Circuit complexity of quantum access models for encoding classical data

Check for updates

Xiao-Ming Zhang [1,2,3,4] ✉ & Xiao Yuan [3,4]

How to efficiently encode classical data is a fundamental task in quantum computing. While many existing works treat classical data encoding as a black box in oracle-based quantum algorithms, their explicit constructions are crucial for the efficiency of practical algorithm implementations. Here, we unveil the mystery of the classical data encoding black box and study the Clifford $+ T$ complexity in constructing several typical quantum access models. For general matrices (even including sparse ones), we prove that sparse-access input models and block-encoding both require nearly linear circuit complexities relative to the matrix dimension. We also give construction protocols achieving near-optimal gate complexities. On the other hand, the construction becomes efficient with respect to the data qubit when the matrix is a linear combination of polynomial terms of efficiently implementable unitaries. As a typical example, we propose improved block-encoding when these unitaries are Pauli strings. Our protocols are built upon improved quantum state preparation and a select oracle for Pauli strings, which hold independent values. Our access model constructions provide considerable flexibility, allowing for tunable ancillary qubit numbers and offering corresponding space-time trade-offs.

Quantum computing offers speedups over the classical counterpart in different tasks, including factoring, searching, simulation, etc[1]. However, the speedups, in many cases, rely on the existence of efficient oracles or access models to encode the related classical data[2]. In this context, a function $f(x)$ representing the classical data of interest is encoded using a unitary operation U_f, which acts as an oracle in the computation. To study quantum advantages, the number of queries to U_f in a quantum algorithm is compared to the number of queries to $f(x)$ in classical algorithms. Quantum computing provides substantial reduction in query complexity for many problems of practical importance[3–5].

There are various access models to encode classical data. One commonly used access model is the sparse-access input model (SAIM)[4–12], which encodes general sparse matrices and outputs the value or position of the non-zero elements when provided with appropriate inputs. SAIM is initially introduced for Hamiltonian simulation and discrete quantum walks[4,6–8], and has then found broad applications in other fields such as machine learning[5,9,11] and classical oscillator simulations[12]. For example, the quantum linear system problem could be solved with $\tilde{O}(\kappa)$ queries to SAIM[5,9,10], where κ represents the condition number of the matrix to be inverted.

Another important access model is block-encoding, which serves as a crucial subroutine for quantum signal processing[13,14] and its generalization —quantum singular-value transformations (QSVT)[10,15]. The success of block-encoding enables the realization of Hamiltonian simulation with an optimal query complexity[13,14]. Furthermore, many seminal quantum algorithms, including Grover's algorithm, quantum Fourier transformation, and the HHL algorithm, could be viewed as special cases of QSVT, where the problem of interest is encoded using block-encoding[15].

Many existing works treat access models as black boxes for convenience. However, the actual circuit complexity of the algorithm also depends on the cost of each query to these access models. While being important, this problem only draws much attention very recently with many basic problems still left open. In particular, ref. 16 presents a nearly time-optimal protocol for block-encoding of general dense matrices of $2^n \times 2^n$ dimension. A circuit depth of $\tilde{O}(n)$ can be achieved at the expense of exponential ancillary qubits. ref. 17 examines matrices with D data each appearing M times and considers examples including checkerboard matrices and tridiagonal matrices with polynomial circuit complexities. However, the cost of block-encoding of more general matrices remains

[1]Key Laboratory of Atomic and Subatomic Structure and Quantum Control (Ministry of Education), Guangdong Basic Research Center of Excellence for Structure and Fundamental Interactions of Matter, School of Physics, South China Normal University, Guangzhou 510006, China. [2]Guangdong Provincial Key Laboratory of Quantum Engineering and Quantum Materials, Guangdong-Hong Kong Joint Laboratory of Quantum Matter, Frontier Research Institute for Physics, South China Normal University, Guangzhou 510006, China. [3]Center on Frontiers of Computing Studies, Peking University, 100871 Beijing, China. [4]School of Computer Science, Peking University, 100871 Beijing, China. ✉e-mail: phyxmz@gmail.com

unexplored. Moreover, it is still unclear if there is a fundamental limit to the resource required by data encoding.

In this work, we provide a framework of constructing quantum access models in the fault-tolerant setting using Clifford + T gates. The protocol works for general classical data and takes the underlying structure of the data, such as sparsity and linear combintaion of unitaries (LCU), into consideration. Our results represent a direct mapping from the query complexity of quantum algorithms to their practical circuit complexity. Our protocols allow tunable ancillary qubit numbers and offer space-time trade-off. For general sparse matrices of dimension $2^n = N$, we investigate the SAIM and block-encoding. For both access models, we first show that the gate count lower bound increases about linearly with respect to N. We then develop construction algorithms with varying ancillary qubit numbers ranging from $\Omega(n)$ to $O(N)$. Across the entire range of qubit numbers, we achieve nearly optimal circuit complexity. We next study the block-encoding of LCU. Efficient block-encoding is achievable when the matrix can be represented as a linear combination of a polynomial number of unitaries, which can be implemented using polynomial-size quantum circuits.

Our access model construction relies on optimized realizations of various subroutines that are independently valuable, including quantum state preparation, selective oracles for Pauli strings, and sparse Boolean functions. In all the listed operations, we achieve improved or at least comparable circuit complexities compared to the best-known realizations.

We now introduce the definition of SAIM and block-encoding in below. Let $N = 2^n$, we consider a sparse matrix $H \in \mathbb{C}^{N \times N}$ with at most $s = O(1)$ nonzero elements at each row and column. Let $H_{x,y}$ be the value of the element at the xth row and yth column, and each $H_{x,y}$ is a d-digit integer ($d = O(1)$). Let idx denote a $2n$-qubit index register, and wrd denote an n-qubit word register, the sparse-access input model (SAIM) corresponds to two unitaries O_H, O_F, which satisfies

$$O_H|x, y\rangle_{\text{idx}}|z\rangle_{\text{wrd}} = |x, y\rangle_{\text{idx}}|z \oplus H_{x,y}\rangle_{\text{wrd}}, \tag{1a}$$

$$O_F|x, k\rangle_{\text{idx}} = |x, F(x, k)\rangle_{\text{idx}}. \tag{1b}$$

Here, $F(x, k)$ is the column index of the kth nonzero element in row x. Due to its simplicity and generality, Eq. (1) becomes one of the standard access models in quantum computing, which is usually assumed to be available in processing classical data.

We call a unitary U the block encoding of H if we have

$$\alpha\big(\langle 0^{n_{\text{anc}}}| \otimes \mathbb{I}_N\big) U \big(|0^{n_{\text{anc}}}\rangle \otimes \mathbb{I}_N\big) = H,$$

where $\alpha > 0$ is the normalization factor, n_{anc} is the number of ancillary qubits, and $\mathbb{I}_N$ is the N-dimensional identity. In practice, we may consider approximated construction of the block-encoding. More specifically, we call unitary $\tilde{U}$ an $(\alpha, n_{\text{anc}}, \varepsilon)$ − block-encoding of H if

$$\big\|H - \alpha\big(\langle 0^{n_{\text{anc}}}| \otimes \mathbb{I}_N\big) \tilde{U} \big(|0^{n_{\text{anc}}}\rangle \otimes \mathbb{I}_N\big)\big\| \leqslant \varepsilon \tag{2}$$

for error parameter $\varepsilon \geq 0$. Throughout our manuscript, $\|\cdot\|$ represents either the spectral norm for matrices or Euclidean norm for vectors. For a general N-dimensional matrix H, the construction of its block-encoding requires $\Omega(\text{Poly}(N))$ gate count. This is true even for sparse H as we show in Supplementary Discussion 2.

On the other hand, when H has some other structures, the resource may be significantly reduced. In particular, we consider H in the form of a linear combination of unitaries (LCU) as

$$H = \sum_{p=0}^{P-1} \alpha_p u_p, \tag{3}$$

where u_p are n-qubit unitaries that can be implemented with polynomial-size quantum circuit, and $P = O(\text{poly}(n))$. The concept "LCU" appeared

firstly in[18]. The main purpose of ref. 18 and the follow-up work ref. 19 is to realize non-unitary transformation on quantum computers. In the context of Hamiltonian simulation, ref. 20 has shown that LCU-based method can outperform product formula based methods. Many subsequent works with different applications have then been inspired[14,15,21–23].

Without loss of generality, we may assume that $\log_2 P$ is an integer, and $\sum_{p=0}^{P-1} \alpha_p = 1$. This can always be satisfied by adding terms with zero amplitude, and rescaling the Hamiltonian. In particular, the linear combination of Pauli strings

$$H = \sum_{p=0}^{P-1} \alpha_p H_p \tag{4}$$

will be studied in details. Here, $\alpha_p > 0, P \geqslant 1, H_p = \bigotimes_{l=1}^{n} H_{p,l}$, and $H_{p,l} \in \{\pm I, \pm X, \pm Y, \pm Z\}$ are single-qubit Pauli operators. Eq. (4) is important as it corresponds to the Hamiltonian of almost all physical quantum systems, such as the spin and molecular systems.

In our constructions, we consider the fault-tolerant quantum computing setting. More specifically, we only use two-qubit Clifford gate and single-qubit T gate, which is equivalent to the elementary gate set $\mathcal{G}_{\text{clf}+T} \equiv \{H, S, T, \text{CNOT}\}$. All gates in $\mathcal{G}_{\text{clf}+T}$ are error-correctable with surface code[24]. We benchmark the circuit complexity of a given quantum circuit with three quantities: total number of elementary gates, total qubit number (including data qubits and ancillary qubits), and circuit depth. We will also discuss the space-time trade-off of our algorithm, i.e. the circuit depth under a certain number of ancillary qubits. We also allow at least $O(n)$ ancillary qubits, because this does not increase the total space complexity.

Results
Circuit complexity lower bound

Before discussing the access model construction, we first study the lower bound of the circuit complexity. We will focus on the encoding of sparse matrices. The methodology here is general and can be readily applied to other related problems.

Our strategy is as follows. Firstly, we analyze the *capacity* of a quantum circuit with bounded resource, i.e. how much unique unitaries can be constructed, given fixed number of elementary gates or circuit depth. Secondly, we analyze the *size* of the access model, i.e. the number of unique unitaries required to approximate the access model with arbitrary parameters. The circuit complexity can then be estimated by comparing the capacity of a quantum circuit and the size of the access model. All proofs of our lemma and theorems in this section are provided in Supplementary Discussion 1.

Quantum circuit capacity. Assuming that we are given a finite two-qubit elementary gate set $\mathcal{G}_{\text{ele}}$. We define $g \equiv |\mathcal{G}_{\text{ele}}| = O(1)$ with $|\cdot|$ the number of elements in the set. Our first result is that the capacity can be lower bounded only with the number of elementary gates, independent of the space and time resources.

Lemma 1. Let $\mathcal{G}_C$ be the set containing all n-qubit unitaries that can be constructed with C elementary gates in $\mathcal{G}_{\text{ele}}$. Then, we have $\log|\mathcal{G}_C| = O\big((C\log(C+n))\big)$, even with unlimited ancillary qubit number.

Lemma 1 implies that the capacity does not always increase with ancillary qubit number, which can be understood as follows. All ancillary qubits should be uncomputed at the end of the circuit. When C is fixed, only finite number of unitaries can satisfy this requirement, while constructable by those elementary gates. We also note that the circuit depth D is bounded by C, so Lemma 1 also implies a relation between capacity and circuit depth.

On the other hand, when the ancillary qubit number and circuit depth are finite, the lower bound of capacity can be tighten as follows.

Lemma 2. Let $\mathcal{G}'_{n_{\mathrm{anc}},D}$ be the set containing all unitaries that can be constructed with n_{anc} ancillary qubits and D circuit depth. Then, we have $\log|\mathcal{G}'_{n_{\mathrm{anc}},D}| = O\big(D(n + n_{\mathrm{anc}})\big)$.

Lemma 1, 2 represent the ultimate representational power of quantum circuits constructed with local gates. Lemma 1 and 2 can be used to estimate the circuit complexity lower bound whenever the tasks have requirement on $|\mathcal{G}_C|$ or $|\mathcal{G}'_{n_{\mathrm{anc}},D}|$. Moreover, similar results can be obtained straightforwardly for other type of elementary gate sets, such as k-local operations with $k > 2$.

Circuit complexity for encoding sparse matrices. With Lemma 1 and 2, we now estimate the circuit complexity lower bound for accessing sparse matrices. For SAIM, it turns out that at least $\Omega(N!)$ unique unitaries are required to cover the set of all SAIM for 1-sparse matrices. So according to Lemma 1, 2, we have the following result.

Theorem 1. Given an arbitrary finite two-qubit elementary gate set $\mathcal{G}_{\mathrm{ele}}$. Let n_{anc}, D and C be the number of ancillary qubits, circuit depth and total number of gates in $\mathcal{G}_{\mathrm{ele}}$ required to approximate SAIM in Eq. (1) with any accuracy $\varepsilon < 1$. Then, we have $(n + n_{\mathrm{anc}})D = \Omega(2^n n)$ and $C = \Omega(2^n)$.

A similar result is also obtained for the block-encoding of sparse matrix as follows.

Theorem 2. Given an arbitrary finite two-qubit elementary gate set $\mathcal{G}_{\mathrm{ele}}$. Let n_{anc}, D and C be the number of ancillary qubits, circuit depth and total number of gates in $\mathcal{G}_{\mathrm{ele}}$ required to construct the block-encoding of H with any accuracy $\varepsilon < 2$. Then, we have $(n + n_{\mathrm{anc}})D = \Omega(N)$ and $C = \Omega(N^\alpha)$ for arbitrary $\alpha \in (0, 1)$.

Theorem 1, 2 imply that a general sparse matrix can not be encoded with subexponential quantum gates, for both SAIM and block-encoding. It is possible to trade ancillary qubit numbers for the circuit depth. However, the space and time complexities can not achieve sub-exponential scaling simultaneously. The hardness of SAIM can be interpreted as follows. Although H is assumed to be sparse ($O(1)$ nonzero elements at each row and column), there are still totally $2^n \times O(1) = O(2^n)$ number of independent variables in total. Therefore, the quantum circuit should be large enough to contain exponential number of elementary gates.

We note that the quantum circuits capacity for ancillary-free case has been studied in Section 4.5.4 of[1]. Moreover, a related result to Theorem 1 has obtained in[25], which gives a distinct quantum circuit number lower bound with fixed qubit number, and show that there exists a table of size N requiring $\Omega(N)$ gate count. ref. [1] allows approximated implementations, but does not consider ancillary qubit usage. ref. [25] implicitly allows ancillary qubits, but does not consider approximated implementations. On the contrary, our results are more general, because both ancillary qubit usage and approximated implementations are allowed. Our results can be generalized from unitary to quantum channels. In Supplementary Discussion 1, we show that the circuit capacity and circuit lower bound are similar if we consider two-qubit quantum channels as elementary quantum operations, which can include measurement and feedback controls.

Quantum state preparation
Quantum state preparation is a critical step of our access model construction and of independent interest. We say that a $(n + n_{\mathrm{anc}})$ qubit unitary G prepares the n-qubit quantum state $|\psi\rangle$ with accuracy ε if

$$G(|0^n\rangle \otimes |0^{n_{\mathrm{anc}}}\rangle) = |\tilde{\psi}\rangle \otimes |0^{n_{\mathrm{anc}}}\rangle \qquad (5)$$

for some $\||\psi\rangle - |\tilde{\psi}\rangle\| \leqslant \varepsilon$.

Such a problem has been studied extensively[16,26–37]. When given sufficiently large among of ancillary qubits, the optimal Clifford $+$ T depth $O(n + \log(1/\varepsilon))$ can be achieved[37]. However, with restricted ancillary qubit number, the optimal circuit depth has not been reached. For example, with $O(n)$ ancillary qubits, the best-known Clifford $+$ T construction has achieved $O((N/n)\log(N/\varepsilon))$ circuit depths[32]. Besides, for gate count scaling, all existing algorithms have either $O(N\mathrm{poly}(n))$ or $O(N\mathrm{polylog}(n))$

Table 1 | Clifford+T complexities of n-qubit state preparation protocols with fixed accuracy ε and total qubit (data qubit + ancillary qubit) number $O(n)$

Protocols	Count	Depth
ref. [26–29]	$O(N\,\mathrm{poly}\,(n))$	$O(N\,\mathrm{poly}\,(n))$
ref. [38]	$O(N\log(n))$	$O(N)$
ref. [32]	$O(Nn)$	$O(N)$
Theorem. 3	$O(N)$	$O\!\left(N^{\frac{\log n(\log\log n)}{n}}\right)$

Note: The ε scaling of Clifford $+$ T count and depth are $O(\log(1/\varepsilon))$ for all protocols. The ε scaling of qubit number is $O(\log(1/\varepsilon))$ for ref. [38] and $O(1)$ for all other schemes. ref. [38] also minimize T complexities.

Table 2 | Clifford+T complexities of n-qubit state preparation protocols with fixed ε and exponential ancillary qubits

Protocols	Count	Depth
ref. [32,33]	$O(Nn)$	$O(n^2)$
ref. [16,38]	$O(N\log n)$	$O(n^2)$
ref. [34]*	$O(N\log n)$	$O(n\log n)$
ref. [37]	$O(N\log n)$	$O(n)$
Theorem. 3*	$O(N)$	$O(n\log n)$

Note: The ε scaling of Clifford $+$ T count and depth are $O(\log(1/\varepsilon))$ for all schemes. Total qubit numbers are $O(N\mathrm{poly}(n))$ for ref. [33], $O(N\log(1/\varepsilon))$ for ref. [38], and $O(N)$ for all other protocols. ref. [38] and ref. [16] also minimize T complexities. Protocols labeled * only require sparse connectivity, i.e. each qubit connect to $O(1)$ of other qubits.

Clifford $+$ T count. It remains an outstanding question if a linear gate count scaling with respect to the data dimension N can be reached.

Here, we provide a family of improved quantum state preparation protocols with tunable ancillary qubit number. The result is summarized in below (follows directly from Theorem 8 in Methods).

Theorem 3. With n_{anc} ancillary qubits where $\Omega(n) \leqslant n_{\mathrm{anc}} \leqslant O(N)$, an arbitrary n-qubit quantum state can be prepared to accuracy ε with $O(N\log(1/\varepsilon))$ count and $\tilde{O}\!\left(N\log(1/\varepsilon)\frac{\log(n_{\mathrm{anc}})}{n_{\mathrm{anc}}}\right)$ depth of Clifford $+$ T gates, where $\tilde{O}$ suppresses the doubly logarithmic factors of n_{anc}.

Theorem 3 achieves linear scaling of Clifford $+$ T count with respect to N, and this is applied for arbitrary space complexity. When $n_{\mathrm{anc}} = O(n)$, the circuit depth is lower than the best-known result of $O\!\left(N\frac{\log(N/\varepsilon)}{n}\right)$. Moreover, compared to[32] which also study the space-time trade-off of state preparation, our method improves the circuit depth scaling for a factor of $\tilde{O}(n_{\mathrm{anc}}/\log n_{\mathrm{anc}})$. Summary of some representative state preparation protocols are provided in Table 1 and Table 2.

The main idea of our construction is as follows (see also Fig. 1). For $n_{\mathrm{anc}} = O(n)$, we construct the quantum state with a set of uniformly controlled rotations (UCR) with the method in[28]. Instead of decomposing each UCR with identical accuracy, we distribute the decomposition error in an optimized way. UCR with m controlled qubits, denoted as m-UCR, should be decomposed into 2^m number of m-qubit controlled rotations. When performing Clifford $+$ T decomposition, to reduce the total circuit complexity, we allow larger decomposition accuracy when m becomes larger.

For $n_{\mathrm{anc}} = O(N)$, we improve the Clifford $+$ T decomposition of the method in[34] in a similar way. In both cases, the gate count scaling $O(N\log(1/\varepsilon))$ is achieved. For arbitrary ancillary qubit number between two extreme cases, we provide a scheme combing two protocols together, which allows space-time trade-off. Details of our state preparation scheme and the corresponding complexity analysis are provided in Methods. We also note that our protocol for few qubit case can be combined with the
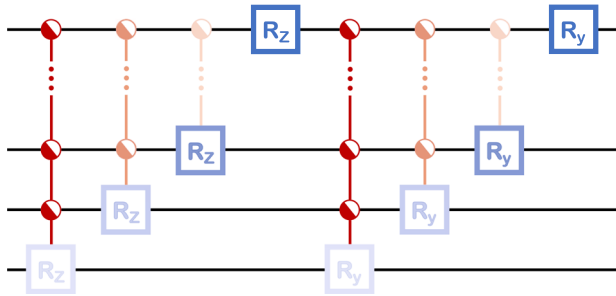
Fig. 1 | State preparation achieving $O(N)$ Clifford + T count for few qubit case. The operation is decomposed into uniformly controlled Z- and Y-rotations, whose control and rotation parts are denoted with red and blue colors respectively. Each m-UCR is decomposed into 2^m multi-qubit controlled single-qubit rotations, and m increases with the opacity of the control part (red). Each Z- or Y-rotation is decomposed into Clifford + T gates, and the decomposition accuracy increases with the opacity of the rotation part (blue).

Table 3 | Summary of the Clifford + T circuit complexities of the operations serving as subroutines in this work

Operations	Count	Depth
SP (Theorem. 3)	$O(N\log(1/\varepsilon))$	$\tilde{O}\left(N\frac{\log(n)\log(1/\varepsilon)}{n}\right)$ $\tilde{O}(n\log(1/\varepsilon))$
SOPS (Theorem. 4)	$O(ML)$	$O\left(ML\frac{\log(m+L)}{m+L}\right)$ $O(m+\log L)$
SBM (Theorem. 5)	$O(ns\tilde{n})$	$O(\log(n)s\tilde{n})$ $O(\log(ns\tilde{n}))$
SSP (Theorem. 9)	$O(s(n\log s + \log(1/\varepsilon)))$	$\tilde{O}(s\log(s)\log(n/\varepsilon))$ $\tilde{O}(\log(s)\log(1/\varepsilon)+\log n)$

Note: Suppose the subroutine has n_{dat} data qubit, in the last column, the first row corresponds to the circuit depth when there are $n_{anc} = O(n_{dat})$ ancillary qubit; the second row corresponds to the circuit depth without qubit number restriction. $\tilde{O}$ suppresses the doubly logarithmic factors with respect to n and s. SP, SOPS, SBM and SSP correspond to state preparation, select oracle for Pauli strings, sparse Boolean memory and sparse state preparation (Supplementary Discussion 2), respectively.

depth-optimal scheme in[37]. The circuit depth can then be improved to $O(N\log(1/\varepsilon)n_{anc}/\log(n_{anc}))$, at the cost of higher gate count.

We note that when the quantum state is sparse, the circuit complexity will be significantly lower. The construction of sparse state preparation is useful for sparse block-encoding. Details about sparse state preparation and sparse matrix block-encoding are provided in Supplementary Discussion 2.

Other useful subroutines
Before discussing the construction of access models in Eq. (1) and Eq. (2), we introduce some other useful subroutines, including select oracle and quantum sparse Boolean memory. These operations may have applications individually in some other scenarios. For both operations, we obtain their space-time trade-off constructions, which have improved or comparable Clifford + T complexities compared to the best-known realizations (see also Table 3).

Select oracle for Pauli strings. We consider a function of Pauli strings $H_x = \bigotimes_{l=1}^{L} H_{x,l}$, where $x \in \{0, 1, \cdots, 2^m - 1\}$ and $H_{x,l} \in \{\pm I, \pm X, \pm Y, \pm Z\}$. We introduce two registers, the *index register* contains m qubits, and the *word register* contains L qubits. Select oracle for H_x is defined as

$$\text{Select}(H_x) = \sum_{x=0}^{2^m-1} |x\rangle\langle x| \otimes H_x, \qquad (6)$$

where $|x\rangle$ represents the computational basis of index register, and the unitary H_x is applied at the word register. In other words, the state of index register controls the operations applied at the word register.

Several proposals of implementing Eq. (6) has been introduced in the literature. For example, with $n_{anc} = m$ ancillary qubits, ref. 38 (Appendix G.4) proposed a method achieving $O(ML)$ circuit depth and gate count with $M = 2^m$. With $n_{anc} = O(ML)$ ancillary qubits, Eq. (6) is a special form of the "*product unitary memory*" in[34], which can be constructed with $O(\log(ML))$ depth and $O(ML)$ count of Clifford + T gates. We provide an algorithm with tunable ancillary qubit number achieving the circuit complexity as follows.

Theorem 4. With n_{anc} ancillary qubits where $\Omega(m + L) \leqslant n_{anc} \leqslant O(ML)$, Eq. (6) can be realized with $O(ML)$ count and $O\left(ML\frac{\log n_{anc}}{n_{anc}}\right)$ depth of Clifford + T gates.

Compared to the result in ref. 38, our protocol reduces the circuit depth for a factor of $O\left(\frac{\log n_{anc}}{n_{anc}}\right)$ while maintaining the gate count scaling. The proof of Theorem 4 and details of circuit constructions are provided in Methods.

Sparse Boolean memory. We consider a sparse Boolean function $B : \{0,1\}^n \to \{0,1\}^{\tilde{n}}$, which has totally s input digits q satisfying $B(q) \neq 0 \cdots 0$. Given an n-qubit index register (denoted as idx) and a $\tilde{n}$-qubit register (denoted as wrd), we define the sparse Boolean memory Select(B) as a unitary satisfying

$$\text{Select}(B)|q\rangle_{\text{idx}}|z\rangle_{\text{wrd}} = |q\rangle_{\text{idx}}|z \oplus B(q)\rangle_{\text{wrd}}. \qquad (7)$$

We have the following result (see Methods for proof).

Theorem 5. With n_{anc} ancillary qubits where $\Omega(n) \leqslant n_{anc} \leqslant O(ns\tilde{n})$, Select($B$) can be realized with $O(ns\tilde{n})$ count and $O\left(ns\tilde{n}\frac{\log n_{anc}}{n_{anc}}\right)$ depth of Clifford + T gates.

Different from SAIM, Eq. (7) contains constant number of nonzero outputs. So its construction requires much less resource.

Construction of SAIM
With all necessary tools ready, we now discuss the construction of the SAIM in Eq. (1). We have the following result.

Theorem 6. Given n_{anc} ancillary qubits where $\Omega(n) \leqslant n_{anc} \leqslant O(Nnds)$, O_H can be constructed with $O(Nnds)$ count and $O\left(Nnds\frac{\log n_{anc}}{n_{anc}}\right)$ depth of Clifford + T gates.

Given n_{anc} ancillary qubits where $\Omega(n) \leqslant n_{anc} \leqslant O(Nns\log s)$, O_F can be constructed with $O(Nns\log s)$ count and $O\left(Nns\log s\frac{\log n_{anc}}{n_{anc}}\right)$ depth of Clifford + T gates.

Proof. O_H corresponds to a $2n$-index, d-word and Ns-sparse Boolean function. So the construction of O_H follows directly from Theorem 5.

The construction of O_F can be realized in three steps. We introduce an n-qubit ancillary register (denoted as anc). In the first step, we perform the following transformation

$$|x, k\rangle_{\text{idx}}|0\rangle_{\text{anc}} \to |x, k\rangle_{\text{idx}}|F(x, k)\rangle_{\text{anc}}. \qquad (8)$$

According to Theorem 4, this step can be constructed with $O(2^n ns)$ count and $O(2^n ns\frac{\log n_{anc}}{n_{anc}})$ depth with n_{anc} ancillary qubits. In the second step, we apply swap gates between the ancillary register and half of the index register which encodes k, i.e.

$$|x, k\rangle_{\text{idx}}|F(x, k)\rangle_{\text{anc}} \to |x, F(x, k)\rangle_{\text{idx}}|k\rangle_{\text{anc}} \qquad (9)$$

This step can be realized with $O(n)$ count and $O(1)$ depth of Clifford + T gates. In the final step, we perform the transformation

$$|x, F(x, k)\rangle_{\text{idx}}|k\rangle_{\text{anc}} \to |x, F(x, k)\rangle_{\text{idx}}|0\rangle_{\text{anc}} \qquad (10)$$

which can be realized by a $2n$-index, $\lceil \log_2 s \rceil$-word and Ns-sparse Boolean memory. According to Theorem 5, this step can be constructed with $O(Nns \log s)$ count and $O\left(Nns \log s \frac{\log n_{\mathrm{anc}}}{n_{\mathrm{anc}}}\right)$ depth of Clifford $+ T$ gates. The total gate complexity is therefore the combination of three steps above. □

Compared to the circuit complexity lower bound obtained in Theorem 1, our protocol has nearly optimal circuit complexities with respect to the matrix dimension up to a factor of n. As mentioned before, SAIM is a standard access model in many quantum algorithms, and the query complexity to SAIM has been studied extensively for various tasks. With Theorem 6, one can directly obtain the natural circuit complexity of those algorithms. Further discussions are provided in the DISCUSSION section.

Construction of LCU-based block-encoding

The construction of LCU-based block-encoding can be realized with quantum state preparation and select oracle[13]. We define $\boldsymbol{\alpha} = [\alpha_1, \cdots, \alpha_P]$ and $|\boldsymbol{\alpha}\rangle = \sum_{p=1}^{P} \sqrt{\alpha_p} |p\rangle$. Let $G_{|\boldsymbol{\alpha}\rangle}$ be the state preparation unitary for $|\boldsymbol{\alpha}\rangle$, and we define $\mathbb{G} \equiv G_{|\boldsymbol{\alpha}\rangle} \otimes \mathbb{I}_{2^n}$. We then define a Select oracle corresponding to Eq. (3) as $\mathrm{Select}(u_p) = \sum_{p=0}^{P-1} |p\rangle\langle p| \otimes u_p$. It can be verified that $\mathbb{G}^{\dagger} \mathrm{Select}(u_p) \mathbb{G}$ is a block-encoding of H with normalization factor $\alpha = 1$[14]. The constructions of LCU-based block-encoding is then reduced to the quantum state preparation and $\mathrm{Select}(u_p)$, both of which can be constructed with polynomial-size quantum circuits.

The exact circuit complexity of block-encoding depends on the specific form of u_p. We take the LCU for Pauli strings (Eq. (4)) as an example. Based on our improved quantum state preparation (Theorem 3) and Select oracle for Pauli strings (Theorem 4), we have the following result, where $(n_{\mathrm{anc}}, \varepsilon)$-block-encoding is the abbreviation of $(1, n_{\mathrm{anc}}, \varepsilon)$-block-encoding (see Methods section for proof).

Theorem 7. With n_{anc} ancillary qubits where $\Omega(\log_2 P) \leqslant n_{\mathrm{anc}} \leqslant O(NP)$, the $(n_{\mathrm{anc}}, \varepsilon)$-block-encoding of H defined in Eq. (4) can be constructed with $O\left(P(n + \log(1/\varepsilon))\right)$ count and $\tilde{O}\left(Pn \log(1/\varepsilon) \frac{\log n_{\mathrm{anc}}}{n_{\mathrm{anc}}}\right)$ depth of Clifford $+ T$ gates, where $\tilde{O}$ suppresses the doubly logarithmic factors of n_{anc}.

The block-encoding of LCU can be constructed with polylogarithmic circuit complexity with respect to the data dimension, as oppose to the SAIM requiring polynomial gate count. Therefore, for structured classical data in the form of Eq. (3) exponential quantum advantage can be expected. In below, we provide further discussions about by our results.

Discussion

As demonstrated in Theorem 1, a general SAIM can not be implemented with $O(\mathrm{Poly}(n))$ size quantum circuit. In the language of complexity class, this implies that $\mathrm{BQP}^{\mathrm{SAIM}} \neq \mathrm{BQP}$, where SAIM represent the quantum oracles in the form of Eq. (1). In other words, if problem A can be solve with polynomial number of queries to the SAIM, A is not necessarily solvable with polynomial-size quantum circuits. In fact, it is reasonable to conjecture that $\mathrm{BQP}^{\mathrm{SAIM}} \neq \mathrm{PSPACE}$ when considering the scaling with n. The reason is that for a general matrix with 2^n dimension, storing all its element requires exponentially large space, and this is true even for sparse matrix. The same argument applies to the block-encoding of sparse matrices as well.

This argument is consistent with the results about classical dequantization algorithms[39,40], which demonstrate that sub-linear classical runtime can be achieved for tasks such as recommendation systems and solving linear systems. Note that these algorithms assumes a classical oracle similar to SAIM.

On the other hand, our study on sparse matrix encoding still has its great value. First of all, it is rare to have structured classical data that can be encoded with logarithmic complexity. In many cases, sparse matrix is the most compact representation for classical data of interest. Second, with SAIM or block-encoding, polynomial quantum speedup with respect to the matrix dimension N is still possible. Our constructions are nearly optimal, and can be used to estimate the concrete Clifford $+ T$ complexities of many quantum algorithms of practical interest. Finally, techniques developed here may serve as a subroutine for encoding a larger matrix with special

structures, with which the with which exponential quantum advantage may be possible.

An open question is how to determine whether a given matrix is efficiently block-encodable. This problem can be considere as a generalization of the unitary complexity problem[41–44], which is important due to the broad applications of block-encoding[15]. According to Theorem 7, LCU for efficient unitaries [Eq. (3)] is a sufficient condition of efficient block-encoding. Due to the generality and simplicity of LCU, it is reasonable to conjecture that the decomposition of a matrix in the form of Eq. (3) has close relation to the efficiency of its block-encoding. The block encoding of H is challenging when it can not be well approximated by Eq. (3) with $P = O(\mathrm{Poly}(n))$.

In conclusion, we have studied the circuit complexities of typical quantum access models, such as SAIM and block-encoding. We show that the circuit complexity lower bound for encoding sparse matrix is polynomial with respect to the matrix dimension. We provide nearly-optimal construction protocols to achieve the lower bound. For LCU-based block-encoding, we develop a construction protocol based on the improved implementation of quantum state preparation and select oracle for Pauli strings. Our protocols are based on Clifford $+ T$ gates and allow tunable ancillary qubit number. We expect that our results are useful for processing classical data with quantum devices[45–47]. Future works may include the study of the circuit complexity lower bound for block-encoding, and how to further improve our protocols to achieve the lower bounds. Another interesting topic is about the power of quantum circuits with global quantum channels. For example, if the feedback controls are dependent on the measurement outcomes of many measurements. In this case, the elementary operations may no longer be described by local operations, and the computation power of the circuit is expected to be enhanced. In the direction of applications, it is interesting to find practical classical problems, whose data structure are able to be represented in the form LCU. In those scenarios, exponential quantum advantage can be expected.

Methods

Quantum state preparation

We first consider the preparation with n ancillary qubits. There are some state preparation protocol with optimal single- and two-qubit gate count, such as ref. [28]. However, with direct Clifford $+ T$ decomposition, the gate complexity becomes suboptimal. We achieve gate count and circuit depth linear to the state dimension with an optimized Clifford $+ T$ decomposition. The result is as follows.

Lemma 3. With n ancillary qubits, an arbitrary quantum state can be prepared to precision ε with $O(N \log(1/\varepsilon))$ depth and $O(N \log(1/\varepsilon))$ count of Clifford $+ T$ gates.

Proof. According to[28], with single- and two-qubit gates, an arbitrary quantum state $|\psi_{\mathrm{targ}}\rangle$ can be expressed as

$$|\psi_{\mathrm{targ}}\rangle = \left(\prod_{j=1}^{n} F_j^y\right)\left(\prod_{j=1}^{n} F_j^z\right)|0\cdots0\rangle, \tag{11}$$

where F_j^z and F_j^y are uniformly controlled Z- and Y-rotations

$$F_j^z = \sum_{k=0}^{2^{j-1}-1} |k\rangle\langle k| \otimes R_z(\alpha_{j,k}^z) \otimes \mathbb{I}_{2^{n-j}}, \tag{12a}$$

$$F_j^y = \sum_{k=0}^{2^{j-1}-1} |k\rangle\langle k| \otimes R_y(\alpha_{j,k}^y) \otimes \mathbb{I}_{2^{n-j}}, \tag{12b}$$

with single qubit rotation gates $R_y(\theta) = e^{-i\theta\sigma_y/2}$, $R_z(\theta) = e^{-i\theta\sigma_z/2}$. Here $\alpha_{j,k}^y \in \mathbb{R}$ and $\alpha_{j,k}^z \in \mathbb{R}$ are some rotation angles, the exact values of which are not important for our analysis.

Single-qubit rotations can be approximated with Clifford $+ T$ gates. According to ref. [48], unitary $\widetilde{u}_z$ satisfying $\|\widetilde{u}_z - R_z(\alpha^z_{j,k}/2)\| \leqslant \varepsilon_j/2$ can be constructed with $O(\log(1/\varepsilon_j))$ single-qubit Clifford $+ T$ gates without ancilla. Accordingly, we can implement single-qubit-controlled-$R_z(\alpha^z_{j,k}, \varepsilon_j)$, such that

$$\left\| R_z\left(\alpha^z_{j,k}, \varepsilon_j\right) - R_z\left(\alpha^z_{j,k}\right) \right\| \leqslant \varepsilon_j \tag{13}$$

with the following circuit.
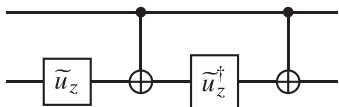
Note that $\widetilde{u}^\dagger_z$ can be realized by the inverse conjugation of the Clifford $+ T$ gate sequence of $\widetilde{u}_z$. Similar argument is also applied for $R_y(\alpha^y_{j,k})$. Then, according to Lemma 6 as will be introduced in the next section, one can construct the following unitaries

$$\widetilde{F}^j_y = \sum_{k=0}^{2^{j-1}-1} |k\rangle\langle k| \otimes \widetilde{R}_y\left(\alpha^y_{j,k}, \varepsilon_j\right) \otimes \mathbb{I}_{2^{n-j}} \tag{14}$$

$$\widetilde{F}^j_z = \sum_{k=0}^{2^{j-1}-1} |k\rangle\langle k| \otimes \widetilde{R}_z\left(\alpha^z_{j,k}, \varepsilon_j\right) \otimes \mathbb{I}_{2^{n-j}} \tag{15}$$

with j ancillary qubits, $O(2^j \log(1/\varepsilon_j))$ depth and $O(2^j \log(1/\varepsilon_j))$ count of Clifford $+ T$ gates. We therefore approximate the target state with the following

$$|\widetilde{\psi}_{\text{targ}}\rangle = \left(\prod_{j=1}^n \widetilde{F}^j_z\right)\left(\prod_{j=1}^n \widetilde{F}^j_y\right)|0\cdots 0\rangle. \tag{16}$$

In below, we first bound the distance between $|\psi_{\text{targ}}\rangle$ and $|\widetilde{\psi}_{\text{targ}}\rangle$. It can be verified that $\|\widetilde{F}^y_j|\psi\rangle - F^y_j|\psi\rangle\| \leqslant \varepsilon_j$ and $\|\widetilde{F}^z_j|\psi\rangle - F^z_j|\psi\rangle\| \leqslant \varepsilon_j$ for any quantum state $|\psi\rangle$. In other words, we have $\|\widetilde{F}^y_j - F^y_j\| \leqslant \varepsilon_j$ and $\|\widetilde{F}^z_j - F^z_j\| \leqslant \varepsilon_j$. Therefore,

$$
\begin{aligned}
&\left\|\left(\prod_{j=1}^n \widetilde{F}^y_j - \prod_{j=1}^n F^y_j\right)\right\| \\
\leqslant\ & \left\|\widetilde{F}^y_n\left(\prod_{j=1}^{n-1} \widetilde{F}^y_j - \prod_{j=1}^{n-1} F^y_j\right)\right\| + \left\|\left(\widetilde{F}^y_n - F^y_n\right)\prod_{j=1}^{n-1} F^y_j\right\| \\
\leqslant\ & \left\|\left(\prod_{j=1}^{n-1} \widetilde{F}^y_j - \prod_{j=1}^{n-1} F^y_j\right)\right\| + \varepsilon_n \\
& \cdots \\
\leqslant\ & \sum_{j=1}^n \varepsilon_j.
\end{aligned}
\tag{17}
$$

In a similar way, we can obtain $\left\|\left(\prod_{j=1}^n \widetilde{F}^z_j - \prod_{j=1}^n F^z_j\right)\right\| \leqslant \sum_{j=1}^n \varepsilon_j$. So we have

$$
\begin{aligned}
&\||\psi_{\text{targ}}\rangle - |\widetilde{\psi}_{\text{targ}}\rangle\| \\
\leqslant\ & \left\|\left(\prod_{j=1}^n \widetilde{F}^y_j \prod_{j=1}^n \widetilde{F}^z_j - \prod_{j=1}^n F^y_j \prod_{j=1}^n F^z_j\right)\right\| \\
\leqslant\ & \left\|\left(\prod_{j=1}^n \widetilde{F}^z_j - \prod_{j=1}^n F^z_j\right)\right\| + \left\|\left(\prod_{j=1}^n \widetilde{F}^y_j - \prod_{j=1}^n F^y_j\right)\right\| \\
\leqslant\ & 2\sum_{j=1}^n \varepsilon_j.
\end{aligned}
\tag{18}
$$

According to Eq. (18), to control the total error rate to a constant value i.e. $\||\psi_{\text{targ}}\rangle - |\widetilde{\psi}_{\text{targ}}\rangle\| \leqslant \varepsilon$, it suffice to set $\varepsilon_j = \varepsilon/2^{n-j+1}$. Because each $\widetilde{F}^y_j$ or $\widetilde{F}^z_j$ require $O(2^j \log(1/\varepsilon_j))$ gate count and circuit depth, the total gate count is

$$
\begin{aligned}
C &= \sum_{j=0}^{n-1} O(2^j \log(1/\varepsilon_j)) \\
&= \sum_{j=0}^{n-1} O(2^j \log(2^{n-j}/\varepsilon)) \\
&= O(N \log(1/\varepsilon)).
\end{aligned}
\tag{19}
$$

Similarly, the total circuit depth is

$$D = \sum_{j=0}^{n-1} O(2^j \log(1/\varepsilon_j)) = O(N \log(1/\varepsilon)). \tag{20}$$

□

We then consider the quantum state preparation with exponential ancillary qubits. Our protocol follows the same idea in[34] with improvement.

Lemma 4. Arbitrary n-qubit quantum state can be prepared with $O(N)$ ancillary qubits, $O(n\log(n/\varepsilon))$ depth and $O(N\log(1/\varepsilon))$ count of Clifford $+ T$ gates.

Proof. Our construction is based on the protocol in[34] with revision and improved Clifford$+T$ decomposition.

General procedure. The hardware layout of our method contains a binary tree of qubits with $n + 1$ layers, which is denoted as H. The lth (with $0 \leqslant l \leqslant n$) layer of H is denoted as H_l. For $1 \leqslant l \leqslant n$, H_l connects to another binary tree of qubits, denoted as V_l. The root of the tree V_l serves as the lth data qubit, and we denote it as d_l here.

Our protocol for preparing target state $|\psi_{\text{targ}}\rangle = \sum_{k=0}^{2^n-1} \alpha_k |k\rangle_d$ works as follows. We initialize the root of H as $|1\rangle_{H_1}$ while all other qubits are at state $|0\rangle$. In the first stage, H is prepared at the quantum state (qubits at state $|0\rangle$ are not shown)

$$|1\rangle_{H_1} \to \sum_{k=0}^{2^n-1} \alpha_k |\varphi_k\rangle_H. \tag{21}$$

Here, $|\varphi_k\rangle$ is one of the computational basis of H to be defined later. In the second stage, the data qubits are transferred to the n-qubit computational basis $|k\rangle_d$ conditioned on $|\varphi_k\rangle$, i.e.

$$\sum_{k=0}^{2^n-1} \alpha_k |\varphi_k\rangle_H \to \sum_{k=0}^{2^n-1} \alpha_k |\varphi_k\rangle_H |k\rangle_d. \tag{22}$$

Finally, the binary tree H is uncomputed

$$\sum_{k=0}^{2^n-1} \alpha_k |\varphi_k\rangle_H |k\rangle_d \to \sum_{k=0}^{2^n-1} \alpha_k |0\rangle_H |k\rangle_d. \tag{23}$$

The target state is then obtained after tracing out H. The readers are refereed to[34] for more details. Transformations in Eq. (22) and Eq. (23) can be ideally realized using Clifford circuit with $O(n)$ depth and $O(2^n)$ gate count. On the other hand, the first stage for obtaining Eq. (21) contains rotation that has to be approximated with T gates and hence more complicated. So we focus on Eq. (21) in below.

Realization of Eq. (21). We will first show how Eq. (21) can be realized with single-qubit and CNOT gates with a method slightly different from[34], and then introduce its Clifford $+ T$ decomposition.

We define $\alpha_{n,k} \equiv a_k$ and $\alpha_{L,k} = \arg(\alpha_{L+1,2k})\sqrt{|\alpha_{L+1,2k}|^2 + |\alpha_{L+1,2k+1}|^2}$ for all $0 \leqslant l \leqslant n-1$. Note that we can assume $\arg(\alpha_0) = 0$ without loss of generality. For $0 \leqslant L \leqslant n$, we define

$$|\Psi_L\rangle = \sum_{k=0}^{2^L-1} \alpha_{L,k} \bigotimes_{l=0}^{L} |(k,l)\rangle'_{H_l}. \tag{24}$$

The realization of Eq. (21) contains n steps, with the Lth step corresponds to $|\Psi_{L-1}\rangle \to |\Psi_L\rangle$.

In Eq. (24), we have defined $(0,0) \equiv 0$, and $(k,l) \equiv k_n k_{n-1} \cdots k_{n-l+1}$ for $l \geqslant 1$; $|(k,l)\rangle' \equiv |0\rangle^{\otimes(k,l)}|1\rangle|0\rangle^{\otimes 2^l-(k,l)-1}$; H_l represents the lth layer of H. Eq. (21) and Eq. (24) have the correspondence $|\varphi_k\rangle = \bigotimes_{l=0}^{L}|(k,l)\rangle'_{H_l}$ and $\sum_{k=0}^{2^n-1} \alpha_k|\varphi_k\rangle_H = |\psi_n\rangle$. So $|\psi_n\rangle$ is the target state of the stage 1 introduced in Eq. (21).

We then introduce the realization of $|\Psi_{L-1}\rangle \to |\Psi_L\rangle$. We define single qubit rotation $r_y(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$ and $r_z(\phi) = \begin{pmatrix} e^{-i\phi} & 0 \\ 0 & e^{i\phi} \end{pmatrix}$, and a three-qubit controlled operation as follows.

$$w(\theta;\phi;a;b;c) \quad =$$
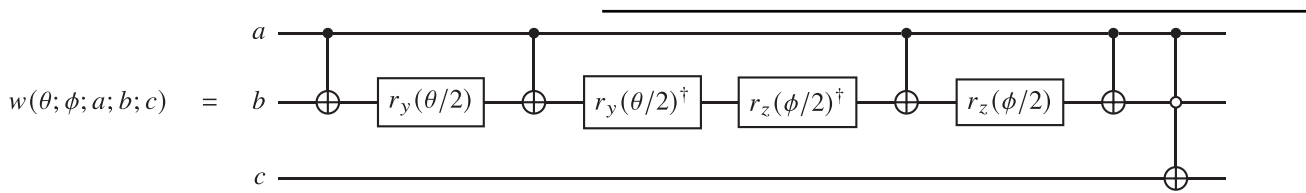
a, b, c are labels of the corresponding qubits. Let $\theta_{l,j} \equiv \arccos(b_{l,2j}/b_{l-1,j})$ and $\phi_{l,j} = \phi_{l,2j+1} - \phi_{l,2j}$, at the Lth step ($1 \leqslant L \leqslant n$), we implement the parallel rotation

$$W_L = \prod_{j=0}^{2^{L-1}-1} w(\theta_{L,j};\phi_{L,j};H_{L-1,j};H_{L,2j};H_{L,2j+1}) \tag{25}$$

which costs $O(1)$ depth and $O(2^L)$ count of single-qubit and CNOT gates. It can be verified that

$$W_L|\Psi_{L-1}\rangle = |\Psi_L\rangle. \tag{26}$$

The total single-qubit $+$ CNOT depth and gate count are $O(n)$ and $O(2^n)$ respectively.

Clifford $+ T$ decomposition. W_L are assumed to be constructed with single- and two-qubit gates. In below, we discuss how to decompose it with Clifford $+T$ gates with high accuracy. According to ref. 48, one can always construct a unitaries $\tilde{r}_y(\theta;\varepsilon), \tilde{r}_z(\phi;\varepsilon)$, with $O(\log(1/\varepsilon))$ depth of gates in $\{H, S, T\}$, which satisfies

$$\| \tilde{r}_y(\theta;\varepsilon) - r_y(\theta) \| \leqslant \varepsilon, \quad \| \tilde{r}_z(\phi;\varepsilon) - r_z(\phi) \| \leqslant \varepsilon. \tag{27}$$

Accordingly, we define $\tilde{w}(\theta;\phi;\varepsilon;a;b;c)$ as the following transformation
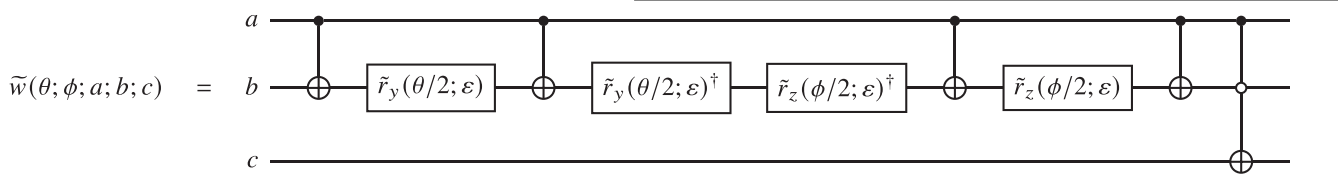
$$\tilde{w}(\theta;\phi;a;b;c) \quad =$$

We have

$$\tilde{w}(\theta;\phi;\varepsilon;a;b;c)(a|0\rangle_a|0\rangle_b|0\rangle_c + b|1\rangle_a|0\rangle_b|0\rangle_c)$$
$$= a|0\rangle_a|0\rangle_b|0\rangle_c + b_1(\varepsilon)|1\rangle|10\rangle + b_2(\varepsilon)|01\rangle, \tag{28}$$

for some $\sqrt{|b_1(\varepsilon) - b_1(0)|^2 + |b_2(\varepsilon) - b_2(0)|^2} \leqslant |b|\varepsilon$. We then define

$$\widetilde{W}_L(\varepsilon) = \prod_{j=0}^{2^{L-1}-1} \tilde{w}(\theta_{L,j};\phi_{L,j};\varepsilon;H_{L-1,j};H_{L,2j};H_{L,2j+1}), \tag{29}$$

which is used to approximate W_L. From Eq. (28), it can be verified that $\|\widetilde{W}_L(\varepsilon)|\Psi_{L-1}\rangle - W_L|\Psi_{L-1}\rangle\| \leqslant \varepsilon$. We set the accuracy at the Lth layer as ε_L, and define

$$|\widetilde{\Psi}_0\rangle = |\Psi_0\rangle, \quad |\widetilde{\Psi}_L\rangle = \widetilde{W}_L(\varepsilon_L)|\widetilde{\Psi}_{L-1}\rangle. \tag{30}$$

We have

$$\begin{aligned}
&\| |\widetilde{\Psi}_L\rangle - |\Psi_L\rangle \| \\
&= \|\widetilde{W}_L(\varepsilon_L)|\widetilde{\Psi}_{L-1}\rangle - W_L|\Psi_{L-1}\rangle\| \\
&\leqslant \|\widetilde{W}_L(\varepsilon_L)|\widetilde{\Psi}_{L-1}\rangle - \widetilde{W}_L(\varepsilon_L)|\Psi_{L-1}\rangle\| \\
&\quad + \|\widetilde{W}_L(\varepsilon_L)|\Psi_{L-1}\rangle - W_L|\Psi_{L-1}\rangle\| \\
&\leqslant \|\widetilde{W}_L(\varepsilon_L)|\widetilde{\Psi}_{L-1}\rangle - \widetilde{W}_L(\varepsilon_L)|\Psi_{L-1}\rangle\| + \varepsilon_L \\
&= \| |\widetilde{\Psi}_{L-1}\rangle - |\Psi_{L-1}\rangle \| + \varepsilon_L.
\end{aligned} \tag{31}$$

By applying the inequality above iteratively from $L = 1$ to $L = n$, we have

$$\| |\widetilde{\Psi}_n\rangle - |\Psi_n\rangle \| \leqslant \sum_{L=1}^{n} \varepsilon_L. \tag{32}$$

According to Eq. (32), to control the total error rate to a constant value, it suffices to set $\varepsilon_L = K\varepsilon/(n-L+1)^2$ for some constant K. This is the key step of our improved construction.

Circuit complexity. Each $\widetilde{W}_L$ can be realized with $O(2^L \log(1/\varepsilon_L))$ count and $O(\log(1/\varepsilon_L))$ depth of Clifford $+ T$ gates. Therefore, the total gate count at stage 1 (Eq. (21)) is

$$\begin{aligned}
C &= O\left(\sum_{L=1}^{n} 2^L \log(1/\varepsilon_L) \right) \\
&= O\left(\sum_{L=1}^{n} 2^L \log((n-L+1)^2/\varepsilon) \right) \\
&= O\left(2^{n+1} \sum_{m=1}^{n} \frac{\log(m)}{2^m} \right) + O(2^n \log(1/\varepsilon)) \\
&= O(2^n) + O(2^n \log(1/\varepsilon)) \\
&= O(N \log(1/\varepsilon)).
\end{aligned} \tag{33}$$

The total circuit depth at stage 1 is

$$
\begin{aligned}
D &= O\left(\sum_{L=1}^{n} \log(1/\varepsilon_L)\right) \\
&= O\left(\sum_{L=1}^{n} \log((n-L+1)^2/\varepsilon)\right) \\
&= O\left(\sum_{m=1}^{n} \log(m^2)\right) + O(n\log(1/\varepsilon)) \\
&= O(\log(n!)) + O(n\log(1/\varepsilon)) \\
&= O(n\log(n/\varepsilon)).
\end{aligned}
\tag{34}
$$

Recall that Eqs. (22), (23) has $O(N)$ count and $O(n)$ depth of Clifford $+ T$ gates. So the total gate count and circuit depth are $O(N\log(1/\varepsilon))$ and $O(n\log(n/\varepsilon))$ respectively. $\square$

We also cares about the controlled quantum state preparation. In our preparation scheme, the initial state is $|1\rangle_{H_1}$, i.e. the root of H is set as $|1\rangle$. If we set H_1 as $|0\rangle_{H_1}$ instead, it can be verified that the output state is $|0\cdots0\rangle_d$. Therefore, to implement controlled state preparation, one can simply replace the root qubit H_1 by the controlled qubit, and the circuit complexity remains unchanged. In other words, we have the following result.

Lemma 5. Arbitrary single-qubit-controlled n-qubit state preparation unitary can be constructed with $O(N)$ ancillary qubits, $O(n\log(n/\varepsilon))$ depth and $O(N\log(1/\varepsilon))$ count of Clifford $+ T$ gates.

Based on Lemma 3, Lemma 4 and Lemma 5, We have the following result for intermediate number of ancillary qubits. Note that Theorem 3 in the main text follows directly from Theorem 8.

Theorem 8. (space-time tradeoff QSP). With n_{anc} ancillary qubits where $\Omega(n) \leqslant n_{\mathrm{anc}} \leqslant O(2^n)$, state preparation and controlled state preparation of an arbitrary n-qubit quantum state can be realized with precision ε with $O(N\log(1/\varepsilon))$ count and $O\left(N\frac{\log(n_{\mathrm{anc}})\log(\log(n_{\mathrm{anc}})/\varepsilon)}{n_{\mathrm{anc}}}\right)$ depth of Clifford $+ T$ gates.

Proof. We separate all data qubits into two registers. Register A contains the last $n_a = n - \lfloor\log_2 m\rfloor$ data qubits, and register B contains the first $n_b = \lfloor\log_2 m\rfloor$ qubits for some $n \leqslant m \leqslant 2^n$. We define $N_a = 2^{n_a}$ and $N_b = 2^{n_b}$. The target state can be rewritten as

$$
|\psi_{\mathrm{targ}}\rangle = \sum_{k=0}^{N_a-1} \beta_k |k\rangle_A |\phi_k\rangle_B
\tag{35}
$$

for some normalized β_k, and normalized quantum states $|\phi_k\rangle$. We define $|\psi_a\rangle_A = \sum_{k=0}^{N_a-1} \beta_k |k\rangle_A$.

In the first step, we prepare register A to a quantum state

$$
|\widetilde{\psi}_a\rangle_A = \sum_{k=0}^{N_a-1} \widetilde{\beta}_k |k\rangle_A
\tag{36}
$$

which satisfies $\||\psi_a\rangle - |\widetilde{\psi}_a\rangle\| \leqslant \varepsilon/2$. According to Lemma 3, this step can be realized with $O(N_a\log(1/\varepsilon)) = O\left(\frac{N}{m}\log(1/\varepsilon)\right)$ count and depth of Clifford $+ T$ circuit.

In the second step, we implement

$$
\mathrm{Select}(\widetilde{G}_k) \sum_{k=0}^{N_a-1} \widetilde{\beta}_k |k\rangle_A |0^{n_b}\rangle_B = \sum_{k=0}^{N_a-1} \widetilde{\beta}_k |k\rangle_A |\widetilde{\phi}_k\rangle_B
\tag{37}
$$
$$
\equiv |\widetilde{\psi}_{\mathrm{targ}}\rangle
$$

where $\widetilde{G}_k$ is a state preparation unitary satisfying $\widetilde{G}_k|0\rangle = |\widetilde{\phi}_k\rangle$ for some $\||\phi_k\rangle - |\widetilde{\phi}_k\rangle\| \leqslant \varepsilon/2$. It can be then verified that $\||\psi_{\mathrm{targ}}\rangle - |\widetilde{\psi}_{\mathrm{targ}}\rangle\| \leqslant \varepsilon$. According to Lemma 4, controlled-$\widetilde{G}_k$ such that $\widetilde{G}_k|0^{n_b}\rangle = |\widetilde{\phi}_k\rangle$ can be constructed with $O(m)$ ancillary qubits, $O(N_b\log(1/\varepsilon))$ count and

$O(n_b\log(n_b/\varepsilon)) = O(\log(m)\log(\log(m)/\varepsilon))$ depth of Clifford $+ T$ gates. Then, according to Lemma 6, with $O(m)$ ancillary qubits, $\mathrm{Select}(\widetilde{G}_k)$ can be constructed with

$$
C = O(N_a \times N_b \log(1/\varepsilon)) = O(N\log(1/\varepsilon))
\tag{38}
$$

gate count, and

$$
\begin{aligned}
D &= O(N_a \times \log(m)\log(\log(m)/\varepsilon)) \\
&= O\left(N\frac{\log(m)\log(\log(m)/\varepsilon)}{m}\right)
\end{aligned}
\tag{39}
$$

depth of Clifford $+ T$ gates. By setting $n_{\mathrm{anc}} = O(m)$ for some $n_{\mathrm{anc}} \geqslant n$, we complete the proof. $\square$

Select oracle for general unitary functions. Suppose x is an m-bit bitstring, and U_x are general unitaries. We consider the unitary

$$
\mathrm{Select}(U_x) = \sum_{x=0}^{M-1} |x\rangle\langle x| \otimes U_x,
\tag{40}
$$

where $M = 2^m$. In below, we discuss how to construct $\mathrm{Select}(U_x)$ based on the implementation of single-qubit-controlled-U_x, and the corresponding circuit complexity upper bound. We define $C_{\mathrm{ctrl}}(U_x, r)$ and $D_{\mathrm{ctrl}}(U_x, r)$ as the count and depth of Clifford $+ T$ gates required to construct the controlled-U_x, given r ancillary qubits. The following result corresponds to the case with $m + r$ ancillary qubits.

Lemma 6. (Appendix G.4 of[58]). With $m + r$ ancillary qubits, $\mathrm{Select}(U_x)$ can be constructed with $O(MC_{\mathrm{ctrl}}(U_x, r))$ count and $O(MD_{\mathrm{ctrl}}(U_x, r))$ depth of Clifford $+ T$ gates.

Proof. We introduce an ancillary register with m qubits. We denote the jth qubit at the index register (encoding $|x\rangle$) and ancillary registers as C_j, A_j respectively. We also denote $C = [C_1, C_2, \cdots, C_m]$ and $A = [A_0, A_1, A_2, \cdots, A_m]$. A_0 is initialized as $|1\rangle$ while all other ancillary qubits are initialized as $|0\rangle$. $\square$

Eq. (40) can be realized by querying $\mathrm{Select}(C, A, m, 0)$, which is defined recursively by Algorithm 1. In Algorithm 1, $\mathrm{Toffoli}(a, b; c)$ is the Toffoli gate with qubit a and b as the controlled qubits and c as the target qubit; $C\text{-}U_x(a)$ is the controlled-U_x with qubit a as controlled qubit and the corresponding word register as target qubits; $\dim(v)$ represent the dimension of the vector (for example, $\dim(C) = n$); v_j represents the jth element of v and $v_{j:} = [v_j, v_{j+1}, \cdots, v_{\dim(v)}]$.

Algorithm 1. Select(y, q, l, x)

1: **if** $l \neq 0$:
2:   $\mathrm{Toffoli}(\overline{y_1}, q_1; q_2)$
3:   Select($y_2, q_2, l-1, x$)
4:   $\mathrm{Toffoli}(\overline{y_1}, q_1; q_2)$
5:   $\mathrm{Toffoli}(y_1, q_1; q_2)$
6:   Select($y_2, q_2, l-1, x+2^{l-1}$)
7:   $\mathrm{Toffoli}(y_1, q_1; q_2)$
8: **elseif** $l = 0$:
9:   $C\text{-}U_x(q_1)$
10: **end if**

In our implementation, the controlled-U_x are queried for totally M times with $x \in \{0, \cdots, m-1\}$ sequentially. Moreover, there are totally $O(M)$ Toffoli gates acting sequentially. Therefore, the total gate count and circuit depth are $O(MC_{\mathrm{ctrl}}(U_x, r))$ and $O(MD_{\mathrm{ctrl}}(U_x, r))$ respectively.

We note that Algorithm 1 can be further simplified by combining some concatenated gates[58]. But the asymptotic scaling here is optimal.

We then consider the construction of expoential ancillary qubits. In Algorithm 4,5 of[54], based on the bucket-brigade architecture for quantum random access memory[49–51], it has been shown that any $\mathrm{Select}(U_x)$ can be

constructed by $4M - 1$ ancillary qubits, $O(M)$ Clifford $+ T$ gates arranged in $O(m)$ circuit depth, and queries to all single-qubit-controlled-U_x for $x \in \{0, \cdots, M-1\}$ in parallel. If each controlled-U_x uses r ancillary qubits, we require totally $M(4+r) - 1$ ancillary qubits, because they are implemented in parallel. To sum up, we have the following result.

Lemma 7. (many qubit Select oracle). With $M(4+r) - 1$ ancillary qubits, $\text{Select}(U_x)$ can be constructed with $O(MC_{\text{ctrl}}(U_x, r))$ count and $O(m + D_{\text{ctrl}}(U_x, r))$ depth of Clifford $+ T$ gates.

Select oracle for general unitary functions. In below, we give the proof of Theorem 4 about the construction of select oracles for Pauli strings defined in Eq. (6). Note that Eq. (6) is a special case of Eq. (40) with $U_x \in \{\pm I, \pm X, \pm Y, \pm Z\}^{\otimes L}$.

proof of Theorem 4. Recall that Select oracle for Pauli strings corresponds to Eq. (40) with $U_x = H_x$, where $H_x = \bigotimes_{l=1}^{L} H_{x,l}$ and $H_{x,l} \in \{\pm I, \pm X, \pm Y, \pm Z\}$.

Given L ancillary qubits, controlled-H_x can be constructed with the following circuit.
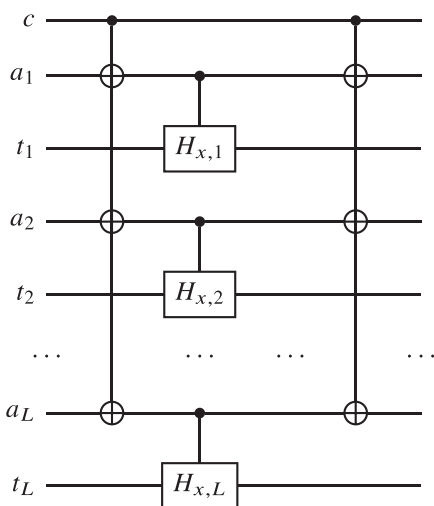
where control qubit is denoted as c, ancillary qubits, all initialized as $|0\rangle$, are denoted as $a_1, a_2, \cdots, a_L$ and target qubits are denoted as $t_1, t_2, \cdots, t_L$ respectively. Two of the L-Toffoli gates can be effectively constructed with $O(L)$ count and $O(\log L)$ depth of Clifford $+ T$ gates. All controlled Pauli gates can be constructed with totally $O(L)$ count and $O(1)$ depth of Clifford $+ T$ gates. In other words, we have $C_{\text{ctrl}}(H_x, L) = O(L)$ and $D_{\text{ctrl}}(H_x, L) = O(\log L)$.

Our protocol of constructing $\text{Select}(H_x)$ uses at least $\Omega(m + L)$ ancillary qubits. We divide the m-qubit index registers into two subregisters A and B with $m_a \geqslant \log_2(m + L)$ and $m_b = m - m_a$ qubits respectively. Let $M_a = 2^{m_a}$, $M_b = 2^{m_b}$, $\text{Select}(H_x)$ can be rewritten as

$$\text{Select}(H_x) = \sum_{x_a=0}^{M_a-1} |x_a\rangle\langle x_a| \otimes V_{x_a} \tag{41}$$

$$V_{x_a} = \sum_{x_b=0}^{M_b-1} |x_b\rangle\langle x_b| \otimes H_{x_a \oplus x_b}. \tag{42}$$

x_a and x_b are bit strings with m_a and m_b bits respectively, and $x \equiv x_a \oplus x_b$. According to Lemma 7, V_{x_a} can be constructed with $M_a(4 + L) - 1$ ancillary qubits, $O(M_a L)$ count and $O(m_a + \log L)$ depth of Clifford $+ T$ gates. According to Lemma 6, with totally $n_{\text{anc}} = M_a(4 + L) - 1 + m_b$ ancillary qubits, the Clifford $+ T$ gate count of $\text{Select}(H_x)$ is

$$C = O(M_b M_a L) = O(ML). \tag{43}$$

The Coifford $+ T$ depth is

$$\begin{aligned} D &= O(M_b(m_a + \log L)) \\ &= O\left(M \frac{\log(M_a L)}{M_a}\right) \\ &= O\left(M \frac{\log((n_{\text{anc}}+1)/4)}{(n_{\text{anc}}+1)/4L}\right) \\ &= O\left(ML \frac{\log n_{\text{anc}}}{n_{\text{anc}}}\right), \end{aligned} \tag{44}$$

which completes the proof. $\square$

Details about LCU-based Block-encoding

Without loss of generality, we assume that $m = \log_2 P$ is an integer. We let $\tilde{G}_{|\alpha\rangle}$ be a state preparation unitary satisfying $\|\tilde{G}_{|\alpha\rangle}|0^m\rangle_{\text{anc}} - G_{|\alpha\rangle}|0^m\rangle_{\text{anc}}\| \leqslant \varepsilon/3$. Let $\tilde{u}_p$ be unitaries satisfying $\|\tilde{u}_p - u_p\| \leqslant \varepsilon/3$. We then define

$$\tilde{\mathbb{G}} \equiv \tilde{G}_{|\alpha\rangle} \otimes \mathbb{I}_N, \tag{45}$$

$$U \equiv \mathbb{G}^\dagger \text{Select}(u_p)\mathbb{G}, \tag{46}$$

$$\tilde{U} \equiv \tilde{\mathbb{G}}^\dagger \text{Select}(u_p)\tilde{\mathbb{G}}, \tag{47}$$

and $W \equiv \tilde{U} - U$. With a similar argument to Eq. (31), we have

$$\|W|\Psi\rangle\| \leqslant \varepsilon, \tag{48}$$

where $|\Psi\rangle = |0^m\rangle \otimes |\psi\rangle$ and $|\psi\rangle$ is an arbitrary N-dimensional quantum state. We may rewrite W as

$$W = \begin{pmatrix} \delta H & W_{1,2} \\ W_{2,1} & W_{2,2} \end{pmatrix} \tag{49}$$

where $\delta H \in \mathbb{C}^{P \times P}$, $W_{1,2} \in \mathbb{C}^{N \times P}$, $W_{2,1} \in \mathbb{C}^{P \times N}$ and $W_{2,2} \in \mathbb{C}^{N \times N}$. Note that if $\|\delta H\| \leqslant \varepsilon$, $\tilde{U}$ is a (m, ε)-block-encoding of H. We have

$$W|\Psi\rangle = \begin{pmatrix} \delta H & W_{1,2} \\ W_{2,1} & W_{2,2} \end{pmatrix}\begin{pmatrix} |\psi\rangle \\ 0 \end{pmatrix} = \begin{pmatrix} \delta H|\psi\rangle \\ W_{2,1}|\psi\rangle \end{pmatrix} \tag{50}$$

Combining Eq. (48) with Eq. (50), we have

$$\|\delta H|\psi\rangle\| \leqslant \|W|\Psi\rangle\| \leqslant \varepsilon. \tag{51}$$

Because Eq. (51) is applied for arbitrary $|\psi\rangle$, we have $\|\delta H\| \leqslant \varepsilon$. Therefore, $\tilde{U}$ is a (m, ε)-block-encoding to H. We can now study the efficiency of block-encoding.

The actual circuit complexity depends on the form of u_p. We now proof Theorem 7 which corresponds to $u_p \in \{\pm I, \pm X, \pm Y, \pm Z\}^{\otimes n}$.

Proof of Theorem 7. With n_{anc} ancillary qubits where $\log_2 P \leqslant n_{\text{anc}} \leqslant O(P)$, $\tilde{\mathbb{G}}$ can be constructed with $O(P \log(1/\varepsilon))$ count and $O\left(P \frac{\log(n_{\text{anc}}) \log(\log(n_{\text{anc}})/\varepsilon)}{n_{\text{anc}}}\right)$ depth of Clifford $+ T$ gates. With $\Omega(\log_2 P) \leqslant n_{\text{anc}} \leqslant O(Pn)$, $\text{Select}(H_x)$ can be constructed with $O(nP)$ count and $O\left(nP \frac{\log n_{\text{anc}}}{n_{\text{anc}}}\right)$ depth of Clifford $+ T$ gates. Therefore, the total gate count of $\text{Select}(H_x)$ is $O(P(n + \log(1/\varepsilon)))$. For $\Omega(\log_2 P) \leqslant n_{\text{anc}} \leqslant O(P)$, the circuit depth is

$$O\left(P \frac{\log n_{\text{anc}}}{n_{\text{anc}}}\left(n + \log(\log(n_{\text{anc}})/\varepsilon)\right)\right) \tag{52}$$

$$= O\left(P\left(n + \log(1/\varepsilon)\right) \frac{\log n_{\mathrm{anc}}}{n_{\mathrm{anc}}} \right). \tag{53}$$

For $\Omega(P) \leqslant n_{\mathrm{anc}} \leqslant O(Pn)$, the circuit depth for $\tilde{\mathbb{G}}$ is $O(\log P \log(\log(P)/\varepsilon)) = O(\log n \log(\log n/\varepsilon))$, where we have used the assumption $P = O(\mathrm{Poly}(n))$. Combining with circuit depth of Select(H_x), the total circuit depth for block-encoding is

$$
\begin{aligned}
&O\left(\left(\frac{n_{\mathrm{anc}} \log(n) \log(\log(n)/\varepsilon)}{\log n_{\mathrm{anc}}} + nP \right) \frac{\log n_{\mathrm{anc}}}{n_{\mathrm{anc}}} \right) \\
&= O\left(\left(\frac{nP \log(n) \log(\log(n)/\varepsilon)}{\log(nP)} + nP \right) \frac{\log n_{\mathrm{anc}}}{n_{\mathrm{anc}}} \right) \\
&= O\left(\left(nP \log(\log(n)) + nP \log(1/\varepsilon) \right) \frac{\log n_{\mathrm{anc}}}{n_{\mathrm{anc}}} \right) \\
&= \tilde{O}\left(nP \log(1/\varepsilon) \frac{\log n_{\mathrm{anc}}}{n_{\mathrm{anc}}} \right),
\end{aligned}
\tag{54}
$$

which completes the proof. □

Sparse Boolean memory

Recall that sparse Boolean memory performs the transformation $\mathrm{Select}(B)|q\rangle_{\mathrm{idx}}|z\rangle_{\mathrm{wrd}} = |q\rangle_{\mathrm{idx}}|z \oplus B(q)\rangle_{\mathrm{wrd}}$, idx represents an n-qubit index register, wrd represents a $\tilde{n}$-qubit register, and there are most s input digits q satisfying $B(q) \neq 0 \cdots 0$. We define q_k as the kth input digit with nonzero output, and $Q_B \equiv \{q_1, q_2, \cdots, q_s\}$. In[34], we have developed a construction of SBM with $O(ns\tilde{n})$ ancillary qubits. The result is as follows.

Lemma 8. (Sec. III B in Supplemental Material of[34]). With $O(ns\tilde{n})$ ancillary qubits, Select(B) can be realized with $O(ns\tilde{n})$ count and $O(\log(ns\tilde{n}))$ depth of Clifford + T gates.

Based on Lemma 8, we can obtain the gate complexity with intermediate number of ancillary qubits. The proof of Lemma 5 is given as follows.

Proof of Lemma 5. Let wrd_l be the lth qubit of the word register, and z_l be the lth digit of z. So $|z\rangle_{\mathrm{wrd}} = \prod_{l=1}^{\tilde{n}} |z_l\rangle_{\mathrm{wrd}_l}$. Select($B$) can be separated into multiple Boolean functions applied at different words. Let $B_l(q)$ be the lth digit of $B(q)$, and $B_{l_{\min}:l_{\max}}(q) \equiv B_{l_{\max}}(q) \cdots B_{l_{\min}+1}(q) B_{l_{\min}}(q)$. We define $\mathrm{Select}(B_{l_{\min}:l_{\max}})$ as a unitary satisfying

$$\mathrm{Select}(B_{l_{\min}:l_{\max}})|q\rangle_{\mathrm{idx}} \prod_{l=l_{\min}}^{l_{\max}} |z_l\rangle_{\mathrm{wrd}_l} \tag{55}$$

$$= |q\rangle_{\mathrm{idx}} \prod_{l=l_{\min}}^{l_{\max}} |z_l \oplus B_l(q)\rangle_{\mathrm{wrd}_l}. \tag{56}$$

For any $1 = l_0 < l_1 < \cdots < l_{n'} = \tilde{n} + 1$, it can be verified that

$$\mathrm{Select}(B) = \prod_{r=1}^{n'} \mathrm{Select}(B_{l_{r-1}:l_r - 1}). \tag{57}$$

We also define $\mathrm{Select}(B_l) = \mathrm{Select}(B_{l:l})$. For each B_l, we further define Boolean functions $B_{l,k_{\min}:k_{\max}}(q) = B_l(q) \wedge (k_{\min} \leqslant k \leqslant k_{\max})$ for $k_{\min} \leqslant k_{\max}$. For any

$0 = k_0 < k_1 < \cdots < k_{s'} = s$, it can be verified that

$$\mathrm{Select}(B_l) = \prod_{j=1}^{s'} \mathrm{Select}(B_{l,k_{j-1}:k_j - 1}). \tag{58}$$

We first consider the construction with ancillary qubit number $O(ns) \leqslant n_{\mathrm{anc}} \leqslant O(ns\tilde{n})$. In this case, we decompose Select($B(q)$) with Eq. (57). We let $d = \lfloor n_{\mathrm{anc}}/(ns) \rfloor$ and $n' = \lceil \tilde{n}/d \rceil$, and

$$
l_r = \begin{cases} rd + 1 & r < n' \\ \tilde{n} + 1 & r = n' \end{cases}. \tag{59}
$$

According to Lemma 8, with n_{anc} ancillary qubits, each $\mathrm{Select}(B_{l_{r-1}:l_r - 1})$ can be constructed with $O(nsd)$ count and $O(\log(nsd)) = O(\log n_{\mathrm{anc}})$ depth of Clifford + T circuit. So the total gate count is $O(nsd) \times n' = O(ns\tilde{n})$, and the total circuit depth is $O(\log(nsn_{\mathrm{anc}})) \times n' = O\left(ns\tilde{n} \frac{\log n_{\mathrm{anc}}}{n_{\mathrm{anc}}} \right)$.

We then consider the construction with ancillary qubit number $O(n) \leqslant n_{\mathrm{anc}} \leqslant O(ns)$. In this case, we first perform the decomposition $\mathrm{Select}(B) = \prod_{r=1}^{\tilde{n}} \mathrm{Select}(B_l)$. Then, we decompose each Select(B_l) with Eq. (58). We let $w = \lfloor m/n \rfloor$ and $s' = \lceil s/w \rceil$, and

$$
k_j = \begin{cases} jw & j < s' \\ s & j = n' \end{cases}. \tag{60}
$$

According to Lemma 8, with n_{anc} ancillary qubits, each $\mathrm{Select}(B_{l,k_{j-1}:k_j - 1})$ can be constructed with $O(nw)$ count and $O(\log(nw)) = O(\log n_{\mathrm{anc}})$ depth of Clifford + T circuit. So each Select(B_l) requires gate count $O(nw) \times s' = O(ns)$, and circuit depth $O(\log(n_{\mathrm{anc}})) \times s' = O\left(ns \frac{\log n_{\mathrm{anc}}}{n_{\mathrm{anc}}} \right)$. In this case, we have $n' = \tilde{n}$ in Eq. (57), so the total gate count and circuit depth of Select($B(q)$) is $O(ns\tilde{n})$ and $O\left(ns\tilde{n} \frac{\log n_{\mathrm{anc}}}{n_{\mathrm{anc}}} \right)$ respectively. □

References

1. Nielsen, M. A. & Chuang, I. *Quantum computation and quantum information* (Cambridge University Press, Cambridge, 2000).
2. Aaronson, S. Open problems related to quantum query complexity. *ACM Trans. Quantum Comput.* **2**, 1–9 (2021).
3. Grover, L. K. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.* **79**, 325 (1997).
4. Berry, D. W., Ahokas, G., Cleve, R. & Sanders, B. C. Efficient quantum algorithms for simulating sparse hamiltonians. *Commun. Math. Phys.* **270**, 359–371 (2007).
5. Harrow, A. W., Hassidim, A. & Lloyd, S. Quantum algorithm for linear systems of equations. *Phys. Rev. Lett.* **103**, 150502 (2009).
6. Childs, A. M. & Kothari, R. Simulating sparse hamiltonians with star decompositions. In *Theory of Quantum Computation, Communication, and Cryptography: 5th Conference, TQC 2010, Leeds, UK, April 13-15, 2010, Revised Selected Papers 5*, 94–103 (Springer, 2011).
7. Childs, A. M. On the relationship between continuous-and discrete-time quantum walk. *Commun. Math. Phys.* **294**, 581–603 (2010).
8. Berry, D. W., Childs, A. M., Cleve, R., Kothari, R. & Somma, R. D. Exponential improvement in precision for simulating sparse hamiltonians. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*, 283–292 (2014).

9. Childs, A. M., Kothari, R. & Somma, R. D. Quantum algorithm for systems of linear equations with exponentially improved dependence on precision. *SIAM J. Comput.* **46**, 1920–1950 (2017).

10. Gilyén, A., Su, Y., Low, G. H. & Wiebe, N. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, 193–204 (2019).

11. Chakraborty, S., Gilyén, A. & Jeffery, S. The power of block-encoded matrix powers: Improved regression techniques via faster hamiltonian simulation. In *Proceedings of the 46th International Colloquium on Automata, Languages and Programming (ICALP)* (2019).

12. Babbush, R., Berry, D. W., Kothari, R., Somma, R. D. & Wiebe, N. Exponential quantum speedup in simulating coupled classical oscillators. *Physical Review X* **13**, 041041 (2023).

13. Low, G. H. & Chuang, I. L. Optimal hamiltonian simulation by quantum signal processing. *Phys. Rev. Lett.* **118**, 010501 (2017).

14. Low, G. H. & Chuang, I. L. Hamiltonian simulation by qubitization. *Quantum* **3**, 163 (2019).

15. Martyn, J. M., Rossi, Z. M., Tan, A. K. & Chuang, I. L. Grand unification of quantum algorithms. *PRX Quantum* **2**, 040203 (2021).

16. Clader, B. D. et al. Quantum resources required to block-encode a matrix of classical data. *IEEE Trans. Quantum Eng.* **3**, 1–23 (2022).

17. Sünderhauf, C., Campbell, E. & Camps, J. Block-encoding structured matrices for data input in quantum computing. *Quantum* **8**, 1226 (2024).

18. Gui-Lu, L. General quantum interference principle and duality computer. *Commun. Theor. Phys.* **45**, 825 (2006).

19. Long, G. L. Duality quantum computing and duality quantum information processing. *Int. J. Theor. Phys.* **50**, 1305–1318 (2011).

20. Childs, A. M. & Wiebe, N. Hamiltonian simulation using linear combinations of unitary operations. *Quantum Inf. Comput.* **12**, 901–924 (2012).

21. Cong, I., Choi, S. & Lukin, M. D. Quantum convolutional neural networks. *Nat. Phys.* **15**, 1273–1278 (2019).

22. Wei, S., Chen, Y., Zhou, Z. & Long, G. A quantum convolutional neural network on nisq devices. *AAPPS Bull.* **32**, 1–11 (2022).

23. Li, H.-S., Fan, P., Xia, H. & Long, G.-L. The circuit design and optimization of quantum multiplier and divider. *Sci. China Phys. Mech. Astronomy* **65**, 260311 (2022).

24. Fowler, A. G., Mariantoni, M., Martinis, J. M. & Cleland, A. N. Surface codes: Towards practical large-scale quantum computation. *Phys. Rev. A* **86**, 032324 (2012).

25. Jaques, S. & Rattew, A. G. Qram: A survey and critique. Preprint at https://arxiv.org/abs/2305.10310 (2023).

26. Long, G.-L. & Sun, Y. Efficient scheme for initializing a quantum register with an arbitrary superposed state. *Phys. Rev. A* **64**, 014303 (2001).

27. Grover, L. & Rudolph, T. Creating superpositions that correspond to efficiently integrable probability distributions. Preprint at https://arxiv.org/abs/quant-ph/0208112 (2002).

28. Möttönen, M., Vartiainen, J. J., Bergholm, V. & Salomaa, M. M. Transformation of quantum states using uniformly controlled rotations. *Quantum. Inf. Comput.* **5**, 467–473 (2005).

29. Plesch, M. & Brukner, Č. Quantum-state preparation with universal gate decompositions. *Phy. Rev. A* **83**, 032302 (2011).

30. Zhang, Z., Wang, Q. & Ying, M. Parallel quantum algorithm for hamiltonian simulation. *Quantum* **8**, 1228 (2024).

31. Zhang, X.-M., Yung, M.-H. & Yuan, X. Low-depth quantum state preparation. *Phys. Rev. Res.* **3**, 043200 (2021).

32. Sun, X., Tian, G., Yang, S., Yuan, P. & Zhang, S. Asymptotically optimal circuit depth for quantum state preparation and general unitary synthesis. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* (2023).

33. Rosenthal, G. Query and depth upper bounds for quantum unitaries via grover search. Preprint at https://arxiv.org/abs/2111.07992 (2021).

34. Zhang, X.-M., Li, T. & Yuan, X. Quantum state preparation with optimal circuit depth: Implementations and applications. *Phys. Rev. Lett.* **129**, 230504 (2022).

35. Yuan, P. & Zhang, S. Optimal (controlled) quantum state preparation and improved unitary synthesis by quantum circuits with any number of ancillary qubits. *Quantum* **7**, 956 (2023).

36. Ashhab, S. Quantum state preparation protocol for encoding classical data into the amplitudes of a quantum information processing register's wave function. *Phys. Rev. Res.* **4**, 013091 (2022).

37. Gui, K., Dalzell, A. M., Achille, A., Suchara, M. & Chong, F. T. Spacetime-efficient low-depth quantum state preparation with applications. *Quantum* **8**, 1257 (2024).

38. Childs, A. M., Maslov, D., Nam, Y., Ross, N. J. & Su, Y. Toward the first quantum simulation with quantum speedup. *Proc. Natl. Acad. Sci.* **115**, 9456–9461 (2018).

39. Tang, E. A quantum-inspired classical algorithm for recommendation systems. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing* (ACM Press, New York, 2019).

40. Chia, N.-H., Li, T., Lin, H.-H. & Wang, C. Quantum-inspired sublinear algorithm for solving low-rank semidefinite programming. In *45th International Symposium on Mathematical Foundations of Computer Science* (Schloss Dagstuhl–Leibniz-Zentrum f´ur Informatik, 2020).

41. Nielsen, M. A. A geometric approach to quantum circuit lower bounds. Preprint at https://arxiv.org/abs/quant-ph/0502070 (2005).

42. Bu, K., Garcia, R. J., Jaffe, A., Koh, D. E. & Li, L. Complexity of quantum circuits via sensitivity, magic, and coherence. arXiv:2204.12051 (2022).

43. Eisert, J. Entangling power and quantum circuit complexity. *Phys. Rev. Lett.* **127**, 020501 (2021).

44. Li, L., Bu, K., Koh, D. E., Jaffe, A. & Lloyd, S. Wasserstein complexity of quantum circuits. Preprint at https://arxiv.org/abs/2208.06306 (2022).

45. Biamonte, J. et al. Quantum machine learning. *Nature* **549**, 195–202 (2017).

46. Liu, J., Hann, C. T. & Jiang, L. Data centers with quantum random access memory and quantum networks. *Phys. Rev. A* **108**, 032610 (2023).

47. Liu, J. & Jiang, L. Quantum data center: Perspectives. Preprint at https://arxiv.org/abs/2309.06641 (2023).

48. Selinger, P. Efficient Clifford+T approximation of single-qubit operators. Preprint at https://arxiv.org/abs/1212.6253 (2012).

49. Giovannetti, V., Lloyd, S. & Maccone, L. Quantum random access memory. *Phys. Rev. Lett.* **100**, 160501 (2008).

50. Hann, C. T. et al. Hardware-efficient quantum random access memory with hybrid quantum acoustic systems. *Phys. Rev. Lett.* **123**, 250501 (2019).

51. Hann, C. T., Lee, G., Girvin, S. & Jiang, L. Resilience of quantum random access memory to generic noise. *PRX Quantum* **2**, 020311 (2021).

Acknowledgements

Author contributions

Xiao-Ming Zhang conceived the project. All authors contributed in the preparation of the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at
https://doi.org/10.1038/s41534-024-00835-8.

Correspondence and requests for materials should be addressed to Xiao-Ming Zhang.

Reprints and permissions information is available at
http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.