $M(\sigma)$ *is defined, there is mixed state* $\sigma'$ *such that*

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

*for every* $\delta \in \mathbb{Q}_{>0}$ *where* $\|\sigma'\| <^+ \|\sigma\| + \mathbf{K}(M,\delta$.

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

**Definition 3** *The BvL Complexity of mixed state* $\rho$ *with respect to QTM* $M$ *is*

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

**Theorem 2 ([Mul08])** *For universal QTM* $\mathfrak{U}$ *and every QTM* $M$,

$$\mathbf{Hbvl}_{\mathfrak{U}}(\sigma) < \mathbf{Hbvl}_M(\sigma) + \mathbf{K}(M).$$

**Definition 4 (BvL Complexity)**

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

## 4 New Proof

**Remark 1** *Let $\mathcal{H}_k^t$ be the linear subspace of $\mathcal{Q}_k$ that spans pure states $|\psi\rangle \in \mathcal{Q}_k$ such that $\mathfrak{U}(|\psi\rangle)$ is defined and halts in $t$ steps. Due to [Mue07, Mul08], if $t \neq t'$ then $\mathcal{H}_k^t \perp \mathcal{H}_k^{t'}$.*

**Theorem 3 ([Mue07, Mul08])** *Given $k, t$, there is an algorithm that can enumerate $\mathcal{H}_k^t$ in the form of elementary projections $\{P_i\}$, such that $\mathrm{Tr} P_i P_j = 0$ for $i \neq j$ and $\sum_i P_i$ projects onto $\mathcal{H}_k^t$. Furthermore, all valid inputs $\sigma$ to $\mathfrak{U}$ have $\sigma \leq P_i$ for some $P_i$.*

**Lemma 1** *Given $t, k, \delta$ one can compute an elementary quantum operation $\Psi_k^{t,\delta} : \mathcal{Q}_k \to \mathcal{Q}$ such that if $\sigma \in \mathcal{H}_k^t$ then $D(\Psi_k^{t,\delta}(\sigma), \mathfrak{U}(\sigma)) \leq \delta$.*

**Proof.** Let $\Psi = \Psi_k^{t,\delta}$. The quantum operation $\Psi$ 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 the unitary matrix $u$ of $\mathfrak{U}$ (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 $p$ to the first $p$ output blocks and projects configurations with states other than $|q_f\rangle$ to $\lambda \in \mathcal{Q}_0$. 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 $\mathcal{C}$ be the finite configuration space. Let $\gamma$ be a parameter to be determined later. First cover $\mathcal{C}$ by elementary mixed states $\rho \in Q$, such that $\max_{\sigma \in \mathcal{C}} \min_{\rho \in Q} D(\sigma, \rho) < \gamma/3$. Next run the algorithm to compute the transition function of $\mathfrak{U}$ long enough to produce unitary matrix $\tilde{u}$ such that for all $\rho \in Q$, $D(u\rho u^*, \tilde{u}\rho\tilde{u}^*) < \gamma/3$. This is possible because the amplitudes of the transition function of $\mathfrak{U}$ can be computed to any accuracy. Thus for any $\sigma \in \mathcal{C}$, for proper choice of $\rho \in Q$, by the triangle inequality of trace distance,

$$\begin{aligned} D(u\sigma u^t, \tilde{u}\sigma\tilde{u}^*) &< D(u\sigma u^*, u\rho u^*) + D(u\rho u^*, \tilde{u}\rho\tilde{u}^*) + D(\tilde{u}\rho\tilde{u}^*, \tilde{u}\sigma\tilde{u}^*) \\ &< D(\sigma, \rho) + \gamma/3 + D(\rho, \sigma) \\ &< \gamma. \end{aligned}$$

If $\tilde{u}$ is run twice with any input $\sigma \in \mathcal{C}_n$, the error is bounded by

$$\begin{aligned} D(\tilde{u}^2\sigma\tilde{u}^{2*}, u^2\sigma u^{2*}) &< D(\tilde{u}^2\sigma\tilde{u}^{2*}, \tilde{u}u\sigma u\tilde{u}) + D(\tilde{u}u\sigma u\tilde{u}, u^2\sigma u^{2*}) \\ &< D(u\sigma u^*, \tilde{u}\sigma\tilde{u}^*) + \gamma \\ &< 2\gamma. \end{aligned}$$

With similar reasoning, one can see that running $\tilde{u}$ a total of $\ell$ times will produce a maximum error of $\gamma\ell$. So $\gamma$ is set to equal $\delta/t$. So for all $\sigma \in \mathcal{Q}_k$,

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

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

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

□

The following new proof of Müller's Theorem is self contained, in that the only characterization of the universal QTM $\mathfrak{U}$ needed is Theorem 3.

**Theorem 4** ([Mue07, Mul09])

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

**Proof.** $\mathbf{Hbvl}(|x\rangle \langle x|) <^{+} \mathbf{C}(x)$ because a universal QTM can simulate a classical Turing machine. Let $k = \mathbf{Hbvl}(|x\rangle \langle x|)$. Let $j = 2^{k+5}$ be the precision parameter. Let $\Psi_k^{t,\delta}(\cdot|j)$ be equal to $\Psi^{t,\delta}(\cdot)$ with the universal QTM $\mathfrak{U}$ (and the QTMs it simulates) with $j$ on the auxilliary tape. Using Theorem 3, enumerate all projection operators $P_i$ of $\mathcal{H}_k^t$ (relativized to $j$) for fixed $k$ over all $t$. So $\mathrm{Tr}\sum_i P_i \leq 2^k$. For each $P_i$ enumerated, compute $O_i = \Psi_k^{t(i),1/j}(P_i)$, where each $O_i$ is a positive operator over $\mathcal{Q}$ with $\mathrm{Tr}\sum_i O_i \leq 2^k$.

Assume there is a $k$ qubit input $\sigma \leq P_i$ and a pure state $|\psi\rangle \in \mathcal{Q}_\ell$ such that $D(\mathfrak{U}(\sigma, j), |\psi\rangle) < 1/j$. If $\xi = \Psi_k^{t(i),1/j}(\sigma|j) \leq O_i$ then $D(\xi, \mathfrak{U}(\sigma, j)) < 1/j$ and by the triangle inequality of trace distances, $D(\xi, |\psi\rangle) < 2/j$ and so $1 - 2/j < F(\xi, |\psi\rangle) = \langle\psi| \xi |\psi\rangle \leq \langle\psi| O_i |\psi\rangle = \langle\psi| O_i^\ell |\psi\rangle$, where $O_i^\ell = Q_\ell O_i Q_\ell$, where $Q_\ell$ is the projector onto $\mathcal{Q}_\ell$.

Let $N_i^\ell$ be a projection over $\mathcal{Q}_\ell$ defined from $O_i^\ell$ in the following way. Since $O_i^\ell = \sum_i v_i |e_i\rangle \langle e_i|$ for some orthonormal basis $\{|e_i\rangle\}$, of $\mathcal{Q}_\ell$, we define $N_i^\ell$ to be equal to $\sum_i [1/2 \leq v_i] |e_i\rangle \langle e_i|$. So $\mathrm{Tr} N_i^\ell \leq 2\mathrm{Tr} O_i^\ell \leq 2^{k+1}$. Some simple math shows that if $\langle\psi| O_i^\ell |\psi\rangle \geq 1 - 2/j$, then $\langle\psi| N_i^\ell |\psi\rangle \geq 1 - 4/j = 1 - 2^{-k-3}$. By Lemma 2, there can be only at most $2\mathrm{Tr} N_i^\ell$ classical states $|y\rangle$, $y \in \{0,1\}^\ell$, with $\langle y| N_i^\ell |y\rangle \geq 1 - 2^{-k-3}$. Since $\mathrm{Tr}\sum_{i,j} N_i^j \leq 2^{k+1}$, there only at most $2^{k+1}$ classical strings $|y\rangle$ such that there is a $k$ qubit state $\rho$ such that $D(\mathfrak{U}(\rho, j), |y\rangle) < j^{-1}$.

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

**Proposition 1** ([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 2** *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 $|f_i\rangle = c_i^{-1} P|e_i\rangle$. So for $i \neq j$,

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

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

## 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.

[GÓ1] 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.