Optimal (controlled) quantum state preparation and improved unitary synthesis by quantum circuits with any number of ancillary qubits

Pei Yuan and Shengyu Zhang

Tencent Quantum Laboratory, Tencent, Shenzhen, Guangdong 518057, China

As a cornerstone for many quantum linear algebraic and quantum machine learning algorithms, controlled quantum state preparation (CQSP) aims to provide the transformation of $|i\rangle|0^n\rangle \to |i\rangle|\psi_i\rangle$ for all $i \in \{0,1\}^k$ for the given n-qubit states $|\psi_i\rangle$. In this paper, we construct a quantum circuit for implementing CQSP, with depth $O\left(n+k+\frac{2^{n+k}}{n+k+m}\right)$ and size $O\left(2^{n+k}\right)$ for *any* given number m of ancillary qubits. These bounds, which can also be viewed as a time-space tradeoff for the transformation, are *optimal* for any integer parameters $m, k \geq 0$ and $n \geq 1$.

When $k = 0$, the problem becomes the canonical quantum state preparation (QSP) problem with ancillary qubits, which asks for efficient implementations of the transformation $|0^n\rangle|0^m\rangle \to |\psi\rangle|0^m\rangle$. This problem has many applications with many investigations, yet its circuit complexity remains open. Our construction completely solves this problem, pinning down its depth complexity to $\Theta(n + 2^n/(n+m))$ and its size complexity to $\Theta(2^n)$ for *any* m.

Another fundamental problem, unitary synthesis, asks to implement a general n-qubit unitary by a quantum circuit. Previous work shows a lower bound of $\Omega(n + 4^n/(n+m))$ and an upper bound of $O(n2^n)$ for $m = \Omega(2^n/n)$ ancillary qubits. In this paper, we quadratically shrink this gap by presenting a quantum circuit of the depth of $O\left(n2^{n/2} + \frac{n^{1/2}2^{3n/2}}{m^{1/2}}\right)$.

1 Introduction

Quantum algorithms use quantum effects such as quantum entanglement and coherence to process information with the efficiency beyond any classical counterparts can achieve. In the past decade, many quantum machine learning algorithms [1] share a common subroutine of *quantum state preparation* (QSP), which loads a 2^n-dimensional complex-valued vector $v = (v_x : x \in \{0,1\}^n)^T \in \mathbb{C}^{2^n}$ to an n-qubit quantum state $|\psi_v\rangle = \sum_{x\in\{0,1\}^n} v_x|x\rangle$. These include quantum principle component analysis [2], quantum recommendation systems [3], quantum singular value decomposition [4], quantum linear system algorithm [5, 6], quantum clustering [7, 8], quantum support vector machine [9], etc. Quantum state preparation is also a key step in many Hamiltonian simulation algorithms [10–13].

Some of these quantum machine learning algorithms, such as quantum linear system algorithm [6], quantum recommendation systems [3] and quantum k-means clustering [7], need an

Pei Yuan: peiyuan@tencent.com

Shengyu Zhang: shengyzhang@tencent.com

oracle that can *coherently* prepare many states: $|i\rangle|0^n\rangle \to |i\rangle|\psi_i\rangle$, for all $i \in \{0,1\}^k$. We shall refer to this as the *controlled quantum state preparation* (CQSP) problem. The QSP and CQSP problems are also used in quantum walk algorithms such as the one by Szegedy [14] and by MNRS [15]. Given a general $N \times N$ state transition probability matrix $P = [P_{xy}]_{x,y\in[N]}$, quantum walk algorithms often call three subroutines: Setup, Check, and Update. The Setup procedure needs to prepare state $\sum_x \sqrt{\pi(x)}|x\rangle$, where π is the stationary distribution of P. The Update procedure needs to realize $|x\rangle|0^{\log N}\rangle \to |x\rangle \sum_y \sqrt{P_{xy}}|y\rangle$, a typical CQSP problem.

More generally, quantum algorithms can be represented as unitaries, which need to be implemented by quantum circuits for a digital quantum computer to run the algorithm. What is the minimum depth and size that any unitary operation can be compressed to? This paper also addresses this Unitary synthesis (US) problem by presenting a parametrized quantum circuit that can implement any given unitary operation.

In all these CQSP, QSP, and US problems, we hope to find quantum circuits as simple as possible for the sake of efficiency of execution and physical realization. Standard measures for quantum circuits include depth, size (i.e. the number of gates), and a number of qubits. The depth of a circuit corresponds to time and the number of qubits to space. The rapid advancement of the number of qubits provides opportunities to trade space for time, and indeed it has been found that ancillary qubits are useful in compressing the circuit depth for many tasks including CQSP, QSP, and US. It is a fundamental question to pin down the time-space tradeoff, or in circuit complexity language, the depth-qubit number tradeoff, for both quantum state preparation and general unitary synthesis problems.

Controlled quantum state preparation and Quantum state preparation Much previous work focuses on specific CQSP by quantum circuits [16–18]. QSP, in contrast, has been extensively studied. Bergholm *et al.* presented a QSP circuit with $2^{n+1}-2n-2$ CNOT gates and depth $O(2^n)$, without ancillary qubits [19]. Plesch and Brukner [20] improve the number of CNOT gate to $\frac{23}{24}2^n - 2^{\frac{n}{2}+1} + \frac{5}{3}$ for even n, and $\frac{115}{96}2^n$ for odd n. Ref. [19] also gives a depth upper bound of $\frac{23}{48}2^n$ for even n and $\frac{115}{192}2^n$ for odd n. The best result was obtained in [21], where the authors achieve the depth $O(2^n/n)$, which is optimal.

Zhang *et al.* [22] presented a QSP circuit of depth $O(n^2)$, by using $O(4^n)$ ancillary qubits, but the circuit involves measurement and the probability of successfully generating the target state is only $\Omega(1/(\max_i |v_i|^2 2^n))$.

The best previous result on QSP for an arbitary number m of ancillary qubits is by [21], where the authors presented a quantum circuit of depth $O\left(n + \frac{2^n}{n+m}\right)$ and size $O(2^n)$ for $m = O\left(\frac{2^n}{n\log n}\right)$ or $m = \Omega(2^n)$, which is asymptotically optimal. For $m \in \left[\Omega\left(\frac{2^n}{n\log n}\right), O(2^n)\right]$, they proposed a QSP circuit of depth $O(n\log n)$, which is only $O(\log n)$ off from the lower bound $\Omega\left(\max\left\{n, \frac{2^n}{n+m}\right\}\right)$. Later, Rosenthal independently constructed a QSP circuit of depth $O(n)$ using $O(n2^n)$ ancillary qubits [23]. The result also showed that an n-qubit quantum state preparation is in QAC^0_f with the same number of ancillary qubits. After that, [24] gave yet another proof of the $O(n)$ depth upper bound using $O(2^n)$ ancillary qubits. Both [23] and [24] did not give results for general m.

A related study is to prepare a quantum state in the *unary* encoding $\sum_{k=0}^{2^k-1} v_k|e_k\rangle$ instead of binary encoding $\sum_{k=1}^{2^n-1} v_k|k\rangle$ in [25], where $e_i \in \{0,1\}^{2^n}$ is the vector with the k-th bit being 1 and all other bits being 0. The binary encoding quantum state preparation is more efficient than unary encoding because binary encoding QSP utilizes n qubits but unary encoding utilizes 2^n qubits. In [25], Johri *et al.* prepared a unary encoding quantum state by a circuit of depth $O(n)$. Moreover, by encoding k to a d-dimensional tensor $(k_1, k_2, \ldots, k_d)$, they extended the

QSP circuit construction and obtained circuit depth $O\left(\frac{n}{d}2^{n-n/d}\right)$. If $d = n$, their encoding of k is binary encoding, and the depth upper bound is $O(2^n)$.

In this paper, we first give new quantum circuit constructions for CQSP with quantum content.

Theorem 1 (CQSP). *For any integers $k, m \geq 0$, $n > 0$ and any quantum states $\{|\psi_i\rangle : i \in \{0,1\}^k\}$, the following controlled quantum state preparation*

$$|i\rangle |0^n\rangle \to |i\rangle |\psi_i\rangle , \ \forall i \in \{0,1\}^k$$

can be implemented by a quantum circuit consisting of single-qubit and CNOT gates of depth $O\left(n + k + \frac{2^{n+k}}{n+k+m}\right)$ and size $O\left(2^{n+k}\right)$ with m ancillary qubits. These bounds are optimal for any $k, m \geq 0$.

Taking $k = 0$, This immediately implies the following result for QSP.

Theorem 2 (QSP). *For any $m \geq 0$, any n-qubit quantum state $|\psi_v\rangle$ can be generated by a quantum circuit, using single-qubit gates and CNOT gates, of depth $O\left(n + \frac{2^n}{n+m}\right)$ and size $O(2^n)$ with m ancillary qubits. These bounds are optimal for any $m \geq 0$.*

These bounds match the known lower bounds of circuit depth and size for QSP: $\Omega(\max\{n, \frac{4^n}{n+m}\})$ for depth [21, 26] and $\Omega(4^n)$ for size [27]. Thus we completely characterize the depth and size complexity for QSP with any number m of ancillary qubits.

Unitary synthesis For general unitary synthesis, Barenco *et al.* constructed a circuit involving $O(n^3 4^n)$ CNOT gates [28]. Knill reduced the circuit size to $O(n4^n)$ in [29], which was further improved by Vartiainen *et al.* [30] and Mottonen and Vartiainen [31] to $O(4^n)$, the same order as the lower bound of $\left\lceil \frac{1}{4}(4^n - 3n - 1) \right\rceil$ for for the number of CNOT gates [27].

These results assume no ancillary qubits. When there are m ancillary qubits available, Ref. [21] presented a quantum circuit for n-qubit general unitary synthesis of depth $O\left(n2^n + \frac{4^n}{n+m}\right)$, and also proved a depth lower bound $\Omega\left(n + \frac{4^n}{n+m}\right)$. Hence, their circuit depths are asymptotically optimal when $m = O\left(2^n/n\right)$, and leave a gap of $\left[\Omega\left(n + \frac{4^n}{m}\right), O\left(n2^n + \frac{4^n}{m}\right)\right]$ when $m = \Omega\left(2^n/n\right)$. By using Grover search in a clever way, Rosenthal improved the depth upper bound to $O(n2^{n/2})$ with $m = \Theta(n4^n)$ ancillary qubits [23], but did not give results for smaller m.

For general unitary synthesis, based on cosine-sine decomposition and Grover search, we optimize the circuit depth for general unitary synthesis.

Theorem 3 (Unitary synthesis). *For any $m \geq 0$, any n-qubit unitary $U \in \mathbb{C}^{2^n \times 2^n}$ can be implemented by a quantum circuit with m ancillary qubits, using single-qubit gates and CNOT gates, of depth $O\left(\frac{n^{1/2}2^{3n/2}}{m^{1/2}}\right)$ when $\Omega\left(2^n/n\right) \leq O(4^n/n)$. In particular, the depth is $O(n2^{n/2})$ when $m \geq \Omega(4^n/n)$.*

This result improves the one in [23] is two-fold. First, to achieve the same minimum depth of $O(n2^{n/2})$, we need fewer ancillary qubits: we need $m = \Theta(4^n/n)$ compared to $m = \Theta(n4^n)$ used in [23]. Second, our method works for any m as opposed to the one in [23] which needs $m = \Theta(n4^n)$ many ancillary qubits. Note that there is still a gap between upper and lower bounds when $m = \omega(2^n/n)$, left as an interesting open question for future studies.

Theorem 3 and previous results on circuit depth for general unitary synthesis are shown in Figure 1.

Relation to QRAM. The CQSP problem has a close relation to quantum random access memory (QRAM). In the original proposal [32, 33], QRAM aims to provide the transformation of

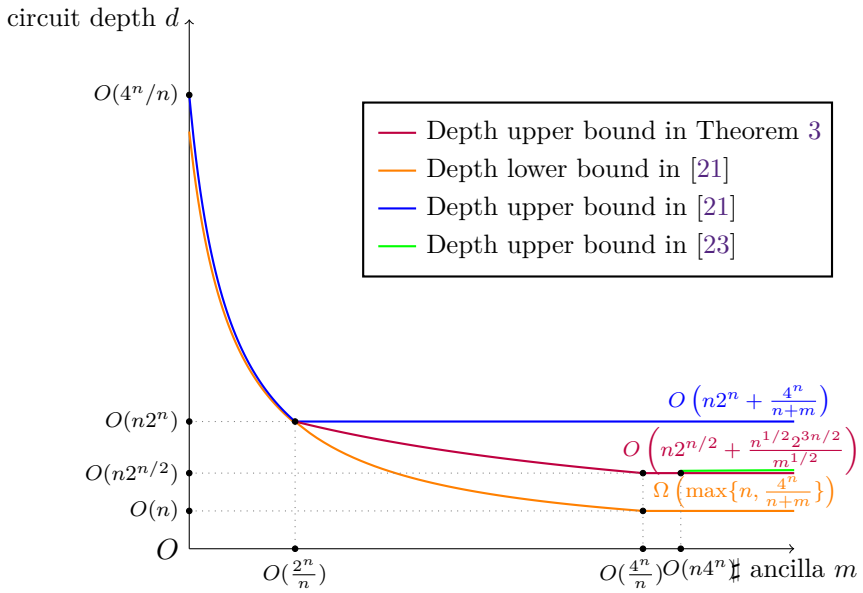

Figure 1: Circuit depth upper and lower bounds for general n-qubit unitary when m ancillary qubits are available. Ref. [21] gives an upper bound of $O\left(n2^n + \frac{4^n}{n+m}\right)$ and a lower bound of $\Omega\left(\max\left\{n + \frac{4^n}{n+m}\right\}\right)$, Ref. [23] presents a quantum circuit of depth $O\left(n2^{n/2}\right)$ using $m = \Theta(n4^n)$ ancillary qubits. This paper gives an upper bound of $O\left(n2^{n/2} + \frac{n^{1/2}2^{3n/2}}{m^{1/2}}\right)$ for any $m = \Omega(2^n/n)$.

$|i\rangle|0^n\rangle \to |i\rangle|\psi_i\rangle$ for all $i \in \{0,1\}^k$, where $|\psi_i\rangle$'s are states in $\{|0\rangle, |1\rangle\}^{\otimes n}$ or in $(\mathbb{C}^2)^{\otimes n}$, depending on whether the QRAM stores classical or quantum information as its content. Many quantum algorithms such as those mentioned at the beginning of this section, usually assume an efficient implementation of QRAM with classical content, and the hope is to have a hardware device to realize this. Despite some conceptual designs, working QRAM devices are yet to be convincingly demonstrated, even for a small scale. Results in this paper address a related and fundamental question of *implementing QRAM (with quantum content) by standard quantum circuits*, and show tight depth and size bounds for it.

Organization. The rest of this paper is organized as follows. In Section 2, we introduce notation and review some previous results. In Section 3, we will present a quantum circuit for (controlled) quantum state generation using arbitrary number of ancillary qubits. Then we will show a quantum circuit for general unitary synthesis in Section 4.

2 Preliminary

Notation Let $[n]$ denote the set $\{1, 2, \cdots, n\}$. All logarithms $\log(\cdot)$ are base 2 in this paper. For any $x = x_1 \cdots x_s \in \{0,1\}^s, y = y_1 \cdots y_t \in \{0,1\}^t$, xy denotes the $(s+t)$-bit string $x_1 \cdots x_s y_1 \cdots y_t \in \{0,1\}^{s+t}$. The n-qubit state $|i\rangle = |i_0 i_1 \cdots i_{n-1}\rangle \in (\{|0\rangle, |1\rangle\})^{\otimes n}$ is the *binary* encoding of i satisfying $i = \sum_{j=0}^{n-1} i_j \cdot 2^j$.

Quantum gates and circuits An n-qubit gate/unitary is a $2^n \times 2^n$ unitary operation on n qubits. The identity unitary is usually denoted by $\mathbb{I}_n$. The X gate is the single-qubit gate that flips the basis $|0\rangle$ and $|1\rangle$. Single-qubit gates are known to have the following factorization.

Lemma 4 ([34], Corollary 4.2)**.** *Any single-qubit gate U can be written as $U = e^{i\alpha}AXBXC$ for some $\alpha \in \mathbb{R}$ and some single-qubit gate A, B and C satisfying $ABC = \mathbb{I}_1$.*

A CNOT gate acts on two qubits, one control qubit, and one target qubit. The gate flips the basis $|0\rangle$ and $|1\rangle$ on the target qubit, conditioned on the control qubit is on $|1\rangle$. A quantum circuit on n qubits implements a unitary transform of dimension $2^n \times 2^n$. A quantum circuit may consist of different types of gates. One typical set of gates contains all 1-qubit gates and 2-qubit CNOT gates. This is sufficient to implement any unitary transform. For notational convenience, we call this type of quantum circuits the *standard quantum circuits*. Unless otherwise stated, a circuit in this paper refers to a standard quantum circuit. A subset of circuits is *CNOT circuits*, which are the ones consisting of 2-qubit CNOT gates only.

A Toffoli gate is a 3-qubit CCNOT gate where we flip the basis $|0\rangle, |1\rangle$ of (i.e. apply X gate to) the third qubit conditioned on the first two qubits are both on $|1\rangle$. Namely, there are two control qubits and one target qubit. This can be extended to an n-fold Toffoli gate, which applies the X gate to the $(n+1)$-th qubit conditioned on the first n qubits all being on $|1\rangle$. This n-fold Toffoli gate can be implemented by a standard quantum circuit of linear depth and size without ancillary qubits [35], and of logarithmic depth and linear size if a linear number of ancillary qubits are available [36].

Lemma 5. *An n-fold Toffoli gate can be implemented by a standard quantum circuit of $O(n)$ depth and size without using any ancillary qubit and to $O(\log n)$ depth and $O(n)$ size using $O(n)$ ancillary qubits.*

A non-standard quantum circuit model is QAC^0_f circuit. A QAC^0_f circuit is a quantum circuit with one-qubit gates, unbounded-arity Toffoli

$$|x_1, \ldots, x_k, b\rangle \to |x_1, \ldots, x_k, b \oplus \prod_{i=1}^{k} x_i\rangle ,$$

and fanout gates

$$|b, x_1, \ldots, x_k\rangle \to |b, x_1 \oplus b, \ldots, x_k \oplus b\rangle .$$

CQSP, QSP, and US problems

1. The Controlled Quantum State Preparation (CQSP) problem is: Given 2^k quantum states $|\psi_i\rangle$ of n qubits, realize the transformation of

   $$|i\rangle |0^n\rangle \to |i\rangle |\psi_i\rangle , \ \forall i \in \{0,1\}^k.$$

   We sometimes write (k, n)-CQSP to emphasize the parameters.

2. The Quantum State Preparation (QSP) problem is the above CQSP problem in the special case of $k = 0$. Given a complex vector $v = (v_0, v_1, v_2, \ldots, v_{2^n-1})^T \in \mathbb{C}^{2^n}$ with $\sqrt{\sum_{j=0}^{2^n-1} |v_j|^2} = 1$, generate the corresponding n-qubit quantum state

   $$|\psi_v\rangle = \sum_{j=0}^{2^n-1} v_j |j\rangle,$$

   by a quantum circuit from the initial state $|0\rangle^{\otimes n}$, where $\{|j\rangle : j = 0, 1, \ldots, 2^n - 1\}$ is the computational basis of the quantum system. We sometimes call a quantum circuit for quantum state preparation a QSP circuit.

3. The general Unitary Synthesis (US) problem is: Given an n-qubit unitary U, find a quantum circuit to implement it.

In all these problems, we hope to find circuits as simple as possible, and standard measures for quantum circuits include depth, size (i.e. the number of gates), and number of qubits. The depth of a circuit corresponds to time and the number of qubits to space. For many information processing tasks including QSP and US, ancillary qubits turn out to be very helpful, and indeed there have been studies on quantum circuits with ancillary qubits for QSP and US. Since these tasks are often used as subroutines, it is usually desirable to have the ancillary qubits initialized to $|0\rangle$ at the beginning and are restored to $|0\rangle$ at the end. Thus we say that a quantum circuit C prepares an n-qubit quantum state $|\psi\rangle$ with m ancillary qubits if

$$C\left(|0\rangle^{\otimes n}|0\rangle^{\otimes m}\right) = |\psi\rangle|0\rangle^{\otimes m}.$$

Similarly, we call an $(n+m)$-qubit quantum circuit C implements an n-qubit unitary U using m ancillary qubits if

$$C\left(|\psi\rangle|0\rangle^{\otimes m}\right) = (U|\psi\rangle)\otimes|0\rangle^{\otimes m}, \text{ for any } n\text{-qubit state } |\psi\rangle.$$

Uniformly Controlled Unitary (UCU) Let $S=\{s_1,\ldots,s_k\}, T=\{t_1,\ldots,t_\ell\}$ and $S\cap T=\emptyset$. A *uniformly controlled unitary* V_T^S consists of 2^k controlled unitary operations, where S is the index set of the control qubits, and T is the index set of target qubits. The 2^k multiple-controlled unitary operations are conditioned on distinct basis states of the k control qubits; see Figure 2 for the circuit representation of V_T^S, where U is a shorthand for the collection of $U_0, U_1, \ldots, U_{2^k-1}$. To make the sizes of S and T explicit, we sometimes call V_T^S a (k,ℓ)-UCU. The matrix representation of V_T^S is

$$V_T^S = \begin{pmatrix} U_0 & & & \\ & U_1 & & \\ & & \ddots & \\ & & & U_{2^k-1} \end{pmatrix} \in \mathbb{C}^{2^{(k+\ell)}\times 2^{(k+\ell)}},$$

where $U_0, U_1, \ldots, U_{2^k-1} \in \mathbb{C}^{2^\ell\times 2^\ell}$ are unitary matrices. If $S=\emptyset$, V_T^S is a just an ℓ-qubit unitary operation. If $\ell=1$, the UCU is also called *uniformly controlled gate* (UCG), and we refer to k-UCG for $(k,1)$-UCU.

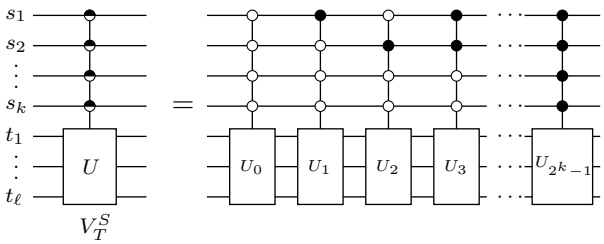

Figure 2: A uniformly controlled unitary (UCU) V_T^S, where $S=\{s_1,\ldots,s_k\}$ is the index set of the control qubits and $T=\{t_1,\ldots,t_\ell\}$ is the index set of the target qubits.

Ref. [21] gives the following size and depth upper bounds of a general UCG, which is a special case of our later Lemma 10 with $p=1$ and $q=n-1$.

Lemma 6 ([21], Lemma 12)**.** *Given m ancillary qubits, any n-qubit UCG $V_{\{n\}}^{[n-1]}$ can be implemented by a standard quantum circuit of size $O(2^n)$ and depth $O\left(n+\frac{2^n}{m+n}\right)$.*

The following framework of a QSP circuit was given in [3, 37].

Lemma 7. *The QSP problem can be solved by n UCGs of growing sizes, $V_{\{n\}}^{[n-1]} \cdots V_{\{3\}}^{[2]} V_{\{2\}}^{[1]} V_{\{1\}}^{\emptyset}$.*

Decomposition of n-qubit quantum gate Based on cosine-sine decomposition, any n-qubit unitary can be decomposed into two $(1, n-1)$-UCUs and one $(n-1)$-UCG.

Lemma 8 ([38])**.** *Any n-qubit unitary $U \in \mathbb{C}^{2^n \times 2^n}$ can be decomposed as*

$$U = \begin{pmatrix} V_1' & \\ & V_1'' \end{pmatrix} \begin{pmatrix} C & S \\ -S & C \end{pmatrix} \begin{pmatrix} V_2' & \\ & V_2'' \end{pmatrix}, \tag{1}$$

where $V_1', V_1'', V_2', V_2'' \in \mathbb{C}^{2^{n-1} \times 2^{n-1}}$ are unitary matrices, $C, S \in \mathbb{C}^{2^{n-1} \times 2^{n-1}}$ are diagonal matrices whose diagonal elements are $\cos\theta_1$, $\cos\theta_2$, ..., $\cos\theta_{2^{n-1}}$ and $\sin\theta_1$, $\sin\theta_2$, ..., $\sin\theta_{2^{n-1}}$, respectively.

The circuit representation of cosine-sine decomposition is shown in Figure 3.

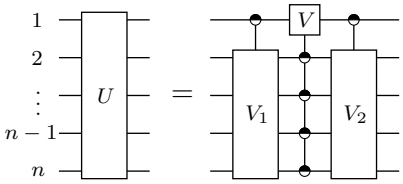

Figure 3: Cosine-sine decomposition of an n-qubit quantum gate in the language of UCU.

3 Asymptotically optimal circuit depth for (controlled) quantum state preparation

Now we give a more detailed implementation and analyze the correctness and cost of the quantum circuit. Recall that we are constructing quantum circuits to implement QSP and CQSP, without assuming any QRAM hardware available.

First, we will use the following copying circuit many times so we single it out as a lemma.

Lemma 9 ([21])**.** *For any $x = x_1 x_2 \ldots x_n \in \{0,1\}^n$, a unitary transformation U_{copy} satisfying*

$$|x\rangle |0^{mn}\rangle \xrightarrow{U_{copy}} |x\rangle \underbrace{|x\rangle |x\rangle \cdots |x\rangle}_{m \text{ copies of } |x\rangle},$$

can be implemented by a CNOT circuit of depth $O(\log m)$ and size $O(mn)$.

The next lemma says that a special type of UCU can be implemented efficiently.

Lemma 10. *For all $i \in [p]$ and $x \in \{0,1\}^q$, suppose that U_i^x is a single-qubit gate and let $L^x = \bigotimes_{i=1}^p U_i^x$. Then for any $m \geq pq$, the unitary $\sum_{x \in \{0,1\}^q} |x\rangle\langle x| \otimes L^x$ can be implemented by a standard quantum circuit of depth $O\left(\log p + q + \frac{p2^q}{m}\right)$ and size $O(p2^q)$ with m ancillary qubits.*

Proof. For any $x \in \{0,1\}^q$ and $y = y_1 \cdots y_p \in \{0,1\}^p$, unitary $\sum_{x\in\{0,1\}^q} |x\rangle\langle x| \otimes L^x$ can be realized as follows.

$$
\begin{aligned}
& |x\rangle |y\rangle |0^m\rangle \\
=\ & |x\rangle \left(\bigotimes_{i=1}^{p} |y_i\rangle |0^q\rangle_{\mathtt{R}_i} \right) |0^{m-pq}\rangle \\
\xrightarrow{U_{copy}}\ & |x\rangle \left(\bigotimes_{i=1}^{p} |y_i\rangle |x\rangle_{\mathtt{R}_i} \right) |0^{m-pq}\rangle \qquad \text{(depth } O(\log p), \text{size } O(pq), \text{ Lemma 9)} \qquad (2) \\
\xrightarrow{\bigotimes_{i=1}^{p} \sum_x U_i^x \otimes |x\rangle_{\mathtt{R}_i}\langle x|_{\mathtt{R}_i}}\ & |x\rangle \left(\bigotimes_{i=1}^{p} U_i^x |y_i\rangle |x\rangle_{\mathtt{R}_i} \right) |0^{m-pq}\rangle \qquad \left(\text{depth } O\left(q + \frac{p2^q}{m}\right), \text{ size } O(p2^q)\right) \qquad (3) \\
\xrightarrow{U_{copy}^\dagger}\ & |x\rangle \left(\bigotimes_{i=1}^{p} U_i^x |y_i\rangle |0^q\rangle_{\mathtt{R}_i} \right) |0^{m-pq}\rangle \quad \text{(depth } O(\log p), \text{size } O(pq), \text{ Lemma 9)} \qquad (4) \\
=\ & |x\rangle L^x |y\rangle |0^m\rangle
\end{aligned}
$$

The first pq ancillary qubits are divided into p registers, which are labelled as register $\mathtt{R}_1, \mathtt{R}_2, \ldots, \mathtt{R}_p$. Based on Lemma 9, we make p copies of $|x\rangle$, using a quantum circuit of depth $O(\log p)$ and size $O(pq)$ in Eq. (2). For every $i \in [p]$, we apply a q-UCG $\sum_{x\in\{0,1\}^q} U_i^x \otimes |x\rangle_{\mathtt{R}_i} \langle x|_{\mathtt{R}_i}$ on $|y_i\rangle |x\rangle_{\mathtt{R}_i}$. All these q-UCGs act on different qubits, so they can be implemented in parallel, each with $\frac{m-pq}{p}$ ancillary qubits. According to Lemma 6, Eq. (3) can be realized by a quantum circuit of depth $O\left(q + \frac{2^q}{(m-pq)/p+q}\right) = O\left(q + \frac{p2^q}{m}\right)$ and size $p \cdot O(2^q) = O(p2^q)$. In Eq. (4), we restore register $\mathtt{R}_1, \mathtt{R}_2, \ldots, \mathtt{R}_p$ by the inverse circuit of Eq. (2), of depth $O(\log p)$ and size $O(pq)$. The total depth is $2 \cdot O(\log p) + O\left(q + \frac{p2^q}{m}\right) = O\left(\log p + q + \frac{p2^q}{m}\right)$ and the total size is $2 \cdot O(pq) + O(p2^q) = O(p2^q)$. □

Two remarks are in order. First, we can compare this result to Theorem 2 in [39], which says that the unitary $\sum_{x\in\{0,1\}^q} |x\rangle \langle x| \otimes L^x$ can be implemented by a quantum circuit of depth $O(q^2 + \frac{p2^q}{m})$ using m ancillary qubits. Apart from the difference between their depth bound and ours, the assumptions are also different. On one hand, our construction works for any $m \geq pq$, while theirs needs $\sqrt{p2^q} \leq m \leq p2^q$. On the other hand, ours takes m "clean" qubits of $|0\rangle$ (and restore them afterwards), while they can handle "dirty" qubits, i.e. those with unknown content before the circuit.

Second, the above Lemma 10 extends to general UCUs: as long as each U_i in a UCU has a shallow circuit implementation, the UCU can be easily implemented.

Lemma 11. *For all $x \in \{0,1\}^q$, suppose that W^x can be implemented by a standard p-qubit quantum circuit of depth d. Then for any $m \geq pq$, the (q,p)-UCU $\sum_{x\in\{0,1\}^q} |x\rangle\langle x| \otimes W^x$ can be implemented by a standard quantum circuit of depth $O\left(\log p + dq + \frac{dp2^q}{m}\right)$ and size $O(dp2^q)$ with m ancillary qubits. In particular, if we have sufficiently many ancillary qubits, then the circuit depth for a (q,p)-UCU is $O(\log p + dq)$.*

Proof. Similar to Lemma 10, we first make p copies of $|x\rangle$ and un-copy these at the end. Between these two steps, we proceed layer by layer for the d layers of the W^x circuits.

In each layer, we use the method of Lemma 10 to handle the single-qubit gates, and use Lemma 5 to handle the q-controlled CNOT gates i.e. $(q+1)$-fold Toffoli gates.

The cost is analyzed as follows. The copy and un-copy steps take depth $O(\log p)$, size $O(pq)$, and pq ancillary qubits. In each layer, all the single-qubit gates can be handled in parallel, as we have one copy of $|x\rangle$ for each of them. Same as Lemma 10, these single-qubit gates take depth $O\left(q + \frac{p2^q}{m}\right)$, size $O(p2^q))$, and $m - pq$ ancillary qubits. Since the ancillary qubits are restored to $|0\rangle$, they can be reused in the next layer. Each CNOT layer takes $O(q)$ depth and size, without using ancillary qubits. And again these q-controlled CNOT gates i.e. $(q+1)$-fold Toffoli gates, can be paralleled as we have one copy of $|x\rangle$ for each of these Toffoli gates. Putting all these costs together gives the claimed bounds. □

3.1 Rosenthal's quantum state preparation framework

In [23] Rosenthal presents a QAC^0_f circuit of depth $O(n)$ with $O(n2^n)$ ancillary qubits for n-qubit QSP. As mentioned in [23], this result suffices to yield a standard quantum circuit for QSP, with depth $O(n)$ and $O(n2^n)$ ancillary qubits. Indeed, each k-qubit Toffoli or fanout gate can be simulated by a standard quantum circuit of depth $O(\log k)$ with $O(k)$ ancillary qubits (Lemma 5). However, the QAC^0_f circuit needs $O(n2^n)$ ancillary qubits, which is out of our parameter regime of $m \in \left[\omega\left(\frac{2^n}{n\log n}\right), o(2^n)\right]$.

Next we will analyze the QAC^0_f circuit and see how to make it suitable for any $m = \Omega(2^n/n^2)$. Let us first review Rosenthal's framework. In the following, we will use ϵ to denote the empty string. Let $\{0,1\}^{\le n} \stackrel{\text{def}}{=} \bigcup_{i=1}^{n}\{0,1\}^i \cup \{\epsilon\}$ denote the set of $\{0,1\}$ strings of length at most n, and $\{0,1\}^{<n} \stackrel{\text{def}}{=} \bigcup_{i=1}^{n-1}\{0,1\}^i \cup \{\epsilon\}$ denote the set of $\{0,1\}$ strings of length at most $n-1$. For any $x = x_1x_2\cdots x_n \in \{0,1\}^n$, let $x_{\le i}$ denote the i-bit string $x_1x_2\cdots x_i$ and $x_{<i}$ denote the $(i-1)$-bit string $x_1x_2\cdots x_{i-1}$. Let $R(\alpha)$ denote a single-qubit gate $R(\alpha) = \begin{bmatrix} 1 & \\ & e^{i\alpha} \end{bmatrix}$ for any $\alpha \in \mathbb{R}$, which puts a phase of α on $|1\rangle$ basis.

Let $|\psi_v\rangle = \sum_{x\in\{0,1\}^n} v_x |x\rangle$ denote the target quantum state. For all $x \in \{0,1\}^{<n}$, let $|x|$ denote the length of x. Define $(n-|x|)$-qubit states $\{|\psi_x\rangle : 0 \le |x| < n\}$ recursively by the equations

$$|\psi_\epsilon\rangle = |\psi_v\rangle \quad \text{and} \quad |\psi_x\rangle = \begin{cases} \beta_{x0}|0\rangle|\psi_{x0}\rangle + \beta_{x1}|1\rangle|\psi_{x1}\rangle, & \text{if } |x| \le n-2, \\ \beta_{x0}|0\rangle + \beta_{x1}|1\rangle, & \text{if } |x| = n-1, \end{cases}$$

It can be verified that $v_x = \prod_{i=1}^{n} \beta_{x\le i}$ for all $x \in \{0,1\}^n$. For all $x \in \{0,1\}^{<n}$, further define a one-qubit quantum state

$$|\phi_x\rangle = \beta_{x0}|0\rangle + \beta_{x1}|1\rangle. \tag{5}$$

Next let us define a *leaf function* $\ell : \{0,1\}^{\{0,1\}^{<n}} \to \{0,1\}^n$. The set $\{0,1\}^{\{0,1\}^{<n}}$ consists of all bit strings of length $|\{0,1\}^{<n}| = 2^n - 1$. Each string in $\{0,1\}^{\{0,1\}^{<n}}$ has its bits indexed by elements in $\{0,1\}^{<n}$. For example, $\{0,1\}^{\{0,1\}^{<3}}$ consists of 7-bit strings $z := z_\epsilon z_0 z_1 z_{00} z_{01} z_{10} z_{11}$, where $z_x \in \{0,1\}$ for all $x \in \{0,1\}^{<3}$. The leaf function is defined in the following way: Identify the input index set $\{0,1\}^{<n}$ with the vertices of the complete binary tree, with each interior vertex x having the left and right children $x0$ and $x1$, respectively. The root corresponds to the empty string ϵ. Given an input z, $\ell(z)$ is the leaf that the following walk from the root lead to: at any interior node x, move to the left or right child if $z_x = 0$ or 1, respectively. For example, given an input $z := z_\epsilon z_0 z_1 z_{00} z_{01} z_{10} z_{11}$=0110010, $\ell(z)$ is obtained as follows. First, since $z_\epsilon = 0$, we move to the left child of ϵ, which is labeled by 0. Second, since $z_0 = 1$, we move to the right child

of 0, which is labeled by 01 and is the leaf node $\ell(z)$, i.e. $\ell(z) = 01$. It can be verified that

$$\ell(z)_j = \bigvee_{t\in\{0,1\}^j : t_j = 1} \bigwedge_{i\in[j]} [z_{t_{<i}} = t_i], \forall j \in [n],$$

where

$$[z_{t_{<i}} = t_i] = \begin{cases} 1 & \text{if } z_{t_{<i}} = t_i, \\ 0 & \text{if } z_{t_{<i}} \neq t_i \end{cases}.$$

Also define a corresponding $(2^n + n - 1)$-qubit unitary transformation U_ℓ by

$$U_\ell \left|z, a\right\rangle = \left|z, a \oplus \ell(z)\right\rangle, \quad \forall z \in \{0,1\}^{\{0,1\}^{<n}}, \forall a \in \{0,1\}^n. \tag{6}$$

In the rest of this section, $\mathtt{R}_x$ is a one-qubit register for each $x \in \{0,1\}^n$, and $\mathtt{S}$ is an n-qubit register.

The QSP algorithm in [23] can be summarized as follows.

Lemma 12. *Any n-qubit quantum state $|\psi\rangle$ can be generated by the following three steps:*

1. $|0\rangle_{\mathtt{R}_x} \to |\phi_x\rangle_{\mathtt{R}_x}$, *for all* $x \in \{0,1\}^{<n}$.
2. *Apply* U_ℓ *to* $\bigotimes_{x\in\{0,1\}^{<n}} |\phi_x\rangle_{\mathtt{R}_x} \otimes |0^n\rangle_{\mathtt{S}}$.
3. *Apply* $\Gamma^\dagger$, *where* Γ *is any unitary satisfying*

$$|t\rangle_{\mathtt{S}} \bigotimes_{x\in\{0,1\}^{<n}} |0\rangle_{\mathtt{R}_x} \xrightarrow{\Gamma} |t\rangle_{\mathtt{S}} \bigotimes_{x\in\{0,1\}^{<n}} \begin{cases} |t_i\rangle_{\mathtt{R}_x} & \text{if } x = t_{<i} \text{ for some } i \in [n], \\ |\phi_x\rangle_{\mathtt{R}_x}, & \text{otherwise,} \end{cases} \quad \forall t \in \{0,1\}^n. \tag{7}$$

For correctness please refer to [23], and here we focus on the implementation and the corresponding analysis in a way suitable for our later circuit construction.

The first step of the algorithm consists of single-qubit rotations on $2^n - 1$ qubits, and thus naturally has depth 1 and size $2^n - 1$. We denote by L_1^v this step of operation, where the superscript emphasizes that the gate parameters depend on the target vector $v \in \mathbb{C}^{2^n}$.

As shown in [23], the second step can be implemented by a QAC_f^0 circuit on $O(n2^n)$ qubits, which transfers to a standard circuit of depth $O(n)$ and size $O(n2^n)$, with $O(n2^n)$ ancillary qubits. We also note that this second step is independent of the target state. We denote by C_1' the circuit of this step, where the absence of superscript v emphasizes the independence of the target state.

The third step, though also of depth $O(n)$ and size $O(n2^n)$ with $O(n2^n)$ ancillary qubits, unfortunately, depends on the target vector v. This brings us some difficulty for small m, and we will show how to handle it next.

3.2 Implementation: separating depth and dependence on the target state

In this section we will show how to implement the third step in Rosenthal's algorithm in such a way that (1) it has a constant number of rounds, some deep and some shallow, (2) deep rounds have depth $O(n)$, but are independent of the target vector v, (3) shallow rounds each have depth 1, and depend on v. This separation of depth and dependence is useful for our later construction of efficient circuits. The circuit and these conditions are formalized in the following lemma.

Lemma 13. *A unitary transformation $\Gamma^\dagger$ satisfying Eq.(7) can be implemented by a standard quantum circuit of the following form*

$$\Gamma^\dagger = C_5 L_5^v C_4 L_4^v C_3 L_3^v C_2 L_2^v C_1''.$$

Here each $L_i^v = \bigotimes_{k=1}^{s_i} U_k^{i,v}$ is a depth-1 circuit consisting of $s_i = O(2^n)$ single-qubit gates with $U_k^{i,v}$ determined by $|\psi_v\rangle$. C_1'', $C_2, \ldots, C_5$ are all independent of $|\psi_v\rangle$; C_1'', C_4 and C_5 are circuits of depth $O(n)$ and size $O(n2^n)$, and C_2 and C_3 are circuits of depth $O(1)$ and size $O(2^n)$.

Proof. We first introduce notation $C_{\mathtt{R}_x}^{\mathtt{S},y}(V)$: For any $y = y_1 \cdots y_\ell \in \{0,1\}^{\leq n}$, $C_{\mathtt{R}_x}^{\mathtt{S},y}(V)$ is a unitary operation acting on an n-qubit register $\mathtt{S}$ (the first n qubits) and 1-qubit register $\mathtt{R}_x$ (the last qubit) as follows

$$C_{\mathtt{R}_x}^{\mathtt{S},y}(V) \stackrel{\text{def}}{=} |y\rangle\langle y| \otimes \mathbb{I}_{n-\ell} \otimes V + \sum_{y' \in \{0,1\}^\ell - \{y\}} |y'\rangle\langle y'| \otimes \mathbb{I}_{n-\ell} \otimes \mathbb{I}_1,$$

The unitary $C_{\mathtt{R}_x}^{\mathtt{S},y}(V)$ makes the following transformation

$$|t\rangle_{\mathtt{S}} |0\rangle_{\mathtt{R}_x} \to |t\rangle_{\mathtt{S}} V^{[t_{\leq \ell} = y]} |0\rangle_{\mathtt{R}_x}, \tag{8}$$

where

$$[t_{\leq \ell} = y] \stackrel{\text{def}}{=} \begin{cases} 1, & \text{if } t_{\leq \ell} = y, \\ 0, & \text{if } t_{\leq \ell} \neq y. \end{cases}$$

By introducing an ancillary qubit called register $\mathtt{A}$, $C_{\mathtt{R}_x}^{\mathtt{S},y}(V)$ can be implemented by the quantum circuit in Figure 4. In the quantum circuit, the single-qubit gate $A, B, C, R(\alpha)$ satisfy $V = e^{i\alpha} AXBXC$ and $ABC = \mathbb{I}_1$ (Lemma 4).

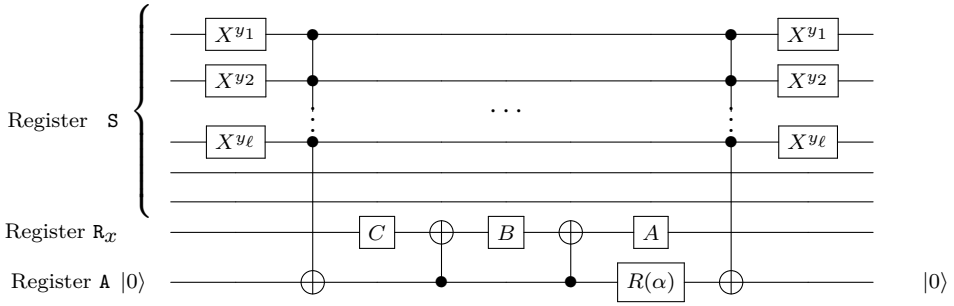

Figure 4: Quantum circuit for $C_{\mathtt{R}_x}^{\mathtt{S},y}(V)$. Register $\mathtt{A}$ is an ancillary qubit. Single-qubit gate $A, B, C, R(\alpha)$ satisfy $V = e^{i\alpha} AXBXC$ and $ABC = \mathbb{I}_1$.

According to Figure 4, we can rewrite the circuit of $C_{\mathtt{R}_x}^{\mathtt{S},y}(V)$:

$$C_{\mathtt{R}_x}^{\mathtt{S},y}(V) = W_y^2 \underbrace{(\mathbb{I}_n \otimes A \otimes R(\alpha))}_{D_V^3} (\mathbb{I}_n \otimes CNOT_{\mathtt{R}_x}^{\mathtt{A}}) \underbrace{(\mathbb{I}_n \otimes B \otimes \mathbb{I}_1)}_{D_V^2} (\mathbb{I}_n \otimes CNOT_{\mathtt{R}_x}^{\mathtt{A}}) \underbrace{(\mathbb{I}_n \otimes C \otimes \mathbb{I}_1)}_{D_V^1} W_y^1, \tag{9}$$

where W_y^1, W_y^2 are defined as

$$W_y^1 := \mathsf{Tof}_{\mathtt{A}}^{\mathtt{S}} (\bigotimes_{i=1}^{y_\ell} X^{y_i}),$$
$$W_y^2 := (\bigotimes_{i=1}^{y_\ell} X^{y_i}) \mathsf{Tof}_{\mathtt{A}}^{\mathtt{S}},$$

and $\mathsf{Tof}_{\mathtt{A}}^{\mathtt{S}}$ is a Toffoli gate whose control qubits are in $\mathtt{S}$ and target qubit is in $\mathtt{A}$. Because any n-qubit Toffoli gate can be implemented by a quantum circuit of depth $O(n)$ based on Lemma 5, W_y^1, W_y^2 can be implemented by a quantum circuit of depth $O(n)$. Unitary D_v^1, D_V^2 consists of single-qubit gates and D_V^3 consists of 2 single-qubit gates. The total depth of $C_{\mathtt{R}_x}^{\mathtt{S},y}(V)$ is $O(n)$. It is worth mentioning that in the circuit construction of $C_{\mathtt{R}_x}^{\mathtt{S},y}(V)$, only D_V^1, D_V^2, D_V^3 depend on unitary V.

Now we start the circuit construction of Γ. For all $x \in \{0,1\}^{<n}$, let U_x denote a single-qubit gate satisfying $U_x|0\rangle = |\phi_x\rangle$. First, we implement the following transformation $\Gamma_{\mathtt{R}_x}^{\mathtt{S},x}$ on register $\mathtt{S}$ and $\mathtt{R}_x$ by the method in Figure 4:

$$|t\rangle_{\mathtt{S}}|0\rangle_{\mathtt{R}_x} \to |t\rangle_{\mathtt{S}} \begin{cases} |t_i\rangle_{\mathtt{R}_x}, & \text{if } x = t_{<i} \text{ for some } i \in [n], \\ |\phi_x\rangle_{\mathtt{R}_x}, & \text{otherwise,} \end{cases} \qquad \forall t \in \{0,1\}^n. \tag{10}$$

This needs depth and size $O(n)$ with 1 ancillary qubit:

$$\begin{aligned}
& |t\rangle_{\mathtt{S}}|0\rangle_{\mathtt{R}_x}|0\rangle_{\mathtt{A}} \\
\xrightarrow{\mathbb{I}_n \otimes U_x} & |t\rangle_{\mathtt{S}}|\phi_x\rangle_{\mathtt{R}_x}|0\rangle_{\mathtt{A}} && \text{(depth 1, size 1)} && (11) \\
\xrightarrow{C_{\mathtt{R}_x}^{\mathtt{S},x}(U_x^\dagger)} & |t\rangle_{\mathtt{S}} \begin{cases} |0\rangle_{\mathtt{R}_x}, & \text{if } x = t_{<i} \text{ for some } i \in [n] \\ |\phi_x\rangle_{\mathtt{R}_x}, & \text{otherwise} \end{cases} |0\rangle_{\mathtt{A}} && \text{(depth } O(n), \text{ size } O(n)) && (12) \\
\xrightarrow{C_{\mathtt{R}_x}^{\mathtt{S},x1}(X)} & |t\rangle_{\mathtt{S}} \begin{cases} |t_i\rangle_{\mathtt{R}_x}, & \text{if } x = t_{<i} \text{ for some } i \in [n] \\ |\phi_x\rangle_{\mathtt{R}_x}, & \text{otherwise} \end{cases} |0\rangle_{\mathtt{A}} && \text{(depth } O(n), \text{ size } O(n)) && (13)
\end{aligned}$$

For each $x \in \{0,1\}^{<n}$, $\mathtt{S}_x$ denotes a register which stores a copy of $|t\rangle$ in register $\mathtt{S}$. Base on the construction of $\Gamma_{\mathtt{R}_x}^{\mathtt{S}_x,x}$, we can now implement Γ by a quantum circuit of depth $O(n)$ and size $O(n2^n)$ with $(n+1)(2^n-1)$ ancillary qubits. To compress the depth, we first make a copy of $|t\rangle$ for each $x \in \{0,1\}^{<n}$.

$$\begin{aligned}
& |t\rangle_{\mathtt{S}} \left(\bigotimes_{x\in\{0,1\}^{<n}} |0\rangle_{\mathtt{R}_x} \right) |0^{(n+1)(2^n-1)}\rangle \\
= & |t\rangle_{\mathtt{S}} \bigotimes_{x\in\{0,1\}^{<n}} \left(|0\rangle_{\mathtt{R}_x} |0^n\rangle_{\mathtt{S}_x} |0\rangle_{\mathtt{A}_x} \right) && (14) \\
\xrightarrow{U_{copy}} & |t\rangle_{\mathtt{S}} \bigotimes_{x\in\{0,1\}^{<n}} \left(|0\rangle_{\mathtt{R}_x} |t\rangle_{\mathtt{S}_x} |0\rangle_{\mathtt{A}_x} \right) && (15) \\
\xrightarrow{\bigotimes_{x\in\{0,1\}^{<n}} \Gamma_{\mathtt{R}_x}^{\mathtt{S}_x,x}} & |t\rangle_{\mathtt{S}} \bigotimes_{x\in\{0,1\}^{<n}} \left(\begin{cases} |t_i\rangle_{\mathtt{R}_x}, & \text{if } x = t_{<i} \text{ for some } i \in [n], \\ |\phi_x\rangle_{\mathtt{R}_x}, & \text{otherwise.} \end{cases} |t\rangle_{\mathtt{S}_x} |0\rangle_{\mathtt{A}_x} \right) && (16) \\
\xrightarrow{U_{copy}^\dagger} & |t\rangle_{\mathtt{S}} \bigotimes_{x\in\{0,1\}^{<n}} \left(\begin{cases} |t_i\rangle_{\mathtt{R}_x}, & \text{if } x = t_{<i} \text{ for some } i \in [n], \\ |\phi_x\rangle_{\mathtt{R}_x}, & \text{otherwise.} \end{cases} |0^n\rangle_{\mathtt{S}_x} |0\rangle_{\mathtt{A}_x} \right) && (17) \\
= & |t\rangle_{\mathtt{S}} \left(\bigotimes_{x\in\{0,1\}^{<n}} \begin{cases} |t_i\rangle_{\mathtt{R}_x}, & \text{if } x = t_{<i} \text{ for some } i \in [n], \\ |\phi_x\rangle_{\mathtt{R}_x}, & \text{otherwise.} \end{cases} \right) |0^{(n+1)(2^n-1)}\rangle .
\end{aligned}$$

Here all the three transformation steps have depth $O(n)$ and size $O(n2^n)$, by Lemma 9 and the analysis in Eq.(11)-(13).

For every $U_x^\dagger$, $C_{\mathtt{R}_x}^{S_x,x}(U_x^\dagger)$ can be represented as

$$C_{\mathtt{R}_x}^{S_x,x}(U_x^\dagger) = W_x^2 D_{U_x^\dagger}^3 CNOT_{\mathtt{R}_x}^{\mathtt{A}_x} D_{U_x^\dagger}^2 CNOT_{\mathtt{R}_x}^{\mathtt{A}_x} D_{U_x^\dagger}^1 W_x^1, \tag{18}$$

as discussed in Eq. (9). $D_{U_x^\dagger}^1, D_{U_x^\dagger}^2$ are single-qubit gate respectively and $D_{U_x^\dagger}^3$ consists of 2 single-qubit gates which are determined by $U_x^\dagger$ (or by target quantum state $|\psi_v\rangle$). W_x^1, W_x^2 are quantum circuits of depth $O(n)$, independent of $|\psi_v\rangle$. As discussed above, Γ is represented as

$$\begin{aligned}
\Gamma &= U_{copy}^\dagger \left(\bigotimes_{x\in\{0,1\}^{<n}} \Gamma_{\mathtt{R}_x}^{S_x,x} \right) U_{copy}, \\
&= U_{copy}^\dagger \bigotimes_{x\in\{0,1\}^{<n}} (C_{\mathtt{R}_x}^{\mathtt{S}_x,x1}(X) W_x^2 D_{U_x^\dagger}^3 CNOT_{\mathtt{R}_x}^{\mathtt{A}_x} D_{U_x^\dagger}^2 CNOT_{\mathtt{R}_x}^{\mathtt{A}_x} D_{U_x^\dagger}^1 W_x^1 U_x) U_{copy}, \\
&= \underbrace{U_{copy}^\dagger \bigotimes_{x\in\{0,1\}^{<n}} (C_{\mathtt{R}_x}^{\mathtt{S}_x,x1}(X) W_x^2)}_{(C_1'')^\dagger} \underbrace{\bigotimes_{x\in\{0,1\}^{<n}} D_{U_x^\dagger}^3}_{(L_2^v)^\dagger} \underbrace{\bigotimes_{x\in\{0,1\}^{<n}} CNOT_{\mathtt{R}_x}^{\mathtt{A}_x}}_{(C_2)^\dagger} \\
&\quad \underbrace{\bigotimes_{x\in\{0,1\}^{<n}} D_{U_x^\dagger}^2}_{(L_3^v)^\dagger} \underbrace{\bigotimes_{x\in\{0,1\}^{<n}} CNOT_{\mathtt{R}_x}^{\mathtt{A}_x}}_{(C_3)^\dagger} \underbrace{\bigotimes_{x\in\{0,1\}^{<n}} D_{U_x^\dagger}^1}_{(L_4^v)^\dagger} \underbrace{\bigotimes_{x\in\{0,1\}^{<n}} W_x^1}_{(C_4)^\dagger} \underbrace{\bigotimes_{x\in\{0,1\}^{<n}} U_x}_{(L_5^v)^\dagger} \underbrace{U_{copy}}_{(C_5)^\dagger}.
\end{aligned}$$

The conclusion for the decomposition of $\Gamma^\dagger$ then follows. For the cost analysis: According to Eq. (18), $(L_2^v)^\dagger, (L_3^v)^\dagger, (L_4^v)^\dagger, (L_5^v)^\dagger$ are depth-1 circuits consisting of $O(2^n)$ single-qubit gates, which are determined by target state $|\psi_v\rangle$. According to Lemma 9, Figure 4, Eq. (13) and (18), $(C_1'')^\dagger$, $(C_4)^\dagger$ and $(C_5)^\dagger$ are quantum circuits of depth $O(n)$ and size $O(n2^n)$. Based on Eq. (18), $(C_2)^\dagger, (C_3)^\dagger$ are quantum circuits of depth $O(1)$ and size $O(2^n)$. This completes the proof. □

Recall that C_1' is the second step U_ℓ in Lemma 12. Now letting $C_1 = C_1'' C_1'$, we get the following result.

Lemma 14. *Any n-qubit quantum state $|\psi_v\rangle$ can be generated by a quantum circuit QSP_v, using single-qubit gates and CNOT gates, of depth $O(n)$ and size $O(n2^n)$, with $O(n2^n)$ ancillary qubits. The QSP circuit can be written as*

$$QSP_v = C_5 L_5^v C_4 L_4^v C_3 L_3^v C_2 L_2^v C_1 L_1^v.$$

Each $L_i^v = \bigotimes_{k=1}^{s_i} U_k^{i,v}$ is a depth-1 circuit consisting of $s_i = O(2^n)$ single-qubit gates, and L_i^v is determined by $|\psi_v\rangle$. C_1, C_4 and C_5 are circuits of depth $O(n)$ and size $O(n2^n)$, and C_2 and C_3 are circuits of depth $O(1)$ and size $O(2^n)$. For any $i \in [5]$, C_i is independent of $|\psi_v\rangle$.

3.3 Quantum circuit for (controlled) quantum state preparation

Next, we will use Lemma 14 to efficiently realize the controlled quantum state preparation. Let us fix a constant c in the size upper bound of L_i^v in Lemma 14, i.e. $s_i \le c \cdot 2^n$. The next lemma is a restatement of the upper bound part of Theorem 1.

Lemma 15. *For any $k \ge 0$ and quantum states $\{|\psi_i\rangle : i \in \{0,1\}^k\}$, the following controlled quantum state preparation*

$$|i\rangle |0^n\rangle \to |i\rangle |\psi_i\rangle, \ \forall i \in \{0,1\}^k,$$

can be implemented by a standard quantum circuit of depth $O\left(n+k+\frac{2^{n+k}}{n+k+m}\right)$ *and size* $O\left(2^{n+k}\right)$ *with* m *ancillary qubits.*

Proof. We consider two cases depending on m.

Case 1: $m = O(2^{n+k}/(n+k)^2)$**.** Let QSP_i denote the QSP circuit for generating quantum state $|\psi_i\rangle$ on qubits $\{k+1, k+2, \cdots, k+n\}$ obtained from Lemma 7, then QSP_i can be decomposed into n UCGs:

$$QSP_i = V_{\{n+k\}}^{\{k+1,k+2,\cdots,n+k-1\}}(i)\cdots V_{\{k+3\}}^{\{k+1,k+2\}}(i)V_{\{k+2\}}^{\{k+1\}}(i)V_{\{k+1\}}^{\emptyset}(i).$$

Therefore, the controlled quantum state preparation can be implemented as

$$\begin{aligned}
&\sum_{i\in\{0,1\}^k} |i\rangle\langle i| \otimes QSP_i \\
=&\sum_{i\in\{0,1\}^k} |i\rangle\langle i| \otimes (V_{\{n+k\}}^{\{k+1,k+2,\cdots,n+k-1\}}(i)\cdots V_{\{k+3\}}^{\{k+1,k+2\}}(i)V_{\{k+2\}}^{\{k+1\}}(i)V_{\{k+1\}}^{\emptyset}(i)) \\
=&V_{\{n+k\}}^{[n+k-1]}\cdots V_{\{k+3\}}^{[k+2]}V_{\{k+2\}}^{[k+1]}V_{\{k+1\}}^{[k]}.
\end{aligned}$$

For all $i \in [n]$, UCG $V_{\{k+i\}}^{[k+i-1]}$ can be implemented by a quantum circuit of depth $O\left(k+i+\frac{2^{k+i}}{k+i+m}\right)$ and size $O(2^{k+i})$ by Lemma 6, using m ancillary qubits. Therefore, the depth and size of this CQSP circuit are $\sum_{i=1}^{n} O\left(k+i+\frac{2^{k+i}}{k+i+m}\right) = O\left(\frac{2^{n+k}}{m+n+k}\right)$ and $\sum_{i=1}^{n} O\left(2^{k+i}\right) = O\left(2^{n+k}\right)$, respectively.

Case 2: $m = \Omega(2^{n+k}/(n+k)^2)$**.** We will show the quantum circuit for CQSP in two sub-cases: $k \geq \lceil 4\log(n+k)\rceil$ and $k < \lceil 4\log(n+k)\rceil$.

Case 2.1: $k \geq \lceil 4\log(n+k)\rceil$**.** Then $m \geq \max\{2cn2^n, k2^n\}$ for any constant $c > 0$. For all $i \in \{0,1\}^k$, suppose $|\psi_i\rangle = \sum_{j=0}^{2^n-1} v_j^i |j\rangle$. Let QSP_i denote a QSP circuit with $m_1 = cn2^n$ ancillary qubits as guaranteed by Lemma 14 to prepare $|\psi_i\rangle$, which can be represented as

$$QSP_i = C_5L_5^iC_4L_4^iC_3L_3^iC_2L_2^iC_1L_1^i.$$

Here each $L_r^i = \bigotimes_{j=0}^{s_r} U_j^{r,i}$ is a depth-1 circuit consisting of $s_r = O(2^n)$ single-qubit gates, and L_r^i is determined by $|\psi_i\rangle$. For $r \in [5]$, C_r is an $(n+m_1)$-qubit circuit of depth $O(n)$, which is independent of $|\psi_i\rangle$. Note that the task in the statement of this lemma is nothing but the UCU of $\{QSP_i\}$, which can be implemented by applying $\sum_{i\in\{0,1\}^k} |i\rangle\langle i| \otimes QSP_i$. This operator can be decomposed as follows.

$$\begin{aligned}
&\sum_{i\in\{0,1\}^k} |i\rangle\langle i| \otimes QSP_i \\
=&\sum_{i\in\{0,1\}^k} |i\rangle\langle i| \otimes (C_5L_5^iC_4L_4^iC_3L_3^iC_2L_2^iC_1L_1^i) \qquad (19)\\
=&\prod_{r=5}^{1}\left[(\mathbb{I}_t\otimes C_r)\Big(\sum_{i\in\{0,1\}^k} |i\rangle\langle i| \otimes L_r^i\Big)\right].
\end{aligned}$$

where the notation $\prod_{r=5}^{1} A_r$ means to multiply the matrices A_r's in the order of $A_5A_4A_3A_2A_1$. The second equation above holds because, when viewed as matrices, the equation is just a block diagonal matrix multiplication:

$$\begin{aligned}
&\mathrm{diag}(C_5L_5^0C_4L_4^0C_3L_3^0C_2L_2^0C_1L_1^0, \cdots, C_5L_5^{2^k-1}C_4L_4^{2^k-1}C_3L_3^{2^k-1}C_2L_2^{2^k-1}C_1L_1^{2^k-1}) \qquad (20)\\
=&\mathrm{diag}(C_5,\cdots,C_5)\times\mathrm{diag}(L_5^0,\cdots,L_5^{2^k-1})\times\mathrm{diag}(C_4,\cdots,C_4)\times\cdots\times\mathrm{diag}(L_1^0,\cdots,L_1^{2^k-1}).
\end{aligned}$$

In the m ancillary qubits, we used m_1 for the UCU $\{QSP_i\}$, and have $m - m_1$ left. Since $m \geq k2^n$, we can apply Lemma 10 (where $q = k$ and $p \leq c2^n$) and obtain that, for every $r \in [5]$, $\sum_{i\in\{0,1\}^k} |i\rangle\langle i| \otimes L_r^i$ can be implemented by a quantum circuit of depth

$$O\left(n + k + \frac{2^n \cdot 2^k}{m - cn2^n}\right) = O\left(n + k + \frac{2^{n+k}}{m - cn2^n}\right),$$

and size $O\left(2^n \times 2^k\right) = O(2^{n+k})$, with the $m - m_1$ ancillary qubits. For $r \in [5]$, every C_r is a quantum circuit of depth $O(n)$ and size $O\left(n2^n\right)$. Putting everything together and noting $m \geq 2cn2^n$, we can implement $\sum_{i\in\{0,1\}^k} |i\rangle\langle i| \otimes QSP_i$ by a quantum circuit of depth $O\left(n + k + \frac{2^{n+k}}{m-cn2^n}\right) = O\left(n + k + \frac{2^{n+k}}{m}\right)$ and size $O\left(2^{n+k} + n2^n\right) = O(2^{n+k})$, with m ancillary qubits.

Case 2.2 $k < \lceil 4\log(n+k)\rceil$**.** Define n-qubit quantum state $|\psi_i\rangle = \sum_{\tau=0}^{2^n-1} v_{\tau,i} |\tau\rangle$ and $|\psi_i^{(s)}\rangle = \sum_{\eta=0}^{2^s-1} v'_{\eta,i} |\eta\rangle$, where $s \leq n$ and $v'_{\eta,i} = \sqrt{\sum_{p=0}^{2^{n-s}-1} |v_{\eta\cdot 2^{n-s}+p,i}|^2}$. Our construction consists of two steps. In the first step, we implement a $\lceil 4\log(n+k)\rceil$-qubit CQSP, using $m = \Omega(2^{n+k}/(n+k)^2)$ ancillary qubits:

$$\text{CQSP1}: \ |i\rangle |0^n\rangle \to |i\rangle |\psi_i^{(s)}\rangle |0^{n+k-\lceil 4\log(n+k)\rceil}\rangle, \forall i \in \{0,1\}^k, \tag{21}$$

where $s = \lceil 4\log(n+k)\rceil - k$. Note that k and s satisfy $m > \max\{2cs2^s, k2^s\}$, thus similar to Case 2.1 above, we can implement Eq. (21) by a circuit of depth $O(\log(n+k))$ and size $O((n+k)^4)$. In the second step, we implement an $(n+k)$-qubit CQSP using m ancillary qubits:

$$\text{CQSP2}: \ |i\rangle |\eta\rangle |0^{(n+k)-\lceil 4\log(n+k)\rceil}\rangle \to |i\rangle |\eta\rangle |\phi_{i,\eta}\rangle, \forall i \in \{0,1\}^k, \eta \in \{0\} \cup [2^s - 1], \tag{22}$$

where $|\phi_{i,\eta}\rangle \stackrel{\text{def}}{=} \sum_{p=0}^{2^{(n+k)-\lceil 4\log(n+k)\rceil}} v_{\eta\cdot 2^{(n+k)-\lceil 4\log(n+k)\rceil}+p,i}/v'_{\eta,i} |p\rangle$. Eq. (22) is a CQSP, in which the number of controlled qubits $\lceil 4\log(n+k)\rceil$ satisfying $m > \max\{2c((n+k) - \lceil 4\log(n+k)\rceil)2^{(n+k)-\lceil 4\log(n+k)\rceil}, \lceil 4\log(n+k)\rceil 2^{(n+k)-\lceil 4\log(n+k)\rceil}\}$. Therefore Eq. (22) can be implemented in the same way as in Case 2.1, such that the depth and size are $O\left(n + k + \frac{2^{n+k}}{n+k+m}\right)$ and $O(2^{n+k})$, respectively. It can be verified that the CQSP operator can be implemented by CQSP2 $\cdot$ CQSP1 and the depth and size are $O\left(n + k + \frac{2^{n+k}}{n+k+m}\right)$ and $O(2^{n+k})$, respectively.

□

The paper [21] presents an n-qubit QSP circuit with m ancillary qubits. For $m \in \left[0, O\left(\frac{2^n}{n\log n}\right)\right] \cup \left[\Omega(2^n), +\infty\right)$, the circuit depth for n-qubit quantum state preparation is optimal. However, if $m \in \left[\omega\left(\frac{2^n}{n\log n}\right), o(2^n)\right]$, there still exists a logarithmic gap between the upper and lower bounds of QSP circuit depth. Since our Theorem 1 gives a unified construction that works for any k, including $k = 0$, we obtain Theorem 2, which closes the gap left open in [21].

Remarks

1. In [20], it was shown that any n-qubit quantum states are determined by $2^n - 1$ free parameters omitting a global phase. In Theorem 1, an $(n+k)$-qubit CQSP is defined by 2^k n-qubit quantum states. Therefore, it is determined by $2^k \cdot 2^n - 1 = 2^{n+k} - 1$ free parameters. Thus by a similar argument for the depth lower bound of the quantum state preparation in [20], we can get a depth lower bound for (k,n)-qubit CQSP is $\Omega\left(\frac{2^{n+k}}{n+k+m}\right)$ using m ancillary qubits.

Moreover, the same as the proof of Lemma 37 in [21], we can also obtain a depth lower bound $\Omega(n+k)$ by the light cone argument. Combining the two results above, the depth lower bound for CQSP is $\Omega\left(n+k+\frac{2^{n+k}}{n+k+m}\right)$. Therefore, the circuit depth in Theorem 1 is optimal.

2. If the number of controlled qubits k in Theorem 1 is 0, the CQSP degenerates to standard QSP. Therefore, we can obtain an optimal QSP circuit as in Theorem 2.

4 Circuit depth optimization of general unitary synthesis

The following oracle is used in the circuit constructions in [23].

Definition 16 (Oracle O_U of U)**.** *Let $U=[u_{y,x}]_{y,x\in\{0,1\}^n}\in\mathbb{C}^{2^n\times 2^n}$ denote a general n-qubit unitary operator. Let vector $u_x\in\mathbb{C}^{2^n}$ denote the x-th column of U and $|u_x\rangle=\sum_{y\in\{0,1\}^n}u_{y,x}|y\rangle$ is the corresponding n-qubit quantum state. The following unitary transformation O_U is defined as the U-oracle:*

$$|x\rangle|0^n\rangle\xrightarrow{O_U}|x\rangle|u_x\rangle\,, \text{for all } x\in\{0,1\}^n.$$

This oracle is defined as an intermediate step of the circuit construction. Note that O_U prepares the state $|u_x\rangle$ in the second register conditioned on the first register being $|x\rangle$. Given O_U, it is not immediate how to implement U, which changes $|x\rangle$ to $|u_x\rangle$ in place. However, we can indeed implement U if we are allowed to use many queries to O_U and $O_U^\dagger$. First, we can directly apply Theorem 1 to obtain the following circuit construction for the oracle.

Lemma 17. *For any $m\geq 0$ and $U\in\mathbb{C}^{2^n\times 2^n}$, the U-oracle O_U and its inverse $O_U^\dagger$ can each be implemented by a standard quantum circuit of depth $O\left(n+\frac{4^n}{n+m}\right)$ and size $O(4^n)$ with m ancillary qubits.*

Remarks

1. Ref. [23] gives a construction for O_U and $O_U^\dagger$ with $O(n)$ depth using $m=\Theta(n4^n)$ ancillary qubits. In comparison, our Theorem 1 only needs $m=\Theta(4^n/n)$ ancillary qubits to achieve $O(n)$ depth, and works for any $m\geq 0$.

2. Since Theorem 1 is tight for all values of parameters (n,k,m), the bounds in Lemma 17 are also optimal.

Lemma 18 ([23])**.** *For any $m\in[n,O(4^n/n)]$, any n-qubit unitary U can be implemented by $\ell=O\left(2^{n/2}\right)$ many queries to oracle O_U or $O_U^\dagger$:*

$$(U|\phi\rangle)|0\rangle^{\otimes m}=C_\ell O_U^{(\dagger)}C_{\ell-1}O_U^{(\dagger)}C_{\ell-2}O_U^{(\dagger)}\cdots C_2O_U^{(\dagger)}C_1\left(|\phi\rangle|0\rangle^{\otimes m}\right),\ \text{for all } n\text{-qubit states } |\phi\rangle\,,$$

where $O_U^{(\dagger)}$ denotes either the oracle O_U or $O_U^\dagger$, and each C_i is a standard quantum circuit of depth $O(\log m)$ and size $O(m)$, and is independent of U.

By Lemma 17 and 18, we can obtain the following corollary.

Corollary 19. *For any $m\in[n,O(4^n/n)]$, any n-qubit unitary can be implemented by a standard quantum circuit of depth $O\left(n2^{n/2}+\frac{2^{5n/2}}{m}\right)$, using m ancillary qubits.*

Proof. By Lemma 18, we obtain a quantum circuit of $\ell = O(2^{n/2})$ queries to O_U and $O_U^\dagger$, with the total depth between queries is the summation of that of C_i's, which is $\ell \cdot O(\log m)$. By Lemma 17, each query to O_U and $O_U^\dagger$ can be implemented by a circuit of depth $O(n + \frac{4^n}{(m-n)+n})$. Putting the two together, we obtain a circuit of depth

$$O(2^{n/2}) \cdot \Big(\log m + n + \frac{4^n}{(m-n)+n}\Big) = O\Big(n2^{n/2} + \frac{2^{5n/2}}{m}\Big).$$

□

If the number of ancillary qubits is large, this bound improves the previous depth bound of $O(n2^n)$ in [21]. Next, we will show how to further improve the circuit depth for the parameter regime $\Omega(2^n) \leq m \leq O(4^n)$ by cosine-sine decomposition and the following UCU. Note that each cosine-sine decomposition (Lemma 8) reduces a general unitary to two $(1, n-1)$-UCUs and one $(n-1)$-UCG. One can continue this decomposition to further decrease the number of the target qubits to $n-2$, $n-3$, and so on. But it turns out that going all the way down to 1 target qubit does not give the most efficient construction. To see where to stop using the cosine-sine decomposition, we need to understand the circuit complexity of an $(n-k, k)$-UCU for a general k, which is the subject of the next lemma.

Lemma 20. *Let $T = \{n-k+1, n-k+2, \ldots, n\}$ and $S = [n] - T$ for any $k \in \{2, 3, \ldots, n\}$. For any $m \in [n, O(4^n/n)]$, any $(n-k, k)$-UCU V_T^S can be implemented by a quantum circuit of depth $O\left(n2^{k/2} + \frac{2^{n+\frac{3}{2}k}}{m}\right)$ and size $O\left(m2^{k/2} + 2^{n+3k/2}\right)$, with m ancillary qubits.*

Proof. We will implement V_T^S by an $(n+m)$-qubit quantum circuit. The idea is to implement each $(n-k)$-qubit controlled k-qubit unitary U_x by Lemma 18. Observe that these $(n-k)$-qubit controlled qubits can be combined with the k controlled qubits in the definition of oracle O_{U_x} (Definition 16), to form an (n, k)-CQSP. Then we invoke Lemma 15 to implement them and obtain the bounds.

According to Lemma 18, for all $x \in \{0,1\}^{n-k}$, any k-qubit unitary $U_x \in \mathbb{C}^{2^k \times 2^k}$ acting on qubits $\{n-k+1, n-k+2, \ldots, n\}$ can be implemented by $O(2^{k/2})$ queries to the $2k$-qubit oracles O_{U_x} and $O_{U_x}^\dagger$. Here each O_{U_x} is on $2k$ qubits, k of which is for U_x and the other k using ancillary qubits. Using the notation $O_{U_x}^{(\dagger)}$ to denote oracle O_{U_x} or $O_{U_x}^\dagger$, we have that

$$(U_x |\phi\rangle) |0\rangle^{\otimes m} = C_\ell O_{U_x}^{(\dagger)} C_{\ell-1} O_{U_x}^{(\dagger)} \cdots C_2 O_{U_x}^{(\dagger)} C_1 \left(|\phi\rangle |0\rangle^{\otimes m}\right), \text{for all } n\text{-qubit states } |\phi\rangle$$

where $\ell = O(2^{k/2})$ and $C_1, \ldots, C_\ell$ are depth-$O(\log m)$ and size-$O(m)$ quantum circuits independent of U_x. Any n-qubit UCU V_T^S can thus be implemented as follows

$$\begin{aligned} V_T^S &= \sum_{x\in\{0,1\}^{n-k}} |x\rangle\langle x| \otimes U_x, \\ &= \sum_{x\in\{0,1\}^{n-k}} |x\rangle\langle x| \otimes \left[C_\ell O_{U_x}^{(\dagger)} C_{\ell-1} O_{U_x}^{(\dagger)} \cdots C_2 O_{U_x}^{(\dagger)} C_1\right], \\ &= [\mathbb{I}_{n-k} \otimes C_\ell]\Big(\sum_{x\in\{0,1\}^{n-k}} |x\rangle\langle x| \otimes O_{U_x}^{(\dagger)}\Big) \cdots [\mathbb{I}_{n-k} \otimes C_2]\Big(\sum_{x\in\{0,1\}^{n-k}} |x\rangle\langle x| \otimes O_{U_x}^{(\dagger)}\Big)[\mathbb{I}_{n-k} \otimes C_1], \end{aligned} \tag{23}$$

where we switched the summation and multiplication again because of the block diagonal matrix as for Eq. (20). Now we implement $\sum_{x\in\{0,1\}^{n-k}} |x\rangle\langle x| \otimes O_{U_x}^{(\dagger)}$. It can be regarded as

a controlled quantum state preparation, which has n controlled qubits and k target qubits. Hence, by Lemma 15, we can implement it by a circuit of depth $O\left(n+k+\frac{2^{n+k}}{n+k+(m-k)}\right) = O\left(n+\frac{2^{n+k}}{m}\right)$ and size $O\left(2^{n+k}\right)$. Therefore by Eq. (23), for any $m \in [n, O(4^n/n)]$, unitary V_T^S can be realized by a circuit of depth

$$O(2^{k/2}) \cdot O\Big(n+\frac{2^{n+k}}{m}\Big) + O(2^{k/2}) \cdot O(\log m) = O\Big(n2^{k/2} + \frac{2^{n+\frac{3}{2}k}}{m}\Big),$$

and size

$$O(2^{k/2}) \cdot O\Big(2^{n+k}\Big) + O(2^{k/2}) \cdot O(m) = O\Big(m2^{k/2} + 2^{n+3k/2}\Big).$$

□

Remarks.

1. **Extension of UCG**. In [21], it was shown that any n-UCG can be implemented by a standard circuit of depth $O(n + 2^n/(m+n))$. Lemma 20 generalizes this result to any k.

2. **Tightness**. In [27], it was shown that any n-qubit unitary is determined by $4^n - 1$ free parameters omitting a global phase. Because UCU V_T^S in Lemma 20 are defined by 2^{n-k} different k-qubit unitaries, it is determined by $2^{n-k} \cdot 4^k - 1 = 2^{n+k} - 1$ free parameters. Similar to the depth lower bound for general unitary in [21], given m ancillary qubits, the depth lower bound for UCU V_T^S is $\Omega\left(\frac{2^{n+k}}{n+m}\right)$. Moreover, we can also obtain a depth lower bound $\Omega(n)$ by the light cone. This proof of is the same as the proof of depth lower bound for quantum state preparation in [21]. Combining the two results above, giving $m \geq 0$ ancillary qubits, the depth lower bound for UCU V_T^S is $\Omega\left(n+\frac{2^{n+k}}{n+m}\right)$. When $k = O(1)$, the depth in Lemma 20 is asymptotically optimal. The case for general k is left as an interesting open question.

Theorem 21 (Restatement of Theorem 3)**.** *For any $m \geq 0$, any n-qubit unitary U can be implemented by a standard quantum circuit with m ancillary qubits of depth*

$$\begin{cases} O\left(\frac{4^n}{m}\right), & \text{if } m = O\left(\frac{2^n}{n}\right), \\ O\left(\frac{n^{1/2}2^{3n/2}}{m^{1/2}}\right), & \text{if } m \in [\Omega\left(2^n/n\right), O(4^n/n)], \\ O\left(n2^{n/2}\right) & \text{if } m = \Omega(\frac{4^n}{n}). \end{cases}$$

and one of size

$$\begin{cases} O\left(4^n\right), & \text{if } m = O\left(2^n\right), \\ O\left(2^{3n/2}m^{1/2}\right), & \text{if } m \in [\Omega\left(2^n/n\right), O(4^n)], \\ O\left(2^{5n/2}\right), & \text{if } m = \Omega\left(4^n\right). \end{cases}$$

Proof. Let $D_n(k,m)$ and $S_n(k,m)$ denote the minimum circuit depth and size, respectively, of a general n-qubit UCU $V_{\{n-k+1,\ldots,n\}}^{[n-k]}$ with m ancillary qubits. Especially, $D_n(n,m)$ and $S_n(n,m)$ denote the minimum depth and size of an n-qubit unitary U. According to cosine-sine decomposition in Figure 3, for every $k \in [n]$ we have

$$\begin{aligned} D_n(n,m) &\leq 2D_n(n-1,m) + D_n(1,m) && \text{(Eq.(1))} \\ &= 2D_n(n-1,m) + O\Big(n+\frac{2^n}{m}\Big) && \text{(Lemma 6)} \\ &\leq 2^{n-k}D_n(k,m) + O\Big(n2^{n-k} + \frac{2^{2n-k}}{m}\Big) && \text{(by recursion)} \end{aligned}$$

and

$$\begin{aligned} S_n(n,m) &\leq 2S_n(n-1,m) + S_n(1,m) && \text{(Eq.(1))} \\ &= 2S_n(n-1,m) + O\left(2^n\right) && \text{(Lemma 6)} \\ &\leq 2^{n-k}S_n(k,m) + \left(2^{n-k}-1\right) \times O\left(2^n\right) && \text{(by recursion)} \\ &= 2^{n-k}S_n(k,m) + O\left(2^{2n-k}\right). \end{aligned}$$

Now we use Lemma 20, $D_n(k,m) = O\left(n2^{k/2} + \frac{2^{n+\frac{3}{2}k}}{m}\right)$ and $S_n(k,m) = O\left(m2^{k/2} + 2^{n+3k/2}\right)$. Hence, for any $k \in [n]$ we have

$$\begin{aligned} D_n(n,m) &= 2^{n-k} \times O\Big(n2^{k/2} + \frac{2^{n+\frac{3}{2}k}}{m}\Big) + O\Big(n2^{n-k} + \frac{2^{2n-k}}{m}\Big) = O\Big(n2^{n-\frac{k}{2}} + \frac{2^{2n+\frac{1}{2}k}}{m}\Big), \\ S_n(n,m) &= 2^{n-k} \times O\left(m2^{k/2} + 2^{n+3k/2}\right) + O\left(2^{2n-k}\right) = O\left(m2^{n-k/2} + 2^{2n+k/2}\right). \end{aligned}$$

When $m = O(2^n/n)$, we take $k = 1$, and get depth $D_n(n,m) \leq O(4^n/m)$. When $\Omega(2^n/n) \leq m \leq O(4^n/n)$, we take $k = \log m + \log n - n$, and get depth $D_n(n,m) \leq O\left(\frac{n^{1/2}2^{3n/2}}{m^{1/2}}\right)$. When $m = \Omega(4^n/n)$, we take $k = n$, and get depth $D_n(n,m) \leq O(n2^{n/2})$. This completes the proof for the depth. The size follows a similar argument: For $m = O(2^n)$, $\Omega(2^n) \leq m \leq O(4^n)$ and $m = \Omega(4^n)$, we take $k = 1$, $k = \log m - n$, and $k = n$, respectively, obtaining the size upper bound $S_n(n,m) = O(4^n)$, $O(2^{2n/2}m^{1/2})$, and $O(2^{5n/2})$, respectively. This completes the proof. □

Acknowledgments We thank Jonathan Allcock for discussions on the background of QRAM.

References

[1] Jacob Biamonte, Peter Wittek, Nicola Pancotti, Patrick Rebentrost, Nathan Wiebe, and Seth Lloyd. "Quantum machine learning". Nature **549**, 195–202 (2017).

[2] Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost. "Quantum principal component analysis". Nature Physics **10**, 631–633 (2014).

[3] Iordanis Kerenidis and Anupam Prakash. "Quantum Recommendation Systems". In Christos H. Papadimitriou, editor, 8th Innovations in Theoretical Computer Science Conference (ITCS 2017). Volume 67 of Leibniz International Proceedings in Informatics (LIPIcs), pages 49:1–49:21. Dagstuhl, Germany (2017). Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[4] Patrick Rebentrost, Adrian Steffens, Iman Marvian, and Seth Lloyd. "Quantum singular-value decomposition of nonsparse low-rank matrices". Phys. Rev. A **97**, 012327 (2018).

[5] Aram W. Harrow, Avinatan Hassidim, and Seth Lloyd. "Quantum algorithm for linear systems of equations". Phys. Rev. Lett. **103**, 150502 (2009).

[6] Leonard Wossnig, Zhikuan Zhao, and Anupam Prakash. "Quantum linear system algorithm for dense matrices". Phys. Rev. Lett. **120**, 050502 (2018).

[7] Iordanis Kerenidis, Jonas Landman, Alessandro Luongo, and Anupam Prakash. "q-means: a quantum algorithm for unsupervised machine learning". In Advances in Neural Information Processing Systems. Volume 32, pages 4134–4144. (2019).

[8] Iordanis Kerenidis and Jonas Landman. "Quantum spectral clustering". Phys. Rev. A **103**, 042415 (2021).

[9] Patrick Rebentrost, Masoud Mohseni, and Seth Lloyd. "Quantum support vector machine for big data classification". Phys. Rev. Lett. **113**, 130503 (2014).

[10] Dominic W. Berry, Andrew M. Childs, Richard Cleve, Robin Kothari, and Rolando D. Somma. "Simulating hamiltonian dynamics with a truncated taylor series". Phys. Rev. Lett. **114**, 090502 (2015).

[11] Guang Hao Low and Isaac L. Chuang. "Optimal hamiltonian simulation by quantum signal processing". Phys. Rev. Lett. **118**, 010501 (2017).

[12] Guang Hao Low and Isaac L. Chuang. "Hamiltonian Simulation by Qubitization". Quantum **3**, 163 (2019).

[13] Dominic W. Berry, Andrew M. Childs, and Robin Kothari. "Hamiltonian simulation with nearly optimal dependence on all parameters". In 2015 IEEE 56th Annual Symposium on Foundations of Computer Science. Pages 792–809. (2015).

[14] Mario Szegedy. "Quantum speed-up of markov chain based algorithms". In 45th Annual IEEE Symposium on Foundations of Computer Science. Pages 32–41. (2004).

[15] Frédéric Magniez, Ashwin Nayak, Jérémie Roland, and Miklos Santha. "Search via quantum walk". SIAM Journal on Computing **40**, 142–164 (2011).

[16] Daniel K. Park, Francesco Petruccione, and June-Koo Kevin Rhee. "Circuit-based quantum random access memory for classical data". Scientific Reports **9**, 3949 (2019).

[17] Tiago M. L. de Veras, Ismael C. S. de Araujo, Daniel K. Park, and Adenilton J. da Silva. "Circuit-based quantum random access memory for classical data with continuous amplitudes". IEEE Transactions on Computers **70**, 2125–2135 (2021).

[18] Olivia Di Matteo, Vlad Gheorghiu, and Michele Mosca. "Fault-tolerant resource estimation of quantum random-access memories". IEEE Transactions on Quantum Engineering **1**, 1–13 (2020).

[19] Ville Bergholm, Juha J. Vartiainen, Mikko Möttönen, and Martti M. Salomaa. "Quantum circuits with uniformly controlled one-qubit gates". Phys. Rev. A **71**, 052330 (2005).

[20] Martin Plesch and Časlav Brukner. "Quantum-state preparation with universal gate decompositions". Phys. Rev. A **83**, 032302 (2011).

[21] Xiaoming Sun, Guojing Tian, Shuai Yang, Pei Yuan, and Shengyu Zhang. "Asymptotically optimal circuit depth for quantum state preparation and general unitary synthesis" (2021) arXiv:2108.06150v3.

[22] Xiao-Ming Zhang, Man-Hong Yung, and Xiao Yuan. "Low-depth quantum state preparation". Phys. Rev. Res. **3**, 043200 (2021).

[23] Gregory Rosenthal. "Query and depth upper bounds for quantum unitaries via grover search" (2021). arXiv:2111.07992.

[24] Xiao-Ming Zhang, Tongyang Li, and Xiao Yuan. "Quantum state preparation with optimal circuit depth: Implementations and applications". Phys. Rev. Lett. **129**, 230504 (2022).

[25] Sonika Johri, Shantanu Debnath, Avinash Mocherla, Alexandros SINGK, Anupam Prakash, Jungsang Kim, and Iordanis Kerenidis. "Nearest centroid classification on a trapped ion quantum computer". npj Quantum Information **7**, 122 (2021).

[26] Zhicheng Zhang, Qisheng Wang, and Mingsheng Ying. "Parallel quantum algorithm for hamiltonian simulation" (2021). arXiv:2105.11889.

[27] Vivek V. Shende, Igor L. Markov, and Stephen S. Bullock. "Minimal universal two-qubit controlled-not-based circuits". Phys. Rev. A **69**, 062321 (2004).

[28] Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter. "Elementary gates for quantum computation". Phys. Rev. A **52**, 3457–3467 (1995).

[29] Emanuel Knill. "Approximation by quantum circuits" (1995). arXiv:quant-ph/9508006.

[30] Juha J. Vartiainen, Mikko Möttönen, and Martti M. Salomaa. "Efficient decomposition of quantum gates". Phys. Rev. Lett. **92**, 177902 (2004).

[31] M Mottonen and Juha J Vartiainen. "Decompositions of general quantum gates" (2005). arXiv:quant-ph/0504100.

[32] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. "Quantum random access memory". Phys. Rev. Lett. **100**, 160501 (2008).

[33] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. "Architectures for a quantum random access memory". Phys. Rev. A **78**, 052310 (2008).

[34] Michael A. Nielsen and Isaac L. Chuang. "Quantum computation and quantum information: 10th anniversary edition". Cambridge University Press. (2010).

[35] Craig Gidney. "Using quantum gates instead of ancilla bits". `https://algassert.com/circuits/2015/06/22/Using-Quantum-Gates-instead-of-Ancilla-Bits.html`.

[36] Jonathan M Baker, Casey Duckering, Alexander Hoover, and Frederic T Chong. "Decomposing quantum generalized toffoli with an arbitrary number of ancilla" (2019). arXiv:1904.01671.

[37] Lov Grover and Terry Rudolph. "Creating superpositions that correspond to efficiently integrable probability distributions" (2002). arXiv:quant-ph/0208112.

[38] C.C. Paige and M. Wei. "History and generality of the cs decomposition". Linear Algebra and its Applications **208-209**, 303–326 (1994).

[39] Guang Hao Low, Vadym Kliuchnikov, and Luke Schaeffer. "Trading t-gates for dirty qubits in state preparation and unitary synthesis" (2018). arXiv:1812.00954.