Descriptional Complexity of Unitary Transformations

Alexei Kaltchenko[a]

[a]Department of Physics and Computer Science, Wilfrid Laurier University,Waterloo, Ontario N2L 3C5, Canada

ABSTRACT

We introduce the notion of descriptional complexity of finite-dimensional unitary transformations, which is closely related to the notion of Kolmogorov complexity of a quantum state. In quantum computing, quantum states are associated with quantum data, and unitary transformations of quantum states are associated with quantum computer programs.

Keywords: quantum mechanics; information theory; quantum; Kolmogorov complexity; quantum computing; quantum information; unitary.

1. INTRODUCTION

Descriptional complexity, also known as, Kolmogorov complexity, is an important characteristic of information and data and naturally appear in many information processing tasks. In classical data storage and transmission, data processing devices are implicitly assumed to work according to the laws of classical physics. However, as the size of the devices becomes smaller and smaller, they begin to function according to the laws of quantum mechanics, not classical physics. In this work we study Kolmogorov complexity of unitary transformations with application to quantum computing.

For a comprehensive introduction to quantum computing with linear algebra and quantum mechanics, see, for example.[1] In quantum computing, quantum states are associated with quantum data, and a unitary evolution of quantum states is associated with a quantum computer program.

Kolmogorov complexity[2,3] of a classical object is defined as the shortest effective binary description of the object. So it is about how much information (binary data) we need to describe, reproduce or recreate the object. The concept of Kolmogorov complexity has been extended from classical objects (strings, files, images, etc.) to quantum domain: the complexity of quantum states[4,5] (i.e. the complexity of quantum data) and the complexity of a unitary evolution of quantum states (i.e. the complexity of quantum computer program).

In computer science[3] and information theory,[6] Kolmogorov complexity of a (classical) string (for example, a binary sequence) or, more generally, of a classical finite object is commonly known as the shortest binary program p, which runs on a Turing machine and computes (in other words, describes) the string or the object. Thus, Kolmogorov complexity is also called *descriptive complexity.*

There have been several approaches[4,5,7,8] to define a complexity of a quantum state. In,[4,5] the concept of Kolmogorov complexity was extended from classical to quantum domain. Such an extension naturally relies upon the concept of quantum Turing machine.[4,9,10]

The concept of a universal quantum Turing machine ($UQTM$) as a precise mathematical model for quantum computation was first proposed by Deutsch.[11] The detailed construction of $UQTMs$ can be found in.[9,12] These machines work analogously to classical TMs, that is they consist of a read/write head, a set of internal control states and input/output tapes. However, the local transition functions among the machine's configurations (the programs or quantum algorithms) are given in terms of probability amplitudes, implying the possibility of linear superpositions of the machine's configurations. The quantum algorithms work reversibly. They correspond to unitary actions of the $UQTM$ as a whole. An element of irreversibility appears only when the output tape information is extracted by tracing away the other degrees of freedom of the $UQTM$. This provides linear superpositions as well as mixtures of the output tape configurations consisting of the local states $0, 1$ and blanks

Further author information: E-mail: akaltchenko@wlu.ca

International Conference on Micro- and Nano-Electronics 2021, edited by Vladimir F. Lukichev, Konstanten V. Rudenko, Proc. of SPIE Vol. 12157, 121571S · © 2022 SPIE · 0277-786X · doi: 10.1117/12.2620457

#, which are elements of the so-called *computational basis*. The reversibility of the *UQTM*'s time evolution is to be contrasted with recent models of quantum computation that are based on measurements on large entangled states, that is on irreversible processes, subsequently performed in accordance to the outcomes of the previous ones.[13] In this paper we shall be concerned with Bernstein-Vazirani-type *UQTMs* whose inputs and outputs may be bit or qubit strings.[9]

Let $\mathcal{H}$ be a 2-dimensional complex vector space (Hilbert space). A qubit is described by a unit vector in $\mathcal{H}$. Then, for any integer n, the state of n qubits corresponds to a unit vector in n-folded space $\mathcal{H}^{\otimes n}$. We will use the bra–ket Dirac notation with low case Latin letters to denote vectors in $\mathcal{H}^{\otimes n}$, that is $|x\rangle$, $|y\rangle$, etc.

Based on a classical description of a quantum state $|x\rangle$, a variant of Kolmogorov complexity[4] is defined as follows:

$$K_Q\left(|x\rangle\right) \triangleq \min_p \left\{ l(p) + \left\lceil -\log \left\|\langle z|x\rangle\right\|^2 \right\rceil : Q(p) = |z\rangle \right\}, \tag{1}$$

where Q is a quantum Turing machine, p is a classical binary program which runs on the quantum Turing machine Q, $l(p)$ is the number of (classical) bits in the program p, and $|x\rangle$ is the target state that one is trying to describe.

Note that $|z\rangle$ is the quantum state produced by the computation $Q(p)$, and therefore, given Q, is completely determined by p. Thus, the minimum of the right-hand side of the equality(1) is obtained by minimizing over p only. The state $|z\rangle$ that minimizes the right-hand-side of (1) is called the *directly computed part* of $|x\rangle$, while $\left\lceil -\log \left\|\langle z|x\rangle\right\|^2 \right\rceil$ is the *approximation part*.

We point out that the exact classical description (that is computing) of an arbitrary $|x\rangle$ is generally incomputable or infinite. So, in the most general case, $K_Q\left(|x\rangle\right)$ is the length of the binary program which approximates $|z\rangle$. Nevertheless, $K_Q\left(|x\rangle\right)$ may be suitable for *discrete* classical and quantum Turing machines as well as with quantum circuits and quantum algorithms with a *discrete* set of quantum gates.

A different way to define a notion of quantum Kolmogorov complexity is to consider the shortest effective qubit description[5] of a pure quantum state. An advantage of qubit complexity is that the upper bound on the complexity of a pure quantum state is immediately given by the number of qubits involved in the literal description of that pure quantum state. Let us denote the resulting qubit complexity of a pure quantum state $|x\rangle$ by $QC\left(|x\rangle\right)$. Roughly speaking, the qubit complexity $QC\left(|x\rangle\right)$ of $|x\rangle$ is the logarithm in base 2 of the dimension of the smallest Hilbert space (spanned by computational basis vectors) containing a quantum state that, once fed into a UQTM, makes the UQTM compute the output $|x\rangle$ and halt.

It was shown[14] that quantum Turing machines and uniformly generated quantum circuits are polynomially equivalent computational models. It is also known[1] that an arbitrary unitary operation on n qubits can be implemented using a circuit containing $O\left(n^2 4^n\right)$ continuous single qubit and CNOT gates.

On the other hand, according to the Solovay–Kitaev theorem,[15] any continuous single qubit and CNOT gate can be implemented with an accuracy $\epsilon > 0$ using $m \log^c\left(\frac{m}{\epsilon}\right)$ single qubit and CNOT gates from a discrete (finite) gate basis, where $c \approx 2$.

Thus, by setting $m \triangleq n^2 4^n$, an arbitrary unitary operation on n qubits can be implemented using a circuit containing L single qubit and CNOT gates from a discrete (finite) gate basis:

$$L = O\left(n^2 4^n\right) \log^c\left(\frac{n^2 4^n}{\epsilon}\right) \approx O\left(n^2 4^n\right) \log\left(\frac{1}{\epsilon}\right) \tag{2}$$

2. DESCRIPTIONAL COMPLEXITY OF UNITARY TRANSFORMATIONS

Let U be a unitary transformation on $\mathcal{H}^{\otimes n}$, represented by a $2^n \times 2^n$ unitary matrix. It preserves inner product and has properties:

$$U^\dagger U = I,$$
$$U^\dagger = U^{-1}.$$

We note that any unitary transformation U can be implemented[1] as a quantum computation on quantum Turing machine as well as using quantum logic circuits.

Let $\mathcal{V}$ denote a 2^{2n}-dimensional vector space of linear operators acting on $\mathcal{H}^{\otimes n}$. For the vector space $\mathcal{V}$, we define a Hilbert-Schmidt inner product:

$$\langle A, B \rangle_{HS} = \operatorname{tr}\left[A^{\dagger} B\right] \tag{3}$$

Thus, $\mathcal{V}$ becomes a 2^{2n}-dimensional Hilbert space with inner product(3).

We extend the notion of Kolmogorov qubit complexity $QC\left(|x\rangle\right)$ to that for vectors in the Hilbert space $\mathcal{V}$.

Let $|U\rangle$ be a bra–ket Dirac notation for a vector in $\mathcal{V}$, which represents a unitary operator U acting on $\mathcal{H}^{\otimes n}$:

$$K(U) \triangleq QC\left(|U\rangle\right) \tag{4}$$

Since the dimensionality of the Hilbert space $\mathcal{V}$ is equal 2^{2n}, the upper bound on $K(U)$ is given by:

$$K(U) \leq 2n + O(1), \tag{5}$$

3. MAPPING OPERATORS TO PURE STATES

Any unitary operator is also a normal operator (the converse is obviously not true). If a normal operator has trace 1, it can be mapped to a pure quantum state via so-called "purification[1] procedure". It goes as follows. Let ρ be a normal operator acting on $\mathcal{H}^{\otimes n}$ and having trace 1. Suppose ρ has orthonormal decomposition:

$$\rho = \sum_i p_i |i\rangle\langle i|. \tag{6}$$

We note that operator ρ acts on the Hilbert space $\mathcal{H}^{\otimes n}$ and we label the underlying quantum system by A. To purify ρ, we introduce another, axillary quantum system, which we label by R and which has a state space identical with A, with orthonormal basis states $|i^R\rangle$. We now define a pure state for the combined system with the state space $\mathcal{H}^{\otimes n} \otimes \mathcal{H}^{\otimes n}$ as follows:

$$|AR\rangle \triangleq \sum_i \sqrt{p_i} |i^A\rangle |i^R\rangle. \tag{7}$$

It's easy to see that operator ρ can be obtained from the pure state $|AR\rangle$ by tracing out the auxiliary system R as follows:

$$\begin{aligned}
\operatorname{tr}_R\left(|AR\rangle\langle AR|\right) &= \sum_{ij} \sqrt{p_i p_j} |i^A\rangle\langle j^A| \operatorname{tr}\left(|i^R\rangle\langle j^R|\right) \\
&= \sum_{ij} \sqrt{p_i p_j} |i^A\rangle\langle j^A| \delta_{ij} \\
&= \sum_i p_i |i^A\rangle\langle i^A| \\
&= \rho.
\end{aligned} \tag{8}$$

We define the Kolmogorov complexity of ρ as the quantum Kolmogorov complexity of state $|AR\rangle$:

$$K(\rho) \triangleq QC\left(|AR\rangle\right) \tag{9}$$

Since the dimensionality of the Hilbert space for quantum state $|AR\rangle$ is equal 2^{2n}, the upper bound on $K(\rho)$ is given by:

$$K(\rho) \leq 2n + O(1), \tag{10}$$

Remark:
Complexity definition (4) is obviously applicable to ρ, and, moreover, the complexity of ρ defined in (4) is equal

to the complexity defined in (9) up to $O(1)$. It follows from the fact that qubit complexity is minimized over all possible computations and the complexity of mapping

$$\rho \to |AR\rangle \tag{11}$$

is $O(1)$ and such a mapping injects just a constant amount of information into $|AR\rangle$, which does not depend on n.

4. CONCLUSION

In this work, we have introduced the notion of descriptional complexity of finite-dimensional unitary transformations, obtained the complexity upper bound and discussed the mapping of an important class of liner operators to pure quantum states.

REFERENCES

[1] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.

[2] A. Kolmogorov, "Three approaches to the quantitative definition of information," *International Journal of Computer Mathematics* **2**, pp. 157–168, 1968.

[3] M. Li and P. Vitányi, *An Introduction to Kolmogorov Complexity and Its Applications*, Springer New York, 1993.

[4] P. Vitanyi, "Quantum kolmogorov complexity based on classical descriptions," *IEEE Transactions on Information Theory* **47**, pp. 2464–2479, 2001.

[5] A. Berthiaume, W. Van, and S. Laplante, "Quantum kolmogorov complexity," *Journal of Computer and System Sciences* **63**, p. 201, 2001.

[6] T. Cover and J. Thomas, *Information Theory*, Wiley, 1997.

[7] P. Gács, "Quantum algorithmic entropy," *Journal of Physics A: Mathematical and General* **34**, pp. 1–22, 2001.

[8] C. Mora and H. Briegel, "Algorithmic complexity and entanglement of quantum states," *Phys. Rev. Lett.* **95**, p. 200503, 2005.

[9] E. Bernstein and U. Vazirani, "Quantum complexity theory," *SIAM J. Comput.* **26**, pp. 1411—1473, 1997.

[10] F. Benatti, T. Krueger, M. Mueller, R.Siegmund-Schultze, and A. Szkola, "Entropy and quantum kolmogorov complexity: A quantum brudno's theorem," *Communications in Mathematical Physics* **265**, pp. 437–461, 2006.

[11] D. Deutsch, "Quantum theory, the church-turing principle and the universal quantum computer," *Proc. R. Soc. Lond.* **A400**, 1985.

[12] L. Adleman, J. Demarrais, and M. A. Huang, "Quantum computability," *SIAM J. Comput.* **26**, pp. 1524–1540, 1997.

[13] S. Perdrix and P. Jorrand, "Measurement-based quantum turing machines and their universality," 2004.

[14] A. Yao, "Quantum circuit complexity," *Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science* , pp. 352—-361, 1993.

[15] A. Kitaev, A. Shen, and M. Vyalyi, *Classical and Quantum Computation (Graduate Studies in Mathematics)*, American Mathematical Society, 2002.