Optimal universal programming of unitary gates

Yuxiang Yang,[1,*] Renato Renner,[1,†] and Giulio Chiribella[2,3,4,5,‡]

[1] *Institute for Theoretical Physics, ETH Zürich*
[2] *QICI Quantum Information and Computation Initiative, Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong*
[3] *Department of Computer Science, Parks Road, Oxford, OX1 3QD, UK*
[4] *Perimeter Institute for Theoretical Physics, Waterloo, Ontario N2L 2Y5, Canada*
[5] *The University of Hong Kong Shenzhen Institute of Research and Innovation, 5/F, Key Laboratory Platform Building, No.6, Yuexing 2nd Rd., Nanshan, Shenzhen 518057, China*

Keywords: Unitary gate programming; Quantum metrology; Quantum learning

For the full article, see PRL 125.210501 (Editors' Suggestion) or arXiv:2007.10363.

Introduction. A universal quantum processor is the desideratum of quantum computing. Ideally, one would hope to realise quantum computing in the same way as its classical counterpart, i.e., by inserting data and programs, both in the form of quantum states, into a universal quantum computer (see Figure 1). However, the no-programming theorem [1] asserts that any universal quantum processor must be approximate, or have a non-zero probability of failure [1–3].

It has been shown that approximate universal processors with a finite-size program register do exist [1, 4–9]. There one of the most important questions is to determine the cost-accuracy tradeoff or, more specifically, how the program cost, i.e., the number c_{P} of qubits required to store the optimal program, scales with the desired accuracy of implementation, which we quantify in terms of an approximation error ϵ (usually evaluated in terms of the diamond norm [10]).

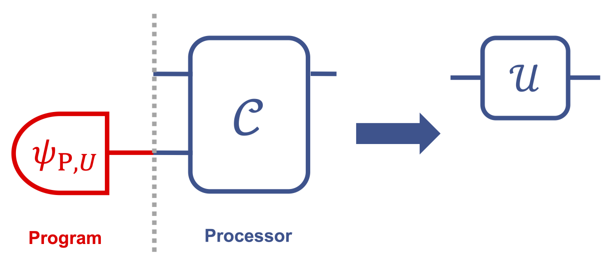

FIG. 1: **An approximate universal quantum processor.** An approximate universal quantum processor executes a unitary gate U on a system. It works by plugging a quantum state – the program for U – into the processor, which performs a quantum channel $\mathcal{C}$ that approximates U on the system.

Over the past two decades, many efforts have been dedicated to finding the optimal approximate universal processor (see, e.g., [4, 5, 8, 9]). The state-of-the-art results, [9, 11] (see also Table I), assert that the optimal program cost c_{P} for a d-dimensional unitary quantum gate lies between $c_{\mathrm{low}} := [(d-1)/2]\log_2(1/\epsilon)$ qubits and $c_{\mathrm{upp}} := d^2\log_2(K/\epsilon)$ qubits, where K is a universal constant. Despite all efforts, the precise value for c_{P} remained largely unknown — especially in the small error regime, where the ratio $c_{\mathrm{low}}/c_{\mathrm{upp}}$ is strictly smaller than one.

In this work, we close this gap by identifying the optimal scaling of the program cost with the accuracy and therefore solving a long-standing open problem of optimal quantum programming. Specifically, our program cost scales as $[(d^2-1)/2]\log_2(1/\epsilon)$ in the small ϵ regime, which reduces the cost of the best existing protocol (see c_{upp} above) by half. The optimal scaling is achieved with a gate learning protocol, where the program is prepared by sending a quantum state through n instances of the gate to learn it [12]. The gate information is later read out by measuring the program. Our protocol achieves a diamond norm error scaling of $1/n^2$ – well-known as the

	Upper bounds	Lower bounds
Previous works	$d^2 \log_2 (K/\epsilon)$ [9] $4d^2 \log_2 d/\epsilon^2$ [8, 17, 18]	$[(1-\epsilon)K]d - (2/3)\log_2 d$ [9] $\log_2 \left(d^2/\epsilon\right)$ [19] $\left(\frac{d+1}{2}\right)\log_2(1/d) + \left(\frac{d-1}{2}\right)\log_2(1/\epsilon)$ [11]
This work	$\left(\frac{d^2-1}{2}\right)\log_2\left(\Theta(d^3)/\epsilon\right)$	$\alpha \log_2 \left(\Theta(d^{-4})/\epsilon\right)$ for any $\alpha < (d^2-1)/2$ and sufficiently small ϵ

TABLE I: **Comparison of bounds on universal quantum gate programming.** In the table we compare our results on the programming cost with the best previous results (summarised from Table I of Ref. [9]). In the vanishing error regime $\epsilon \to 0$, both our lower bound and our upper bound are tighter than all previous results, for the first time closing the gap between the lower and upper bound in this regime. The cost is defined as the number of qubits in the program and the error is evaluated in terms of the diamond norm (1). K denotes a universal constant.

Heisenberg limit of quantum metrology [13–16]. We thus prove the asymptotic equivalence of quantum gate programming, metrology, and learning.

Approximate universal processors. A universal quantum processor consists of two key elements: a set of programs $\{\psi_{\mathrm{P},U}\}_{U\in\mathsf{SU(d)}}$[1], which are quantum states in $\mathcal{H}_\mathrm{P}$, and the action of the processor $\mathcal{C}$, which is a quantum channel (i.e. a completely positive trace-preserving linear map) acting on the composite Hilbert space $\mathcal{H}_\mathrm{S}\otimes\mathcal{H}_\mathrm{P}$ of the system and the program. Notice that all information on U should come from the program, and $\mathcal{C}$ must be independent of U. The program cost c_P is defined as $\log_2 d_\mathrm{P}$, with the program dimension d_P being the dimension of $\mathsf{Supp}\{\psi_{\mathrm{P},U}\}_{U\in\mathsf{SU(d)}}$.

As shown in Figure 1, to run any arbitrary unitary U on the system, one selects the corresponding program $\psi_{\mathrm{P},U}$ and plugs it into the processor, resulting in a channel $\mathcal{E}_U(\cdot) := \mathrm{Tr}_\mathrm{P}\left[\mathcal{C}(\cdot\otimes\psi_{\mathrm{P},U})\right]$ on the system. A tuple $(\mathcal{C},\{\psi_{\mathrm{P},U}\}_{U\in\mathsf{SU(d)}})$ is called a *ϵ-universal processor*, if

$$\frac{1}{2}\left\|\mathcal{U}-\mathcal{E}_U\right\|_\diamond \leq \epsilon \quad \forall\, U\in\mathsf{SU(d)}. \tag{1}$$

Here $\|\cdot\|_\diamond$ denotes the *diamond norm* [10], which equals the maximum trace distance between the outputs of the two channels, maximized over all input states and over all possible reference systems.

Lower bound on the program cost. Our first main result is a lower bound on the program cost, which can be regarded as a quantitative version of the no-programming theorem [1]:

Theorem 1 (Approximate no-programming theorem)**.** *Consider any ϵ-universal processor with program dimension c_P. For any (ϵ-independent) parameter $\delta>0$, the program dimension is lower bounded as*

$$c_\mathrm{P} \geq (1-\delta-4\sqrt{2\epsilon})(d^2-1)\log_2\left(\frac{\delta}{4\sqrt{2\epsilon}(d^2-1)}\right)-1. \tag{2}$$

This immediately implies the expression for the lower bound stated in Table I. The key message from the above theorem is that, for any $\alpha<(d^2-1)/2$, the program dimension $d_\mathrm{P}=2^{c_\mathrm{P}}$ satisfies

$$d_\mathrm{P} = \Omega\left(1/\epsilon^\alpha\right) \tag{3}$$

[1] For a pure state $|\psi\rangle$, we denote by ψ its density matrix.

Taking $\epsilon \to 0$ in Eq. (3), one gets $d_{\mathrm{P}} \to \infty$, recovering the original no-programming theorem [1].

Optimal approximate universal processor. Next we construct an approximate universal processor that achieves the bound in Theorem 1. Our processor works in a measure-and-operate (MO) fashion. It measures the input program $\psi_{\mathrm{P},U}$ with a suitable POVM $\{\mathrm{d}\,\hat{U}\,M_{\hat{U}}\}_{\hat{U}\in\mathsf{SU(d)}}$, where $\mathrm{d}\,\hat{U}$ is the Haar measure. The measurement yields an estimate $\hat{U}$ of the gate U, and the processor performs the corresponding gate on the system. Explicitly, our optimal processor obeys the following procedure:

Protocol 1 A MO universal processor.

1: (Generating the program.)
Apply $U^{\otimes n}$ to a suitable quantum state $|\psi_{\mathrm{P}}\rangle$.
2: Measure $|\psi_{\mathrm{P},U}\rangle := U^{\otimes n}|\psi_{\mathrm{P}}\rangle$ with $\{\mathrm{d}\,\hat{U}\,M_{\hat{U}}\}_{\hat{U}\in\mathsf{SU(d)}}$.
3: Apply $\hat{U}$ to the state of the system, where $\hat{U}$ is the measurement outcome.

The program in Protocol 1 is prepared by applying n parallel uses of U on a quantum state (called the *probe state*). The performance of this processor is then determined jointly by the choice of the probe state $|\psi_{\mathrm{P}}\rangle$ and the choice of the POVM $\{\mathrm{d}\,\hat{U}\,M_{\hat{U}}\}_{\hat{U}\in\mathsf{SU(d)}}$. It is known from quantum metrology [14, 15, 20] that the performance of the measurement is optimised using non-product probe states and POVMs. We identify a probe state and a POVM which, when incorporated into Protocol 1, yields an optimal processor asymptotically achieving the $((d^2-1)/2)\log_2(1/\epsilon)$ scaling bound of Theorem 1:

Theorem 2. *Consider the estimation of an unknown unitary gate on a d-dimensional quantum system. Suppose $n \geq 2d(d-1)$ and $d \geq 2$. The error for the optimal unitary gate estimation is bounded as*

$$\epsilon \leq 2d\left(\frac{\pi(d-1)^2(3d-2)}{d\cdot n}\right)^2. \tag{4}$$

The probe state has dimension bounded as

$$d_{\mathrm{P}} \leq \left(\frac{9n}{3d-2}\right)^{d^2-1}. \tag{5}$$

Ref. [20] showed that the estimation of an arbitrary d-dimensional unitary given n uses can be done with an error scaling $1/n^2$. The error was measured by the entanglement gate infidelity, which is upper bounded by $1-(1-\epsilon)^2$. Here we refine this result by not only achieving the $1/n^2$ scaling but also identifying an explicit expression of the constant of proportionality. In addition, our result holds for the more stringent error criterion ϵ, i.e., the diamond norm error, and we also determine how the probe state dimension scales with n.

Combining Eq. (4) with Eq. (5), we get:

Corollary 1. *The program cost c_{P} of Protocol 1 is upper bounded as* $c_{\mathrm{P}} \leq \left(\frac{d^2-1}{2}\right)\log_2\left(\frac{162\pi^2(d-1)^4}{d\cdot\epsilon}\right)$.

The above corollary is essentially our lower bound in Table I, which achieves a quadratic reduction compared to known results. In conclusion, our lower and upper bounds, taken together, fully answer the question of the optimal scaling in the regime of small ϵ.

* yangyu@ethz.ch

† renner@ethz.ch
‡ giulio@hku.hk

[1] M. A. Nielsen and I. L. Chuang, Physical Review Letters **79**, 321 (1997).
[2] M. Hillery, V. Bužek, and M. Ziman, Physical Review A **65**, 022301 (2002).
[3] M. Sedlák, A. Bisio, and M. Ziman, Physical Review Letters **122**, 170502 (2019).
[4] J. Kim, Y. Cheong, J.-S. Lee, and S. Lee, Physical Review A **65**, 012302 (2001).
[5] M. Hillery, V. Bužek, and M. Ziman, Fortschritte der Physik: Progress of Physics **49**, 987 (2001).
[6] G. Vidal, L. Masanes, and J. I. Cirac, Physical Review Letters **88**, 047905 (2002).
[7] A. Brazier, V. Bužek, and P. L. Knight, Physical Review A **71**, 032306 (2005).
[8] S. Ishizaka and T. Hiroshima, Physical Review Letters **101**, 240501 (2008).
[9] A. M. Kubicki, C. Palazuelos, and D. Pérez-García, Physical Review Letters **122**, 080505 (2019).
[10] A. Y. Kitaev, Russian Mathematical Surveys **52**, 1191 (1997).
[11] D. Pérez-García, Physical Review A **73**, 052315 (2006).
[12] A. Bisio, G. Chiribella, G. M. D'Ariano, S. Facchini, and P. Perinotti, Physical Review A **81**, 032324 (2010).
[13] V. Bužek, R. Derka, and S. Massar, Physical Review Letters **82**, 2207 (1999).
[14] G. Chiribella, G. D'Ariano, P. Perinotti, and M. F. Sacchi, Physical Review Letters **93**, 180503 (2004).
[15] E. Bagan, M. Baig, and R. Munoz-Tapia, Physical Review A **70**, 030301 (2004).
[16] M. Hayashi, Physics Letters A **354**, 183 (2006).
[17] S. Beigi and R. König, New Journal of Physics **13**, 093036 (2011).
[18] M. Christandl, F. Leditzky, C. Majenz, G. Smith, F. Speelman, and M. Walter, arXiv preprint arXiv:1809.10751 (2018).
[19] C. Majenz, *Entropy in Quantum Information Theory–Communication and Cryptography*, Ph.D. thesis, Faculty of Science, University of Copenhagen (2017).
[20] J. Kahn, Physical Review A **75**, 022326 (2007).